KOENIG
step forward

AUTHORIZED
LEARNING
CENTER
cwnp))

Certified Wireless Network Expert (CWNE)

Need to attend below courses:

Enterprise Wi-Fi Security (CWSP)

Certified Wireless Design Professional (CWDP)

Enterprise Wi-Fi Analysis & Troubleshooting (CWAP)

Enterprise Wi-Fi Security (CWSP)
Course outline –

Module 1 – Security Fundamentals

- Security Basics
- CWNA Security Review
- Industry Organizations
- Terminology
- Wireless Vulnerabilities

Module 2 – Wireless Security Challenges

- Network Discovery
- Pseudo-Security
- Legacy Security Mechanisms
- Network Attacks
- Recommended Practices

Module 3 – Security Policy

- Defining Security Policies
- Policy Enforcement

- Policy Management
- Policy Types

Module 4 – Understanding Authentication

- Passphrase Authentication
- AAA
- RBAC
- RADIUS
- 802.1X
- EAP

Module 5 – Authentication and Key Management

- Robust Security Networks (RSN)
- RSN Information Element
- RSN Authentication and Key Management (AKM)

Module 6 – Encryption

- Encryption Fundamentals
- Encryption Algorithms
- WEP
- TKIP
- CCMP

Module 7 – Security Design Scenarios

- Virtual Private Networks (VPN)
- Remote Networking
- Guest Access Networks

Module 8 – Secure Roaming

- Roaming Basics and Terminology
- Preauthentication
- PMK Caching
- Opportunistic Key Caching (OKC)
- 802.11r FT
- Proprietary Roaming
- Voice-Enterprise

Module 9 – Network Monitoring

- Wireless Intrusion Prevention Systems (WIPS)
- WIPS Deployment Models
- WIPS Policy
- Threat Mitigation
- Location Services
- WNMS
- Protocol Analysis
- Spectrum Analysis

Certified Wireless Design Professional (CWDP)

Course outline –

WLAN Design Overview:
- Importance of good design
- Impact of bad design
- Design process
- Design skills
- Design toolkit
- Pre-planning

- Customer interaction
- Requirements gathering
- Discovering existing systems
- Documenting the environment
- Defining constraints
- Creating documentation
- Client device types
- Application types
- Application-specific design
- High density design issues
- Standard corporate networks
- **Industry-specific designs**
  - Government
  - Healthcare
  - Hospitality
  - Education
  - Retail
  - Public hotspots
  - Transportation
  - Mobile offices
  - Outdoor and mesh
  - Remote networks and branch offices
  - Last-mile/ISP and bridging
  - Defining vendor issues
  - Operational planes
  - Design models
  - Understanding architecture differences
  - RF spectrum
  - RF behaviors
  - Modulation and coding schemes
  - RF accessories
  - Throughput factors
  - Antennas

- 802.11n and antennas
- Choosing APs
- Powering APs
- Site survey tools
- Site survey preparation
- Predictive site surveys
- Manual site surveys
- Site survey principles and processes
- Quality of Service (QoS) overview
- QoS application points
- Roaming support
- Bad security
- Authentication solutions
- Encryption solutions
- Security best practices
- Intrusion prevention
- Network health status
- Troubleshooting and validation process
- Troubleshooting and validation tools
- Common problems

- Requirements Analysis
- Designing for Clients and Applications
- Designing for IndustryVendor
- Selection Processes
- Radio Frequency Planning
- WLAN Hardware Selection
- Site Surveys
- Designing for QoS
- Designing for Security
- Installation Testing, Validation and Troubleshooting
- Design Troubleshooting

Enterprise Wi-Fi Analysis & Troubleshooting (CWAP)

Course outline –

Principles of WLAN Communication

- 802.11 Working Group
- OSI reference model and the 802.11 PHY and MAC
- Communication sublayers and data units
- WLAN architecture components
- Organization of station forwarding
- Addressing and internetworking operation
- Modern WLAN product architectures

Physical (PHY) and MAC Layer Formats and Technologies

- Physical layer functions
- Preamble function and format
- Header purpose and structure
- Analysis of PHY problems
- Physical PPDU formats
  - 802.11b
  - 802.11a
  - 802.11g
  - 802.11n
- MAC frame components
- MAC encapsulation
- Fields and subfields of the MAC header
- Frame Control
- Frame types and subtypes and their uses
- Addressing
- Frame body
- Data frame format
- Control frame format

- Management frame format
- Information elements and fields

Protocol Operation

- Beaconing and synchronization
- Scanning
- Client state machine
- 802.11 contention
- QoS
- Admission control
- Band steering and airtime fairness mechanisms
- Fragmentation
- Acknowledgments and Block acknowledgments
- Protection mechanisms and backward compatibility
- Power management
- Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC)
- Security components, methods, and exchanges
- Roaming procedures exchanges
- Future protocol enhancements

802.11n

- Transmit beamforming
- Spatial multiplexing
- Maximal Ratio Combining (MRC)
- Space-Time Block Coding
- 40 MHz channels
- Frame aggregation
- HT-OFDM format
- Modulation and Coding Schemes (MCS)
- HT frame formatting
- And More

Protocol Analysis Tools and Methodology

- Troubleshooting methodology
- Protocol analyzer types
- Analysis NIC/adapter selection and constraints
- Interpreting results based on location
- Analyzer settings and features
- Filtering and channel scanning
- Interpreting decodes
- Using advanced analysis features
- Assessing WLAN health and behavior factors
- Evaluating network statistics
- Troubleshooting common problems
- Wired analysis to support wireless network issues

Spectrum Analysis Tools and Methodology

- Radio frequency behavior review
- Visualizing RF domains using spectrum measurement tools
- Spectrum analyzer types and operation
- Analyzer specifications and characteristics
- Understanding spectrum data presentation
- Interpreting plots and charts
- Common WLAN spectrum analyzer features
- Identifying transmit patterns
- Device classification and network impact
- Recognizing transmit signatures