DC3 Cyber Training Academy

FY23 April Offerings

Enroll Now

Click on the "Enroll Now" link to view the online catalog and to register for classes. Please contact the DC3 Cyber Training Academy Registrar with any questions.

Cyber Fundamentals 200 (CF200)

CF200 is an 80-hour course that serves as the second installment of a two-part curriculum to provide foundational cyber knowledge to cyberspace workforce elements and Department of Defense (DOD) personnel, whose duties include the protection of DOD information systems from unauthorized and/or illegal access. The course comprises three units with multiple lessons; each unit culminates in a unit milestone exam and the 2 course ends with a Capstone Exam. There is a test-out option available to permit qualified personnel to bypass the course.
Delivery: Online asynchronous (Self-paced/no instructor)
Duration: 80 hours of training over 3 weeks
Prerequisite: None
Scheduled offering:
CF200-2308-OL (17 APR – 5 MAY)

Cyber Incident Response Course (CIRC)

The Cyber Incident Response Course (CIRC) is an 80-hour course that prepares students in cyber incident response and evidence collection. In this course, students are provided various scenarios to understand and develop response protocols in a real-world environment. Using trusted forensic tools, students identify and extract digital evidence from various devices such as computers, cell phones and small form factor digital storage devices. Students are taught how to properly document evidence using lawful, professional techniques to ensure the legal admissibility of the seized evidence. CIRC contains three units with quizzes and a course Capstone Exercise.
Delivery: In-residence
Duration: 80 hours of training over 2 weeks
Prerequisite: INCH
IACET CEU-eligible, ACE Recommendation
Scheduled Offerings:
CIRC-2310 (10-21 APR)

DC3 Cyber Training Academy

FY23 April Offerings

Cyber 101 (CY101)

Cyber 101 (CY101) is a 40-hour course that is designed to provide fundamental cyber knowledge to students interested in developing cyber competency or who are in roles where they support cyber operations (such as CPTs, MDTs). CY101 is a requirement for any personnel identified in DoDD 8140 as a “cyber enabler.” The course consists of five units containing modules and lessons, unit Milestone Exams, and a final, graded Capstone Exam.
Delivery: Online asynchronous (Self-paced/no instructor)
Duration: 40 hours of training over 3 weeks
Prerequisite: None
Scheduled Offering:
CY101-2308-OL (17 APR – 5 MAY)

Forensics and Intrusions in a Windows Environment (FIWE)

Forensics and Intrusions in a Windows Environment (FIWE) is an 80-hour scenario-based training course developing students’ skills in conducting a full investigation of a network intrusion. FIWE is designed for Defense Criminal Investigative Organizations (DCIOs), Department of Defense (DOD) intrusion analysts, network operators, and investigators. Students conduct forensic examinations of victim devices, analyze log data and network traffic data, create an event timeline, perform malware analysis, and prepare narrative reports of their findings. These skills prepare students to perform a variety of network investigations. FIWE contains three modules and culminates with a final, graded exam.
Delivery: In-residence
Duration: 80 hours of training over 2 weeks
Prerequisite: NIB and WFE-E
IACET CEU-eligible, ACE Recommendation
Scheduled Offering:
FIWE-2306 (24 APR – 5 MAY)

DC3 Cyber Training Academy

FY23 April Offerings

Introduction to Cyber Investigations (ICI)

Introduction to Cyber Investigations (ICI) is a 40-hour course that prepares students to perform or support the role of a case agent responsible for a basic cyber investigation. ICI is designed for Defense Criminal Investigative Organizations (DCIOs), cyber-intrusions investigators, information assurance professionals, and prospective lab examiners. Students learn basic technical concepts and the legal framework that guides the conduct of cyber investigations. Students also study special aspects of cyber case management (including online evidence collection) and subjects of cyber investigations. ICI contains five modules with module assignments and exercises and culminates with a final, graded exam.

Delivery: Online
Duration: 40 hours of training over 5 weeks
Prerequisite: None
ACE Recommendation
Offering:
ICI-2303-OL (3 APR – 4 MAY)

Introduction to Networks and Computer Hardware In-Residence (INCH-RES)

INCH-RES is a 40-hour course that teaches computer basics, network theory, and input/output device identification and function. INCH-RES is designed for personnel working in or interested in pursuing a career in fields such as computer intrusion investigations, information assurance, and digital evidence examination. Students explore common operating system functionality and the use of the command line in Microsoft Windows. The course material and practical exercises introduce troubleshooting, security, and safety terminology and techniques, complete with the physical disassembly and reassembly of a computer. INCH-RES contains 10 modules and culminates in Capstone Exam. A test-out option is available to permit qualified personnel to bypass the course.

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
IACET CEU-eligible, ACE Recommendation
Scheduled offerings:
INCH-RES-2308 (3-7 APR)
INCH-RES-2309 (24-28 APR)

Please note that INCH Test Out options are available.

DC3 Cyber Training Academy

FY23 April Offerings

Introduction to Networks and Computer Hardware (INCH) OL/ILV

INCH is a 40-hour course that teaches computer basics, network theory, and input/output device identification and function. INCH is designed for personnel working in or interested in pursuing a career in fields such as computer intrusion investigations, information assurance, and digital evidence examinations. Students explore common operating system functionality and the use of the command line in Microsoft Windows. The course material and practical exercises introduce troubleshooting, as well as security and safety terminology and techniques. INCH contains 10 modules and culminates with a Capstone Exam.

Delivery: Online and Instructor-Led Virtual
Duration: Online is 40 hours of training over 4 weeks
Instructor-Led Virtual is 40 hours of training over 5 days
Prerequisite: None
IACET CEU-eligible, ACE Recommendation
Scheduled offering:
INCH-2332-OL (10 APR – 4 MAY)

Introduction to Networks and Computer Hardware Test Out (INCH-TO)

Introduction to Networks and Computer Hardware Test Out (INCH Test-Out) provides students with the opportunity to demonstrate mastery of both the content knowledge portion of the course material in addition to a hands-on desktop computer tear down and rebuild. The content knowledge portion covers computer basics, network theory, and input/output device identification and function. Students must also demonstrate mastery of common operating system functionality and the use of the command line in Microsoft Windows. Students have three hours to complete this portion of the Test -Out. An additional 30 minutes of the test out requires students to complete the physical disassembly and reassembly of a desktop computer. Students must achieve a 70% or greater on both sections of the Test-Out to be eligible to register for the Cyber Incident Response Course (CIRC). If the student fails to successfully complete the INCH Test-Out, they will have the opportunity to request registration in the one-week INCH-RES course offered at a later date.

Delivery: In-residence
Duration: 3 hours over 1 day
Prerequisite: None
Schedule offerings:
INCH-TESTOUT-2307 (7 APR)

DC3 Cyber Training Academy

FY23 April Offerings

Linux Essentials (LXE)

Linux Essentials (LXE) is a 40-hour course that teaches core concepts and techniques of Linux system management and administration. LXE is designed for students who want to develop greater understanding of Linux or who conduct investigative and security activities associated with Linux environments. Students acquire intermediate Linux skills used in cyber investigation studies and real-world investigative and security tasks. The course prepares students to carry out functions and tasks relevant to any standard Linux environment. LXE contains nine lessons and culminates with a final, graded exam.

Delivery: Online
Duration: 40 hours of training over 4 weeks
Prerequisite: None
Schedule offerings:
LXE-2305-OL (10 APR – 4 MAY)

Network + (NET+)

NET+ is a bootcamp-style course that builds on your existing user-level knowledge and experience with computer operating systems and networks so you can master the fundamental skills and concepts needed for success in any networking career. Students are taught to describe the major networking technologies and systems of modern networks and configure, manage, and troubleshoot modern networks. Students must make their own arrangements to take the exam at any CompTIA testing center. Vouchers are not included.

Delivery: In-residence
Duration: Approximately 40 hours over 1 week
Prerequisite: None
Scheduled offerings:
NET+-2306 (10-14 APR)
NET+-2307 (17-21 APR)

DC3 Cyber Training Academy

FY23 April Offerings

Network Intrusions Basics (NIB)

NIB is a 10-hour course that provides core knowledge needed to perform a network intrusion investigation. Students learn the language of intrusions and explore network fundamentals, including network architecture. The concepts presented in this course prepare students for additional network investigations courses. NIB contains two modules, each comprising two lessons, and a final, graded exam.

Delivery: Online asynchronous (Self-paced/no instructor)
Duration: Approximately 10 hours over 1 week
Prerequisite: None
Scheduled offerings:
NIB-2324-OL (3-7 APR)
NIB-2325-OL (10-14 APR)
NIB-2326-OL (17-21 APR)
NIB-2327-OL (24-28 APR)

Security + (SEC+)

Security+ (SEC+) is a bootcamp-style course that will be a significant part of your preparation to pass the CompTIA Security+ (Exam SY0-601) certification examination. The CompTIA SEC+ certification will help you build your cybersecurity skill set so you can confidently perform your duties in any entry-level security role. Vouchers are not included in this course and students must make their own arrangements to take the exam at any CompTIA testing center.

Delivery: In-Residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offerings:
SEC+-2305 (24-28 APR)

Windows Forensic Examinations - EnCase (WFE-E)

WFE-E is a 40-hour course designed for students who wish to develop skills in conducting a computer forensic examination of digital devices and data including Defense Criminal Investigative Organizations (DCIOs). WFE-E instructs students in a comprehensive forensic examination process, including technical procedures and reporting. While students will use the EnCase forensic tool to conduct course examinations of Windows systems, the skills, processes, and techniques are applicable regardless of the tool a student will use in the field. WFE-E contains six modules and culminates with a final, graded exam.

Delivery: In-residence and Online
Duration: 40 hours of training over 1 week in-residence or over 4 weeks online
Prerequisite: CIRC
IACET CEU-eligible
Scheduled offering:
WFE-E-2308 (24-28 APR)
