Threat Intelligence with AI

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

Course Overview

Course Dates: April 6 - 17, 2026

Duration: 2 weeks

Estimated Time Commitment: 10 hours per week

Instructional Hours: 15 contact hours

Delivery Format: Asynchronous online

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

Required Background: Learners should be comfortable using the internet and have a basic understanding of how the internet works.

CEUs: 1.5, **CPEs:** 18

Course Instructor(s):

Instructor	Email
Dr. Elizabeth Rasnick	erasnick@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. The lectures build upon the National Institute of Standards and Technology (NIST) guidelines documented in the following Special Publications (SP): NIST-SP 800-30 (Risk Management Guide for IT Systems), 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. The course will culminate with the application of lessons learned on a capstone hands-on exercise involving a cyber kill chain scenario.

NIST NICE Cybersecurity Workforce Framework Mapping

The course addresses cybersecurity work roles as identified in NIST's Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce

Framework available at
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.

Cybersecurity Work Roles and Categories:

- Cyber Defense Analyst (Protect and Defend, PR-CDA-001)
- Cyber Defense Incident Responder (Protect and Defend, PR-CIR-001)
- Vulnerability Assessment Analyst (Protect and Defend, PR-VAM-001)
- Threat/Warning Analyst (Analyze, AN-TWA-001)
- Exploitation Analyst (Analyze, AN-EXP-001)
- 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).

Learning Outcomes mapped to the NICE Cybersecurity Workforce Framework Knowledge, Skills and Abilities (KSAs):

Upon completion of the course, students will be able to:

- Demonstrate the ability to recognize cyber threats and vulnerabilities (K0005)
- Understand Insider Threat investigations, reporting, investigative tools and laws/regulations. (K0107)
- Understand adversarial tactics, techniques, and procedures. (K0110)
- Apply knowledge of current and emerging threats/threat vectors. (K0151)
- Understand cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks). (K0177)
- Analyze target or cyber threat actors and procedures. (K0548)
- Perform packet-level analysis using appropriate tools (S0046)
- Perform a log review in identifying evidence of past intrusions. (S0120)
- Identify cyber threats which may jeopardize organization and/or partner interests (S0229)
- Respond and take local actions in response to threat sharing alerts from service providers. (S0371)

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 Learning 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 an 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.

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
Labs	50%
Quizzes	50%
Total:	**100%**

Course Outline

Modules and Lessons	Assessments
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	**Lab** Case study: Applying the cyber kill chain **Quiz**
Module 2: Threat Intelligence Sources Topics: ▪ Threat intelligence feeds ▪ Threat hunting and tactics ▪ Data collection methods o Open Source Intelligence (OSINT) o Human Intelligence (HUMINT) o Cyber Counter-Intelligence (CCI) o Indicators of Compromise (IoCs) ▪ Exposure to Cuckoo Sandbox for automated malware analysis	**Lab** Threat hunting tactics **Quiz**
Module 3: Open Source Threat Intelligence Tools Topics:	**Lab** Using Open Source Tools

▪ 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**
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	**Lab** Using Threat Sharing Platforms **Quiz**
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	**Lab** Threat Analysis **Quiz**