CYBEREYE™
The Science of Security
BY
US-COUNCIL

CYBEREYE
Cybersecurity Professional

The CYBEREYE Cybersecurity Professional certificate course is geared towards creating the absolute cybersecurity expert, equally at ease in providing security for futuristic networks and legacy systems.

The CYBEREYE Cybersecurity Professional course provides comprehensive training in all aspects of cyber defense methodologies. This course covers the proactive defense mechanisms required of a cybersecurity professional including ethical hacking, firewalls, IPS, vulnerability assessment and cryptography. Vital cybersecurity reactive techniques are also discussed including SIEM, mobile and digital forensics, log analysis and patch management. This course consists of three modules viz

1. Security Risk Assessment (Ethical Hacking)
2. Proactive Defense and Countermeasures
3. SIEM & Incident Response

A thorough understanding of the underlying principles of networking and operating systems is a prerequisite to pursuing this advanced course. The student is expected to be knowledgeable in IP networks, TCP / IP stack, protocols like http, https, ICMP, ARP, services like DNS, DHCP, LDAP, telnet, ssh as well as routing protocols like RIP, EIGRP, BGP, etc. Expertise in Linux and Windows servers and related technologies is a must.

Key Topics:

- Vulnerability Assessment
- Security Risk Assessment
- Dos and DDos Attacks
- Attack Mitigation Techniques
- Firewalls, IDS, IPS
- Cryptography
- Incident Response and Management
- Log Analysis

CYBEREYE
Cybersecurity Professional

CYBEREYE™ The Science of Security BY US-COUNCIL

Module 1: Security Risk Assessment

- Introduction to Ethical Hacking
  - What is Hacking
  - Skills of a hacker
  - Types of Hackers
  - Network Security Challenges
  - What is Ethical Hacking
- Information Security
- Information Assurance
- Elements of Information Assurance
- Stages of Hacking
- Vulnerability Based Hacking
  - Footprinting
    - What is Footprinting
    - Footprinting Techniques
  - Scanning
    - What is Scanning
    - What is Enumeration
    - Scanning methodology
    - Continuous Automated Red Teaming (CART)
    - AI Fuzzing
    - Vulnerability Assessment
    - Penetration Testing
- Hacking Web Applications
  - What is a Web Application
  - Web Application Attacks
    - Code Injection
    - Web site defacement
    - SQL Injetion
    - XSS
- Cryptography
  - What is Cryptography
  - Types of Cryptography
  - Cryptographic Hash
- Password Hacking Attacks
  - Password guessing
  - Shoulder Surfing
  - Social Engineering
  - System hacking
  - Bruteforce attack
  - Dictionary attack
  - Rainbow tables
- Sniffers
  - What is a sniffer
  - How does a sniffer function
  - Sniffing techniques
- Phishing
  - What is Phishing
  - Phishing techniques
  - Spear Phishing
  - Whaling
  - Pharming
  - Vishing
- Wireless Hacking
  - What is a Wireless Network
  - Types of Wireless Networks
  - Different WiFi standards
  - WiFi attacks
- Malware
  - What is Malware
  - Types of Malware
  - Privilege Escalation
  - Unauthorized Application Execution
- IoT Attacks
  - What is IoT
  - IoT communication methods
  - IoT communication protocols
  - IoT Operating Systems
  - Security Challenges in IoT
  - IoT Attacks
- Cloud Computing
  - What is Cloud Computing
  - Types of Cloud Computing
  - Cloud Computing Services
  - Cloud Computing Attacks
- Blockchain Attacks
  - What is Blockchain
  - Blockchain Attacks

- Denial of Service (DoS)
  - What is DoS
  - What is DDoS
  - Botnets
  - DoS/ DDoS attack techniques
- Anonymizers
  - What is an anonymizer
  - Why are anonymizers used
  - Types of anonymizers
    - Proxy
    - VPN Proxy
    - TOR Browser
- DarkWeb
  - What is DarkWeb
  - Different DarkWeb technologies
    - Freenet
    - I2P
    - TOR
- Covering Tracks
  - How hackers cover their tracks
- Cyber Kill Chain
- Securing the Network
  - Hardware encryption
  - Software encryption
  - PKI
- Introduction to MITRE ATT&CK Framework
- Introduction to Security Compliance Standards
- Cyber Resilience
- Cyber Fusion Center

Module 2: Proactive Defense and Countermeasures

- Network Security
  - Introduction to Security
  - Network Security Challenges
  - Elements of Information Security
  - Network Security Devices
  - The Castle Moat approach
  - Zero Trust approach
- Firewalls
  - What is a Firewall
  - Different Firewall technologies
    - Packet Filtering Firewall
    - Application Gateway
    - Stateful Firewall
  - Designing Security with Firewall
  - NAT
  - Security Policy
  - Content Management
  - User Identity Management
  - Logging
  - Reporting
- Intrusion Prevention System (IPS)
  - What is Intrusion Prevention System
  - Difference between Intrusion Prevention System & Intrusion Detection System
  - Configuring Intrusion Prevention System
- Virtual Private Network (VPN)
  - What is a VPN
  - Types of VPNs
    - GRE
    - IPSec
    - SSL
- High Availability
- Cloud Firewalls

Module3: SIEM & Incident Response

- SIEM
  - What is SIEM
- Incident Response
  - What is Incident Response