CENTER for APPRENTICESHIP & ADULT TRAINING
520 Butler Farm Rd, Hampton VA 23666
757-766-1101
www.nhrec.org/cfaat

Course Name: Cybersecurity Security+

Contact Hours: 144

Number of Sessions: 48

Number of Hrs./Session: 3

Mode of Instruction: Classroom

Course Description:
The Cybersecurity Security+ program reviews baseline skills related to core security functions for students to pursue a career in the IT security sector. Most employers will require security clearance to secure employment. Upon successfully completing this program students will take the NOCTI exam in Cybersecurity Fundamentals. The tuition includes the NOCTI exam, textbooks, and materials used in class. This course covers topics on the CompTIA Security+ certification exam and students may register to take this exam separately once the course is complete.

Texts: CompTIA Security+ Guide to Network Security Fundamentals, 7th Ed. (Ciampa)

Course Outline:

1. Module 1. Introduction to Security
    a. What Is Information Security?
    b. Understanding Security
    c. Defining Information Security
    d. Who Are the Threat Actors?
    e. Script Kiddies
    f. Hacktivists
    g. State Actors
    h. Insiders
    i. Other Threat Actors
    j. Vulnerabilities and Attacks
    k. Vulnerabilities
    l. Attack Vectors
    m. Social Engineering Attacks
    n. Impacts of Attacks
2. Module 2. Threat Management and Cybersecurity Resources
    a. Penetration Testing
    b. Defining Penetration Testing
    c. Why Conduct a Test?
    d. Who Should Perform the Test?
    e. Rules of Engagement

   f. Performing a Penetration Test
   g. Vulnerability Scanning
   h. What Is a Vulnerability Scan?
   i. Conducting a Vulnerability Scan
   j. Data Management Tools
   k. Threat Hunting
   l. Cybersecurity Resources
   m. Frameworks
   n. Regulations
   o. Legislation
   p. Standards
   q. Benchmarks/Secure Configuration Guides
   r. Information Sources
3. Module 3. Threats and Attacks on Endpoints
   a. Attacks Using Malware
   b. Imprison
   c. Launch
   d. Snoop
   e. Deceive
   f. Evade
   g. Application Attacks
   h. Scripting
   i. Injection
   j. Request Forgery
   k. Replay
   l. Attacks on Software
   m. Adversarial Artificial Intelligence Attacks
   n. What Are Artificial Intelligence (AI) and Machine Learning (ML)?
   o. Uses in Cybersecurity
   p. Risks in Using AI and ML in Cybersecurity
4. Module 4. Endpoint and Application Development Security
   a. Threat Intelligence Sources
   b. Categories of Sources
   c. Sources of Threat Intelligence
   d. Securing Endpoint Computers
   e. Confirm Boot Integrity

   f. Protect Endpoints
   g. Harden Endpoints
   h. Creating and Deploying SecDevOps
   i. Application Development Concepts
   j. Secure Coding Techniques
   k. Code Testing
5. Module 5. Mobile, Embedded, and Specialized Device Security
   a. Securing Mobile Devices
   b. Introduction to Mobile Devices
   c. Mobile Device Risks
   d. Protecting Mobile Devices
   e. Embedded Systems and Specialized Devices
   f. Types of Devices
   g. Security Issues
6. Module 6. Basic Cryptography
   a. Defining Cryptography
   b. What Is Cryptography?
   c. Cryptography Use Cases
   d. Limitations of Cryptography
   e. Cryptographic Algorithms
   f. Hash Algorithms
   g. Symmetric Cryptographic Algorithms
   h. Asymmetric Cryptographic Algorithms
   i. Cryptographic Attacks and Defenses
   j. Attacks on Cryptography
   k. Quantum Cryptographic Defenses
   l. Using Cryptography
   m. Encryption through Software
   n. Hardware Encryption
   o. Blockchain
7. Module 7. Public Key Infrastructure and Cryptographic Protocols
   a. Digital Certificates
   b. Defining Digital Certificates
   c. Managing Digital Certificates
   d. Types of Digital Certificates
   e. Public Key Infrastructure (PKI)

   f. What Is Public Key Infrastructure (PKI)?
   g. Trust Models
   h. Managing PKI
   i. Key Management
   j. Cryptographic Protocols
   k. Secure Sockets Layer (SSL)
   l. Transport Layer Security (TLS)
   m. Secure Shell (SSH)
   n. Hypertext Transport Protocol Secure (HTTPS)
   o. Secure/Multipurpose Internet Mail Extensions (S/MIME)
   p. Secure Real-time Transport Protocol (SRTP)
   q. IP Security (IPsec)
   r. Weaknesses of Cryptographic Protocols
   s. Implementing Cryptography
   t. Key Strength
   u. Secret Algorithms
   v. Block Cipher Modes of Operation
   w. Crypto Service Providers
8. Module 8. Networking Threats, Assessments, and Defenses
   a. Attacks on Networks
   b. Interception Attacks
   c. Layer 2 Attacks
   d. DNS Attacks
   e. Distributed Denial of Service Attack
   f. Malicious Coding and Scripting Attacks
   g. Tools for Assessment and Defense
   h. Network Reconnaissance and Discovery Tools
   i. Linux File Manipulation Tools
   j. Scripting Tools
   k. Packet Capture and Replay Tools
   l. Physical Security Controls
   m. External Perimeter Defenses
   n. Internal Physical Security Controls
   o. Computer Hardware Security
9. Module 9. Network Security Appliances and Technologies
   a. Security Appliances

   b. Firewalls
   c. Proxy Servers
   d. Deception Instruments
   e. Intrusion Detection and Prevention Systems
   f. Network Hardware Security Modules
   g. Configuration Management
   h. Security Technologies
   i. Access Technologies
   j. Technologies for Monitoring and Managing
   k. Design Technologies
10. Module 10. Cloud and Virtualization Security
   a. Cloud Security
   b. Introduction to Cloud Computing
   c. Securing Cloud Computing
   d. Virtualization Security
   e. Defining Virtualization
   f. Infrastructure as Code
   g. Security Concerns for Virtual Environments
   h. Secure Network Protocols
   i. Simple Network Management Protocol (SNMP)
   j. Domain Name System Security Extensions (DNSSEC)
   k. File Transfer Protocol (FTP)
   l. Lightweight Directory Access Protocol (LDAP)
   m. Internet Protocol Version 6 (IPv6)
11. Module 11. Wireless Network Security
   a. Wireless Attacks
   b. Bluetooth Attacks
   c. Near Field Communication (NFC) Attacks
   d. Radio Frequency Identification (RFID) Attacks
   e. Wireless Local Area Network Attacks
   f. Vulnerabilities of WLAN Security
   g. Wired Equivalent Privacy
   h. Wi-Fi Protected Setup
   i. MAC Address Filtering
   j. Wi-Fi Protected Access (WPA)
   k. Wireless Security Solutions

   l. Wi-Fi Protected Access 2 (WPA2)
   m. Wi-Fi Protected Access 3 (WPA3)
   n. Additional Wireless Security Protections
   o. Installation
   p. Configuration
   q. Specialized Systems Communications

12. Module 12. Authentication
   a. Types of Authentication Credentials
   b. Something You Know: Passwords
   c. Something You Have: Smartphone and Security Keys
   d. Something You Are: Biometrics
   e. Something You Do: Behavioral Biometrics
   f. Authentication Solutions
   g. Password Security
   h. Secure Authentication Technologies
13. Module 13. Incident Preparation, Response, and Investigation
   a. Incident Preparation
   b. Reasons for Cybersecurity Incidents
   c. Preparing for an Incident
   d. Incident Response
   e. Use SOAR Runbooks and Playbooks
   f. Perform Containment
   g. Make Configuration Changes
   h. Incident Investigation
   i. Data Sources
   j. Digital Forensics
14. Module 14. Cybersecurity Resilience
   a. Business Continuity
   b. Introduction to Business Continuity
   c. Resilience through Redundancy
   d. Policies
   e. Definition of a Policy
   f. Types of Security Policies
15. Module 15. Risk Management and Data Privacy
   a. Managing Risk
   b. Defining Risk

c. Risk Types
d. Risk Analysis
e. Risk Management
f. Data Privacy
g. User Concerns
h. Data Breach Consequences
i. Data Types
j. Protecting Data
k. Data Destruction

16. Final and NOCTI Exam
17. Preparing for the CompTIA Security+ Exam