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

Cybersecurity Market Scope:

Cybersecurity jobs are in high demand. According to the US Bureau of Labor and Services, there were 163,000 Information Security Analysts in 2021, with just 300 of these self-employed. Additionally, there was an almost unheard-of 100 percent employment rate in this sector. In fact, the BLS expects demand to increase by nearly 35 percent by 2031 an additional 56,500 positions to be filled.

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 the 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.

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. Good presentation skills

Class Schedule:

Sat & Sun 9:00 AM - 12:00 PM EST

Tue & Thu 7:00 PM - 10:00 PM EST

Mon & Wed 7:00 PM - 10:00 PM EST

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.
- We help you with Resume preparation, Interview preparation, before and after job support.
- Bootcamp session for real-world project.
- 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 Applications under DDoS
  - Overview of WAF
  - How to onboard an application under WAF
  - Monitoring Application under WAF
  - WAF Blocking mode vs alert mode

Module 21

- **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 22 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 23 Real-world Job Interview Preparation

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

LABS:

Penetration Test:

- Properly plan and prepare for an enterprise penetration test.
- Perform detailed reconnaissance to aid in social engineering, phishing, and making well-informed attack decisions.
- Scan target networks using best-of-breed tools to identify systems and targets that other tools and techniques may have missed.
- Perform safe and effective password guessing to gain initial access to the target environment, or to move deeper into the network.
- Exploit target systems in multiple ways to gain access and measure real business risk.
- Execute extensive post-exploitation to move further into the network.
- Use privilege escalation techniques to elevate access on Windows or Linux systems, or the Microsoft Windows domain.
- Perform internal reconnaissance and situational awareness tasks to identify additional targets and attack paths.
- Execute lateral movement and pivoting to extend access to the organization further and identify risks missed by surface scans.
- Crack passwords using modern tools and techniques to extend or escalate access.
- Use multiple Command and Control (C2, C&C) frameworks to manage and pillage compromised hosts
- Attack the Microsoft Windows domain used by most organizations.
- Execute multiple Kerberos attacks, including Kerberoasting, Golden Ticket, and Silver Ticket attacks
- Conduct Azure reconnaissance.
- Execute Azure Active Directory (AD) password spray attacks.
- Execute commands in Azure using compromised credentials.
- Develop and deliver high-quality reports.

Risk Assessment (Governance, Risk and Compliance):

- Calculate a cybersecurity risk
- Inherent risk vs residual risk
- Compensating controls
- Risk assessment report

- Risk visualization

Develop cybersecurity standards and Technical Hardening Requirements:

- Develop Network security standard
- Develop application security standard
- Develop Windows servers hardening standards
- Develop Unix/Linux server hardening standards
  Develop database servers hardening standards