skillsoft global knowledge™

CSFI: DEFENSIVE CYBER OPERATIONS ENGINEER (DCOE)

Course Code: 9733

Develop your cyberspace operations skills for the deployment of NETOPS, DCO, and OCO.

Students will develop the skills for executing defensive cyberspace operations (DCO) into organizational missions. Adversarial tactics, techniques, and procedures (TTPs) and associated tools are presented following the cyber kill chain for students to learn to defend friendly networks against current and emerging threats. Using multiple labs, this course provides students with hands-on exposure to deploy live attacks and analysis in a controlled environment to then learn how to prevent, detect, and counter such activities.

The DCOE training provides a unique opportunity to certify in a critical field of cyberspace operations, enhancing mission readiness and employability. The DCOE certification follows the NICE work role and standards for a Cyber Operator.

This course in endorsed by Capitol Technology University (CTU), a designated National Security Agency (NSA) Center of Excellence.

What You'll Learn

- Cyberspace Operations and Cyber Mission Force
- Cyber Kill Chain
- Kali Linux
- Reconnaissance (Passive and Active)
- PBED for Cyberspace Operations
- Attack Across Networks and Systems
- Persistent, Integrated Operations
- Network Protection

Who Needs to Attend

- Anyone interested in the field of cyber warfare/cyberspace operations
- Anyone looking to expand a cyber security career
- Military commanders
- Information operations officers
- Information security/assurance professionals
- Cyber security consultants

- Cyber planners
- Military members (J2, J3, J5, J6, J9)
- Security analysts
- Network security engineers
- Penetration testers
- Auditors
- Government officials
- Security engineers
- Threat hunters

Prerequisites

Developed exclusively for the Cyber Security Forum Initiative (CSFI) by professionals with experience in military cyberspace operations, this course is designed to help students acquire knowledge and appreciation of preserving the ability to protect data, networks, net-centric capabilities, and mission critical systems.

CSFI is highly invested in protecting American national security in cyberspace and is proud to provide cyberspace operations training to American entities, as well as foreign allies and partners in support of interoperability.

While not a prerequisite, students of this course would benefit by having a working knowledge of TCP/IP, at least one year of IT security experience, and completed the CSFI Introduction to Cyber Warfare and Operations Design (ICWOD) course.

CSFI: DEFENSIVE CYBER OPERATIONS ENGINEER (DCOE)

Course Code: 9733

CLASSROOM LIVE	$2,595 USD	3 Day

Classroom Live Outline

- **Introduction**
  - Certification Requirements
  - Commander's Intent
  - Evolution of Cyber Espionage and Collection Efforts
- **Cyberspace Operations and Cyber Mission Force**
  - Cyberspace as a Warfighting Domain
  - The Operating Environment
  - Cyberspace Militarization
  - DoD Cyber Strategy
  - Cyberspace Operations
    - NetOps, DODIN Ops
    - DCO
      - DCO-IDM
      - DCO-RA
  - OCO
  - CMF Construct – CPT, NMT, CMT
  - CPT Methodology (Survey, Secure, Protect)
- **Cyber Kill Chain**
  - Steps of the Cyber Kill Chain
  - Stages of an Attack
  - Case Study: Data Breach and Lessons Learned
  - Threat Intelligence Sharing
- **Kali Linux**
  - Cyber Tradecraft
  - Installation
  - Command Line Tasks
  - Navigating Kali

- **Reconnaissance (Passive and Active)**
  - CIA's MICE Motivational Framework
  - Open Source Intelligence (OSINT) – Common Tools
  - Information Sources
  - Case Study: Social Media Experiment
  - Reconnaissance with Kali Linux
  - Network Scanning
  - SQL Mapping
- **PBED for Cyberspace Operations**
  - PBED Framework
  - Plan – ME3C-(PC)2 Model
  - Brief
  - Execute
  - Debrief
  - PBED Exercise
- **Attack Across Networks and Systems**
  - Web Application Vulnerabilities
  - Cross-Site Scripting (XSS)
  - SQL Injection (SQLi)
  - Webshell
  - Wireless Threats
  - Network Exploitation
  - Conducting Attacks with Metasploit
  - Password Cracking
- **Persistent, Integrated Operations**
  - Command and Control (C2): Maintaining Access
  - Rootkits
  - Tunneling
  - Remote Access
  - Elevated Privileges
  - Covert Channels
  - Covering Tracks: Hiding Evidence
  - Altering Logs and History Files
  - Hidden Files
  - Timestamps
- **Network Protection**
  - Network Traffic Analysis
  - Vulnerability Scanning
  - Intrusion Detection System (IDS) and Intrusion Protection System (IPS)

Classroom Live Labs

- Lab 01: Navigating Kali Linux
- Lab 02: Network Mapping
- Lab 03: Python Scripting: Scanning and Brute Force

- Lab 04: PBED Exercise
- Lab 05: Cracking Wireless
- Lab 06: Metasploit 1
- Lab 07: Metasploit 2
- Lab 08: Metasploit 3
- Lab 09: EternalBlue (Shadow Brokers)
- Lab 10: SQL Injection
- Lab 11: Password Cracking
- Lab 12: Data Exfiltration
- Lab 13: Kernel Rootkit
- Lab 14: Packet Capture and Analysis
- Lab 15: IDS Deployment, Alert Analysis, and Reporting
- Bonus Lab: Vulnerability Scanning
- Bonus Lab: OSINT and Malware Analysis: Syrian Electronic Army (SEA)
- Bonus Lab: Whispergate Malware Analysis - Destructive Malware Targeting Ukrainian Organizations and Government
- CAPSTONE: Capture-the-Flag (CTF)

CSFI: DEFENSIVE CYBER OPERATIONS ENGINEER (DCOE)

Course Code: 9733

VIRTUAL CLASSROOM LIVE	$2,595 USD	3 Day

Virtual Classroom Live Outline

- **Introduction**
  - Certification Requirements
  - Commander's Intent
  - Evolution of Cyber Espionage and Collection Efforts
- **Cyberspace Operations and Cyber Mission Force**
  - Cyberspace as a Warfighting Domain
  - The Operating Environment
  - Cyberspace Militarization
  - DoD Cyber Strategy
  - Cyberspace Operations
    - NetOps, DODIN Ops
    - DCO
      - DCO-IDM
      - DCO-RA
  - OCO
  - CMF Construct – CPT, NMT, CMT
  - CPT Methodology (Survey, Secure, Protect)
- **Cyber Kill Chain**
  - Steps of the Cyber Kill Chain
  - Stages of an Attack
  - Case Study: Data Breach and Lessons Learned
  - Threat Intelligence Sharing
- **Kali Linux**
  - Cyber Tradecraft
  - Installation
  - Command Line Tasks
  - Navigating Kali

- **Reconnaissance (Passive and Active)**
  - CIA's MICE Motivational Framework
  - Open Source Intelligence (OSINT) – Common Tools
  - Information Sources
  - Case Study: Social Media Experiment
  - Reconnaissance with Kali Linux
  - Network Scanning
  - SQL Mapping
- **PBED for Cyberspace Operations**
  - PBED Framework
  - Plan – ME3C-(PC)2 Model
  - Brief
  - Execute
  - Debrief
  - PBED Exercise
- **Attack Across Networks and Systems**
  - Web Application Vulnerabilities
  - Cross-Site Scripting (XSS)
  - SQL Injection (SQLi)
  - Webshell
  - Wireless Threats
  - Network Exploitation
  - Conducting Attacks with Metasploit
  - Password Cracking
- **Persistent, Integrated Operations**
  - Command and Control (C2): Maintaining Access
  - Rootkits
  - Tunneling
  - Remote Access
  - Elevated Privileges
  - Covert Channels
  - Covering Tracks: Hiding Evidence
  - Altering Logs and History Files
  - Hidden Files
  - Timestamps
- **Network Protection**
  - Network Traffic Analysis
  - Vulnerability Scanning
  - Intrusion Detection System (IDS) and Intrusion Protection System (IPS)

Virtual Classroom Live Labs

- Lab 01: Navigating Kali Linux
- Lab 02: Network Mapping
- Lab 03: Python Scripting: Scanning and Brute Force

- Lab 04: PBED Exercise
- Lab 05: Cracking Wireless
- Lab 06: Metasploit 1
- Lab 07: Metasploit 2
- Lab 08: Metasploit 3
- Lab 09: EternalBlue (Shadow Brokers)
- Lab 10: SQL Injection
- Lab 11: Password Cracking
- Lab 12: Data Exfiltration
- Lab 13: Kernel Rootkit
- Lab 14: Packet Capture and Analysis
- Lab 15: IDS Deployment, Alert Analysis, and Reporting
- Bonus Lab: Vulnerability Scanning
- Bonus Lab: OSINT and Malware Analysis: Syrian Electronic Army (SEA)
- Bonus Lab: Whispergate Malware Analysis - Destructive Malware Targeting Ukrainian Organizations and Government
- CAPSTONE: Capture-the-Flag (CTF)

CSFI: DEFENSIVE CYBER OPERATIONS ENGINEER (DCOE)

Course Code: 9733

PRIVATE GROUP TRAINING	3 Day

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 4/19/2025 11:18:37 AM