digital Point IT Consulting Training IT Infrastructure Support Cloud Migration

http://training.digitalpoint.tech

Cyber Security and Risk Management Specialist

Training Methodology

- Digital point is a global classroom. All classes are featured online (No recorded version). Students around world can join this online live class
- Each class is instructor oriented live class and will be recorded, and students will get access to watch video for practice.
- Real-world scenario labs.
- VPN access to digital Point's Lab that is accessible from anywhere 24/7
- Class Notes and Labs for each class

Contact Us

Phone: 1-703-652-9640 | 226-972-1877

Web: http://training.digitalpoint.tech Email: admin@digitalpoint.tech

Cyber Security Market Scope:

Cybersecurity jobs are in high demand. According to the Bureau of Labor Statistics, the rate of growth for jobs in information security is projected at 37% from 2012–2022 that's much faster than the average for all other occupations. Obtaining work in this industry can mean a great income, job security, and advancement potential. There are many business opportunities, including company management positions, available for professional hackers in today's workforce.

The Highest-Paid Cybersecurity Jobs:

- **Application Security Engineer:** This cybersecurity role tops the list with an average salary range that falls between $100,000 to $210,000, according to Salary Outlook guide.
- **Network Security Analyst:** Another of the highest-paid cybersecurity jobs, Network Security Analysts make on average between $90,000 and $150,000.
- **Cybersecurity Analyst:** The average annual salary for this cybersecurity title falls between $90,000 and $185,000.
- **Penetration Tester:** The Penetration Tester role nets an average salary between $80,000 and $130,000.
- **IS Security Engineer:** This role nets an average salary range of $90,000 to $150,000.

Benefit of the Course:

>> **Better Job Opportunities:** If you are looking for a new job, completion of this course, you can apply as a Cyber Security Specialist/Engineer/ IS Security Engineer/Security Analyst
>> **Improved Skills & Knowledge:** If you are already a QA/IT professional, completion of this course will improve your skills to latest technologies.
>> **Increased Salary:** Cyber Security professionals are the highest paid in the IT industry.

Prerequisites:

1. A bachelor degree in any background
2. You must have good presentation skills

digital Point IT Consulting Training IT Infrastructure Support Cloud Migration

http://training.digitalpoint.tech

Course Duration (4 months, every Sat and Sun)

Class Schedule: **SAT & SUN 9:00 AM - 2:00 PM EST**
MON & WED 6:00 PM - 10:00 PM EST
TUE & THU 6:00 PM - 10:00 PM EST

Training Methodology:

- Real-world scenario labs.
- One dedicated Server for each student that is accessible from anywhere 24/7
- Class Notes and Labs for each class
- Each class is instructor oriented live class and will be recorded, and students will get access to watch video for practice.

Why choose us?

- Digital point is a global classroom. All classes are featured online (No recorded version). Students around world can join this online live class.
- The course is very interactive and has lots of lab practice with it. A remote server will provided to each student for lab practice.
- We help you with Resume preparation, Interview preparation, before and after job support
- Student can repeat the same program two times with no extra cost.

Course Curriculum

Phase 1: Foundation Training

Module 1 Overview of enterprise applications and N-Tier Infrastructure
Module 2 Operating System –Windows Server 2012/2016, UNIX
Module 3 Networking, Active Directory and DNS
Module 4 Power Shell Scripting, Batch Scripting
Module 5 Incident, Problem and Change Management process

Module 6 Infrastructure setup

- Installation of Virtual Machine on Physical Server
- Installation of Virtual Machine on Cloud

- Configure VPN
- Connect Remote Windows Servers
- Connect Remote Unix Server

Phase 2: Security Management

Module 7

- **Identifying Security Fundamentals**
  - Identify Information Security Concepts
  - Identify Basic Security Controls
  - Identify Basic Authentication and Authorization Concepts
  - Identify Basic Cryptography Concepts

Module 8

- **Analyzing Risk**
  - Analyze Organizational Risk
  - Analyze the Business Impact of Risk

Module 9

- **Identifying Security Threats**
  - Identify Social Engineering Attacks
  - Identify Malware
  - Identify Software-Based Threats
  - Identify Network-Based Threats
  - Identify Wireless Threats
  - Identify Physical Threats

Module 10

- **Conducting Security Assessments**
  - Identify Vulnerabilities
  - Assess Vulnerabilities
  - Plan for remediation of findings

Module 11

- **Implementing Host and Software Security**
  - Implement Host Security
  - Implement Cloud and Virtualization Security
  - Implement Mobile Device Security
  - Incorporate Security in the Software Development Lifecycle

Module 12

- **Implementing Network Security**
  - Configure Network Security Technologies
  - Secure Network Design Elements
  - Implement Secure Networking Protocols and Services
  - Secure Wireless Traffic

Module 13

- **Managing Identity and Access**
  - Implement Identity and Access Management
  - Configure Directory Services
  - Configure Access Services
  - Manage Accounts

Module 14

- **Implementing Cryptography**
  - Identify Advanced Cryptography Concepts
  - Select Cryptographic Algorithms
  - Configure a Public Key Infrastructure
  - Enroll Certificates
  - Back Up and Restore Certificates and Private Keys
  - Revoke Certificates

Module 15

- **Implementing Operational Security**
  - Evaluate Security Frameworks and Guidelines
  - Incorporate Documentation in Operational Security
  - Implement Security Strategies
  - Manage Data Security Processes
  - Implement Physical Controls

Module 16

- **Addressing Security Incidents**
  - Troubleshoot Common Security Issues
  - Respond to Security Incidents

- Investigate Security Incidents

Module 17

- **Ensuring Business Continuity**
  - Select Business Continuity and Disaster Recovery Processes
  - Develop a Business Continuity Plan

Module 18

- **Network Penetration Test**
  - Plan for Network Penetration Testing
  - External Network Penetration Testing
  - Internal Network Penetration Testing
  - Wireless Network Penetration Testing
  - Generate Report for Network Penetration Testing

Module 19

- **Application Penetration Test**
  - Plan for application Penetration Testing
  - External Application Penetration Testing
  - Internal Application Penetration Testing
  - Generate Report for Application Penetration Testing

Module 20

- **DDoS**
  - Overview of DDoS
  - How to onboard an application under DDoS
  - Monitoring Application under DDoS

Module 21

- **Web Application Firewall (WAF)**
  - Overview of WAF
  - How to onboard an application under WAF
  - Monitoring Application under WAF
  - WAF Blocking mode vs alert mode

Module 22

- **Policies, Standards, Guideline**
  - Overview of Policies ,Standards and Guidelines
  - ISO format
  - Application Security policy ,standards
  - Network Security policy, standards

Phase 3: Real-World Project

Module 23 Boot Camp

- Boot Camp with real-world project - Each student will be required to complete a real-time project lab that covers the entire course curriculum.

Phase 4: Job Marketing

Module 24 Real-world Job Interview Preparation

- Professional real-world Resume Writing
- Project Analysis
- Interview Preparation
- Mock Interview

LABS

- **Information Gathering**
  - Network information gathering
  - Application and domain information gathering
- **Identifying Security Threats**
  - Identify Social Engineering Attacks
  - Identify Malware
  - Identify Software-Based Threats
  - Identify Network-Based Threats
  - Identify Wireless Threats
  - Identify Physical Threats
- **Conducting Security Assessments**
  - Identify Vulnerabilities

- Assess Vulnerabilities
- Plan for remediation of findings

- **Vulnerability Scanning**
  - Vulnerability Scanning Overview and Considerations 206
  - How Vulnerability Scanners Work
  - Manual vs. Automated Scanning
  - Internet scanning vs Internal Scanning
  - Authenticated vs Unauthenticated Scanning
  - Vulnerability Scanning with Nessus
  - Authenticated Scanning With Nessus
  - Vulnerability Scanning with Nmap

- **Web Application Attacks**
  - Web Application Assessment Methodology
  - Web Application Enumeration
  - Inspecting URLs
  - Inspecting Page Content
  - Viewing Response Headers
  - Inspecting Sitemaps
  - Locating Administration Consoles
  - Web Application Assessment Tools
  - DIRB
  - Burp Suite
  - Nikto
  - Exploiting Web-based Vulnerabilities
  - Exploiting Admin Consoles
  - Cross-Site Scripting (XSS)
  - Directory Traversal Vulnerabilities
  - File Inclusion Vulnerabilities
  - SQL Injection

- **Password Attacks**
  - Wordlists
  - Standard Wordlists
  - Brute Force Wordlists
  - Common Network Service Attack Methods
  - HTTP htaccess Attack with Medusa
  - Remote Desktop Protocol Attack with Crowbar
  - SSH Attack with THC-Hydra
  - HTTP POST Attack with THC-Hydra
  - Leveraging Password Hashes

- Retrieving Password Hashes
- Passing the Hash in Windows
- Password Cracking

- **Active Directory Attacks**
  - Active Directory Theory
  - Active Directory Enumeration
  - Active Directory Authentication
  - NTLM Authentication
  - Kerberos Authentication
  - Cached Credential Storage and Retrieval
  - Service Account Attacks
  - Low and Slow Password Guessing
  - Active Directory Lateral Movement
  - Pass the Hash
  - Overpass the Hash
  - Pass the Ticket
  - Distributed Component Object Model
  - Active Directory Persistence
  - Golden Tickets
  - Domain Controller Synchronization

- **Network Penetration Test**
  - Plan for Network Penetration Testing
  - External Network Penetration Testing
  - Internal Network Penetration Testing
  - Wireless Network Penetration Testing
  - Foot printing
  - Scanning and Enumeration
  - System Hacking
  - Malware
  - Sniffing
  - Social Engineering
  - Denial of Service
  - Session Hijacking

- **Application Penetration Test**
  - Plan for application Penetration Testing
  - External Application Penetration Testing
  - Internal Application Penetration Testing
  - Web Servers and Apps
  - SQL Injection

  - OWASP top 10

- **Network exploitation**
  - FTP Exploits
  - Man-in-the middle exploits
  - Wireless Exploits
  - Application Exploits
  - SQL Injection
  - Code Vulnerabilities
  - Local Host Vulnerabilities
  - Privileged Escalation (Unix)
  - privileged Escalation (Windows)

- **Penetration Tet Reports**
  - Network Penetration Test Report

- **Remediation**
  - Design remediation strategy