DC3 Cyber Training Academy

FY23 March 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.

A+ (A+)

A+ course is the industry standard for launching IT careers. In this bootcamp-style course, students install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on personal computers, digital devices, and operating systems. A+ is designed for individuals with basic computer user skills who are interested in obtaining a job as an entry-level IT technician. It is also designed for students seeking the CompTIA A+ certification who want to prepare for the CompTIA's A+ Core 1 (220-1001) and Core 2 (220-1002) certification exams. Students must make their own arrangements to take the exam at any CompTIA testing center. Vouchers are not included with this course.
Delivery: In-residence
Duration: 40 hours of training over 1 week
CompTIA CEU-eligible
Prerequisite: None
Scheduled offering:
A+-2304 (20-24 MAR)

Cyber Analyst Course (CAC)

The Cyber Analyst Course (CAC) is an 80-hour course that presents analytical methodologies and information sources applicable to a cyber environment. CAC is designed for Defense Criminal Investigative Organizations (DCIOs), cyber-intrusions investigators, information assurance professionals, and prospective lab examiners. Topics include interpreting analysis and forensic reports, internet research, computer system and network analysis, log analysis, data-hiding techniques, and intrusion identification. The course also covers using specialized analytical software and writing analysis reports. CAC contains six modules and culminates with a Final Knowledge Exam and a Final Performance Exam.
Delivery: In-residence
Duration: 80 hours of training over 2 weeks
Prerequisite: INCH
Scheduled offering:
CAC-2302 (6-17 MAR)

Cyber Fundamentals 100 (CF100)

CF100 is an 80-hour course that introduces students to hardware and software basics, operating systems, network architecture, and internet applications. It is the first installment of a two-part curriculum providing foundational cyber knowledge to cyberspace workforce elements and Department of Defense (DOD) personnel, whose duties include protecting DOD information systems from unauthorized and/or illegal access. The course contains three units comprising multiple lessons; each unit culminates in a unit Milestone Exam and the course ends with a Capstone Exam. A test-out option is available at the start of each unit so that qualified personnel may bypass portions of the course.

Delivery: Online asynchronous (Self-paced/no instructor)
Duration: 80 hours of training over 3 weeks
Prerequisite: None
Scheduled offering:
CF100-2306-OL (6-24 MAR)
CF100-2307-OL (27 MAR – 14 APR)

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:
CF200-2306-OL (6-24 MAR)
CF200-2307-OL (27 MAR – 14 APR)

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-2309 (20-31 MAR)

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:
CY101-2306-OL (6-24 MAR)
CY101-2307-OL (27 MAR – 14 APR)

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-2329-OL (13 MAR – 6 APR)
INCH-2330-OL (13 MAR – 6 APR)

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-2306 (10 MAR)

FY23 March Offerings

Log Analysis (LA)

LA is a 50-hour course that provides a comprehensive understanding of log analysis techniques. LA is designed for cyber investigators or analysts interested in furthering their skills in determining the how, when, and where of a network intrusion through log file analysis and investigation. Students learn how to process logs from Windows and Linux operating systems, firewalls, intrusion detection systems, and web and email servers. Students learn how to assemble evidence found in logs to assist in tasks ranging from building a case to recognizing an intrusion. LA contains three modules comprising multiple lessons and culminates with a final, graded exam.

Delivery: Online
Duration: 50 hours of training over 5 weeks
Prerequisite: None
Scheduled offering:
LA-2302-OL (27 MAR – 27 APR)

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+-2304 (13-17 MAR)
NET+-2305 (27-31 MAR)

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-2320-OL (6-10 MAR)
NIB-2321-OL (13-17 MAR)
NIB-2322-OL (20-24 MAR)
NIB-2323-OL (27-31 MAR)

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-2306-OL (6-30 MAR)