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.

Cryptocurrency Activities (CCA)

Cryptocurrency Activities (CCA) is a 40-hour in-residence training course designed for law enforcement and counterintelligence professionals and provides students with an understanding of cryptocurrency fundamentals and the skills necessary to conduct investigations into cryptocurrency transactions. The course immerses students in scenario-based exercises that allow them to practice and reinforce what they have learned while using trusted resources. CCA culminates with a graded Final Exam.

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offering:
CCA-2504 (17-21 MAR)

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:
CF200-2505-OL (3-21 MAR)
CF200-2506-OL (24 MAR – 11 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 Offering:
CIRC-2505 (24 MAR – 4 APR)

CompTIA Cloud+ (Cloud+)

The CompTIA Cloud+ bootcamp is 40 hours over 5 days, and it helps validate essential skills necessary to implement, maintain, optimize and troubleshoot cloud-based infrastructure services. Cloud+ prepares the student for the work roles of Network Operations Specialist, Systems Administrator, Enterprise Architect and Security Architect. The DC3 Cyber Training Academy does not provide exam vouchers for CompTIA courses. Students must obtain their own vouchers and make their own arrangements to take the exam at any CompTIA testing location.

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled Offering:
Cloud+-2502-OL (10-14 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:
CY101-2505-OL (3-21 MAR)
CY101-2506B-OL (17 MAR – 4 APR)
CY101-2506-OL (24 MAR – 11 APR)

Cybersecurity Analyst (CySA+)

Cybersecurity Analyst (CySA+) is a bootcamp-style course that teaches incident detection, prevention, and response through continuous security monitoring for success in a high-stakes analysis. Students learn processes in security operations, vulnerability management, incident response and management, and how to apply best practices for reporting and communication. Vouchers are not included.
Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled Offering:
CySA+-2505 (17-21 MAR)

CompTIA DataSys+ (DataSys+)

The CompTIA DataSys+ bootcamp is a 40-hour course that provides the knowledge and skills required to deploy, manage, and maintain databases, including employing the fundamentals of scripting and programming in a database environment while using security and business continuity best practices. The DC3 Cyber Training Academy does not provide exam vouchers for CompTIA courses. Students must obtain their own vouchers and make their own arrangements to take the exam at any CompTIA testing location.

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled Offering:
DataSys+-2502-OL (10-14 MAR)

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 or 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 offerings:
INCH-2509-OL (3-27 MAR)
INCH-2510-OL (3-27 MAR)
INCH-2511-OL (31 MAR – 24 APR)
INCH-2512-OL (31 MAR – 24 APR)

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-2504 (10-14 MAR)

Please note that INCH Test Out options are available.
INCH-TESTOUT-2502 (28 MAR)

Linux+ (Linux+)

The Computing Technology Industry Association's (CompTIA) Linux+ proves you have the skills administrators need to secure the enterprise, power the cloud, and keep systems running. This bootcamp-style course covers an evolving job role that focuses more on how Linux powers the cloud. Students will review cutting edge technologies that help automate and orchestrate business processes, including infrastructure as code and containers. Vouchers are not included.

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled Offering:
Linux+-2504 (17-21 MAR)

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
Scheduled offerings:
LXE-2504-OL (3-27 MAR)
LXE-2505-OL (31 MAR – 24 APR)

Mac Forensics (MACF)

The Mac Forensics (MACF) course focuses on conducting digital investigations of Macintosh operating systems (macOS) and iPhone operating systems (iOS) in a forensically sound manner. It builds on the foundation of the Forensics Intrusions in a Windows Environment course and introduces best practices and relevant technical aspects of macOS forensic examinations and incident response. It includes scenarios that build upon each other so students can practice what they learn using trusted forensic tools

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offerings:
MACF-2505 (24-28 MAR)

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+-2503 (10-14 MAR)

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-2504 (17-21 MAR)

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-2503-OL 31 MAR – 4 APR)

Penetration Testing (PenTest+)

Penetration Testing (PenTest+) is a bootcamp-style course that covers all penetration testing stages and teaches vulnerability management. Students learn planning and scoping, information gathering and vulnerability scanning, how to apply best practices for reporting and communication, updated approaches to attacks and exploits, code analysis, and uses of various tools. Vouchers are not included.

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled Offering:
PenTest+-2503 (3-7 MAR)

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+-2505 (24-28 MAR)

Windows Forensic Examinations (WFE)

WFE provides training that enables professionals to conduct digital analysis of Windows systems in a forensically reliable manner. Building on the foundation of the Cyber Incident Response Course (CIRC), this course introduces best practices and relevant technical aspects of Windows forensic examinations. The course immerses students in mini-scenarios that escalate in difficulty, allowing them to practice and reinforce what they have learned while using trusted forensic tools, and provides a longform practice that prepares students for the Capstone Exam.
Delivery: In-residence
Duration: 80 hours of training over 2 weeks in-residence
Prerequisite: CIRC
Scheduled offering:
WFE-2505 (31 MAR – 11 APR)