Threat Intelligence

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

Course Overview

Course Dates: November 4-15, 2024

Duration: 2 weeks

Estimated Time Commitment: 10-15 hours per week

Instructional Hours: 15 contact hours

Delivery Format: Asynchronous online

Target Audience: IT or Cybersecurity practitioners

Required Prerequisites / Background: Participants should have a working knowledge of computers, basic knowledge of computer networks, familiarity with the usage and administration of Windows and Linux, and basic skills with text editing.

CEUs: 1.5, **CPEs:** 18

Course Instructor(s):

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

Course Description

This course focuses on the fundamentals and the application of threat intelligence to cybersecurity. The course lectures are supplemented with hands-on exercises to reinforce the learning process. These exercises include threat hunting, application of kill, utilization of open-source threat intelligence tools, and application of threat sharing. The lectures build upon the National Institute of Standards and Technology (NIST) guidelines documented in the following Special Publications (SP): 800-181 rev 1 (NICE Cybersecurity Workforce Framework), NIST-SP-800-154 (Data-Centric System Threat Modeling), and NIST-SP-800-150 (Guide to Cyber Threat Information Sharing).

The course is divided into 5 modules. Each module includes a discussion segment, assessment, or hands-on exercises as appropriate. Each student is expected to participate actively in the course.

NIST NICE Cybersecurity Workforce Framework Mapping

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

Cybersecurity Work Roles and Categories:

- Cyber Defense Analyst (Protect and Defend, PR-CDA-001)
- Threat/Warning Analyst (Analyze, AN-TWA-001)

Course Information

Materials:

No Required Texts

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, you agree to abide by the Computing Resources Usage Agreement provided to you.

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	40%

Projects/Exercises	60%
Total:	**100%**

Course Overview / Schedule

Modules and Lessons	Assessment
Module 1: Fundamentals of Threat Intelligence (TI) and Threat Modelling Topics: ○ Cyber Threats and threat actors ○ Strategies and capabilities ○ Maturity models and frameworks ○ Threat intelligence in risk management, Security Incident Event Management, and Incident Response ○ Cyber Kill Chain ○ Courses of Action Matrix ○ MITRE ATT&CK Framework	▪ Quiz ▪ Discussion
Module 2: Threat Intelligence Sources Topics: ▪ Threat intelligence feeds ▪ Threat hunting and tactics ▪ Data collection methods ○ Open-Source Intelligence (OSINT) ○ Human Intelligence (HUMINT) ○ Cyber Counterintelligence (CCI) ○ Indicators of Compromise (IoCs)	▪ Quiz ▪ Discussion
Module 2 Hands-on activity Topics: ○ Threat Hunting tactics	▪ Completion of activity
Module 3: Open-Source Threat Intelligence Tools Topics: ○ Open-Source Threat Exchange (OTX) Framework ○ Threatcrowd search engine ○ OpenPhish ○ Virustotal ○ Maltego ○ Splunk ○ Elasticstack	▪ Quiz ▪ Discussion

○ Fireeye Analysis Tools (Redline IoC Tool) ○ Network Traffic Capture and Analysis Tools ○ AlienVault ○ Cisco Talos ○ Microsoft Security Advisory	
Module 3 hands-on activity ○ Open-source Threat Intelligence tool usage	▪ Completion of activity
Module 4: Consuming Threat Intelligence Topics: ○ Sharing platforms ○ Regulations for sharing data ○ Threat intelligence dissemination: Structured Language for Cyber Threat Intelligence (STIX), Trusted Automated Exchange of Intelligence Information (TAXII), YARA malware tool ○ MISP ○ FireEye IoC Editor ○ Threat Intelligence Matrix	▪ Quiz ▪ Discussion
Module 4 Hands-on activity Topics: ○ Using Threat Sharing Platforms	▪ Completion of activity
Module 5: Threat Intelligence at the Strategic, Operational, and Tactical levels Topics: ○ Recognizing the need for appropriate level of intelligence dissemination ○ Threat Intelligence Analysts: Strategic, Operational, and Tactical levels ○ Threat Intelligence Tools for each level	▪ Discussion ▪ Quiz
Module 5 Hands-on activity Topics: ○ Threat Intelligence Levels Exercise	▪ Completion of activity