DC3 Cyber Training Academy

FY22 August Offerings

Enroll Now

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.

Target Audience: This course is for government civilian and military personnel only - Federal employees and contractors not allowed to take this course.

Delivery: In-residence

Duration: 40 hours of training over 1 week

CompTIA CEU-eligible

Prerequisite: None

Scheduled offering:
A+-2213 (22-26 AUG)

A+-2214 (29 AUG – 2 SEPT)

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:
CF100-2213-OL (22 AUG – 9 SEPT)

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:
CF200-2212-OL (1-19 AUG)
CF200-2213-OL (22 AUG – 9 SEPT)

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-2206-OL (22 AUG – 22 SEPT)

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-2241-OL (1-25 AUG)
INCH-2242-ILV (15-19 AUG)
INCH-2244-OL (29 AUG – 22 SEPT)
INCH-2245-OL (29 AUG – 22 SEPT)

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 offering:
INCH-RES-2243 (29 AUG – 2 SEPT)
Please note that INCH Test Out options are only available.

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 offering:
INCH-TESTOUT-2207 (5 AUG)
INCH-TESTOUT-2208 (12 AUG)
INCH-TESTOUT-2209 (19 AUG)
INCH-TESTOUT-22010 (26 AUG)

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

IACET CEU-eligible, ACE Recommendation

Scheduled offering:
LA-2203-OL (22 AUG – 22 SEPT)

DC3 Cyber Training Academy

FY22 August Offerings

Linux Essentials (LXE)

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 offering:
LXE-2210-OL (15 AUG – 8 SEPT)

Managing Cyber Investigation Units (MCIU)

Managing Cyber Investigation Units (MCIU) is a 30-hour course that prepares students to take on or support the role of manager of a cyber investigation unit (CIU). Students learn how to establish a CIU at the organization level and how to oversee operational policies and procedures. Students also explore requirements and best practices for personnel and facilities. MCIU includes instruction on the importance of training personnel to maintain consistent lab quality and certification standards. MCIU contains four modules, each culminating in a Module Discussion Question Exam; the course ends with a final, graded exam.

Delivery: Online

Duration: Approximately 30 hours over 3 weeks

Prerequisite: None

Scheduled offering:
MCIU-2203-OL (15 AUG – 1 SEPT)

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 offering:
NET+-2208 (1-5 AUG)

NET+-2209 (15-19 AUG)

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 offering:
NIB-2223-OL (1-5 AUG)
NIB-2224-OL (8-12 AUG)
NIB-2225-OL (15-19 AUG)
NIB-2226-OL (22-26 AUG)

Network Mapper (NMAP)

Network Mapper (NMAP) is an 8-hour course that provides instruction in using the Network Mapper tool to manage vulnerabilities, verify baseline configuration compliance, and identify risk among communication protocols, data services, and associated ports. NMAP is designed for work roles assigned to the specific task of exploring networks to isolate vulnerabilities and applying programs that protect exploitable ports from attacks. Students learn how to conduct reconnaissance on adversary networks. The course provides functional information and focuses on useful, real-life examples that students can immediately apply. NMAP contains five modules and culminates with a Final Exam.

Delivery: Online

Duration: 8 hours of training over 5 days

Prerequisite: INCH

Offering:
NMAP-2203-OL (1-5 AUG)

Network Traffic Collection (NTC)

NTC is a 40-hour course that prepares students to strategically place monitoring sensors in a network to capture traffic to and from a specific host. NTC is designed for Department of Defense (DOD), cyber-intrusions investigators, information assurance professionals, prospective lab examiners, and military intelligence and 5 counterintelligence personnel. Students examine how to evaluate a network, both physically and logically, to determine proper sensor placement. Students also study how to filter network traffic to comply with wiretap authority, hide the presence of the monitoring workstation on the network, and evaluate captured traffic for the proper content. NTC contains five modules and culminates with a final, graded exam.

Delivery: In-residence

Duration: Approximately 40 hours over 1 week

Prerequisite: None

Scheduled offering:
NTC-2206 (22-26 AUG)

OpenVAS (OPV)

OPV is an 8-hour course that provides instruction in using OpenVAS software to run vulnerability scans, generate reports, and analyze the results. This course is designed for vulnerability management analysts, information security analysts, cybersecurity specialists, and risk and vulnerability engineers. Students install OpenVAS using the command line and operate the Greenbone Security Assistant interface to navigate and customize the software. Practical exercises train students on OpenVAS terminology and techniques. OPV contains four modules and ends with a final, graded exam.

Delivery: Online

Duration: 8 hours of training over 1 week

Prerequisite: None

Scheduled offering:
OPV-2203-OL (8-13 AUG)

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 offering:
SEC+-2210 (8-12 AUG)
SEC+-2211 (22-26 AUG)

DC3 Cyber Training Academy

FY22 August Offerings

Technology Evidence in Domestic Abuse (TEDA)

TEDA is a 90-minute course that provides first responders an overview of the role that technology can play in domestic abuse and violence cases. TEDA introduces critical concepts on the intersection of technology and domestic abuse and violence, including how abuse manifests, underlying dynamics of abuse, signs of escalation, relevant UCMJ articles, DoD policies, and industry best practices for the collection of digital evidence.

Delivery: Online asynchronous (Self-paced/no instructor)

Duration: 1 hour and 30 minutes over 1 week

Prerequisite: None

Scheduled offering:
TEDA-2219-OL (1-5 AUG)

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

Duration: 40 hours of training over 1 week

Prerequisite: CIRC

IACET CEU-eligible

Scheduled offering:
WFE-E-2214 (29 AUG – 2 SEPT)