ICS 688 : Cyber Threat Intelligence

A. Course Description

Credits: 4

Prerequisites: ICS 462 Operating Systems AND knowledge of Fundamental Concepts in Cybersecurity Concepts” OR By Instructor Permission.

Lab Hours/ Weeks: Corequisites: None

Lecture Hours/ Week :

MnTC Goals: None

The course will provide students with foundational concepts and practical skills in the field of cyber threat intelligence that can be leveraged to defend against sophisticated network intrusions and loss of proprietary information. The course will discuss various phases of the intelligence lifecycle including developing intelligence requirements, collecting, analyzing, and disseminating information; and using cyber threat intelligence to improve security at the tactical, operational, and strategic levels.

B. Course Effective Dates: 01/10/2016 - Present

C. Outline of Major Content Areas:

See Course Description for major content areas.

D. Learning Outcomes (General)

1. To understand CTI, its key characteristics, value, and benefits.
2. To apply CTI at the tactical, operational, and strategic levels in order to identify sophisticated attacks and improve existing defense mechanisms.
3. To examine various models to create consistent and repeatable Cyber Threat Intelligence output.
4. To characterize intruders by understanding tactics, techniques, and procedures that are involved in an attack.
5. To interpret various indicators of compromise that are used in performing intrusion analysis.
6. To demonstrate the understanding of various protocols and frameworks involved in sharing of cyber threat intelligence.
7. To collect and apply cyber threat intelligence from various sources with an emphasis on open source intelligence

E. Learning Outcomes (MN Transfer Curriculum)

This contains no goal areas.

G. Special Information

None