CENTER FOR **CYBERSECURITY**
AT THE UNIVERSITY OF WEST FLORIDA

Industrial Control Systems Threat Intelligence

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

Course Overview

Course Dates: June 3-14, 2024

Duration: 2 weeks

Estimated Time Commitment: 10-15 hours per week

Instructional Hours: 15 contact hours

Delivery Format: Asynchronous online

Target Audience: Courses: IT, OT, or Cybersecurity practitioners

Required Prerequisites / Background: This course requires no prior knowledge of Industrial Control Systems. However, basic knowledge of computer networks is needed to fully comprehend the materials in this course.

CEUs: 1.5, **CPEs:** 18

Course Instructor(s):

Instructor	Email
Dr. Guillermo Francia III	gfranciaiii@uwf.edu
Dr. Elizabeth Rasnick	erasnick@uwf.edu

Course Description

This course focuses on the fundamentals and the application of threat intelligence to industrial control systems and cybersecurity. The course lectures are supplemented with hands-on exercises to reinforce the learning process. 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).

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 Infrastructure Support Specialist (Protect and Defend, PR-INF-001)
- Cyber Operator (Collect and Operate, CO-OPS-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 ▪ Threat Intelligence at the Strategic, Operational, and Tactical levels	▪ Quiz ▪ Discussion
Module 1 Hands-on Activity. Topics: ▪ Case study in applying the cyber kill chain in ICS	▪ Completion of activity
Module 2: Threat Intelligence Sources. Topics: ▪ Threat intelligence feeds ▪ Threat hunting and tactics ▪ Data collection methods ○ Open Source Intelligence (OSINT) ○ Human Intelligence (HUMINT) ○ Cyber Counter-Intelligence (CCI) ○ Indicators of Compromise (IoCs) ▪ Exposure to Cuckoo Sandbox for automated malware analysis	▪ 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 ▪ Fireeye Analysis Tools (Redline IoC Tool) ▪ Network Traffic Capture and Analysis Tools ▪ AlienVault ▪ Cisco Talos ▪ Microsoft Security Advisory	▪ Quiz ▪ Discussion
Module 3 hands-on activity. ▪ Open source Threat Intelligence tool usage	▪ Completion of activity
Module 4: Threats in ICS Environment. Topics: ▪ ICS Protocols and their security considerations ○ Modbus over TCP ○ Distributed Network Protocol ▪ Renewable Energy (RE) Fundamentals ▪ Vulnerabilities in RE systems ▪ Attacks on ICS protocols ▪ Mitigation techniques	▪ Quiz ▪ Discussion
Module 5: Threat Sharing. Topics: ▪ Sharing platforms. ▪ Threat intelligence dissemination: Structured Language for Cyber Threat Intelligence (STIX), Trusted Automated Exchange of Intelligence Information (TAXII). ▪ Malware Information Sharing Platform (MISP). ▪ Strategic, Operational and Tactical Intelligence	▪ Discussion ▪ Quiz
Module 5 Hands-on activity Topics: ▪ Tabletop exercise on Threat Intelligence Types	▪ Completion of activity