Malware Prevention, Discovery and Recovery (PER-382)

INSTRUCTOR-LED. 32 hours.

An intermediate-level course designed for technical personnel who monitor and protect critical cyber infrastructure. Learn how to recognize, identify, and analyze malware; the remedia-tion process to eliminate the malware; and proper procedures to recover from the attack and regain network connectivity.

Malware Prevention, Discovery, and Recovery (MPDR)

MPDR will expose participants to analysis of malicious software used by cyber-criminals and cyber-terrorists. After an introduction to modern malware, participants will learn how to prevent a malware outbreak, discover and identify malware through active network traffic analysis, prepare for dynamic analysis of malware samples of various types and intent, and how to isolate, remediate, and recover from a malware outbreak. Finally, the course will conclude with a review of dynamic malware analysis and a look at emerging trends in the use of malicious software in network intrusions and data theft.

This course is an intermediate level, hands-on course where knowledge and basic experience is required. Alternative experience may be considered in lieu of listed requirements, based upon seating availability and review by CDI admissions staff.

Prerequisite: Participants should have 2 years experience as a system or network administrator, or as an IT security specialist; or should have successfully completed the CDI course, Comprehensive Cybersecurity Defense (CCD). Experience with computer network intrusion response is preferred.

Comprehensive Cybersecurity Defense (PER-256)

INSTRUCTOR-LED. 32 hours.

A basic-level course designed for technical personnel who monitor and protect our nation’s critical cyber infrastructure. The course intro-duces students to cyber-defense tools that will assist in monitoring their computer networks and imple-menting cybersecurity measures to prevent or greatly reduce the risk of a cyber-based attack. This course integrates hands-on computer lab applications to maximize the student’s learning experience.

Comprehensive Cybersecurity Defense (CCD)

CCD is a basic level course. After an introduction to cybersecurity, participants will learn how to protect network systems by survey of the following: planning and preparation of defenses; installation and administration of defenses; hardening network defenses; administration of defenses; monitoring defenses; and testing and modifying defenses—followed by a review of cybersecurity defenses and emerging trends.

Prerequisite: Participants should have some experience as a cybersecurity professional, a basic understanding of network concepts, and a basic understanding of computer operating systems.

Preferred Prerequisite: Experience as a system or network administrator.