Course Curriculum

Building your IT Career

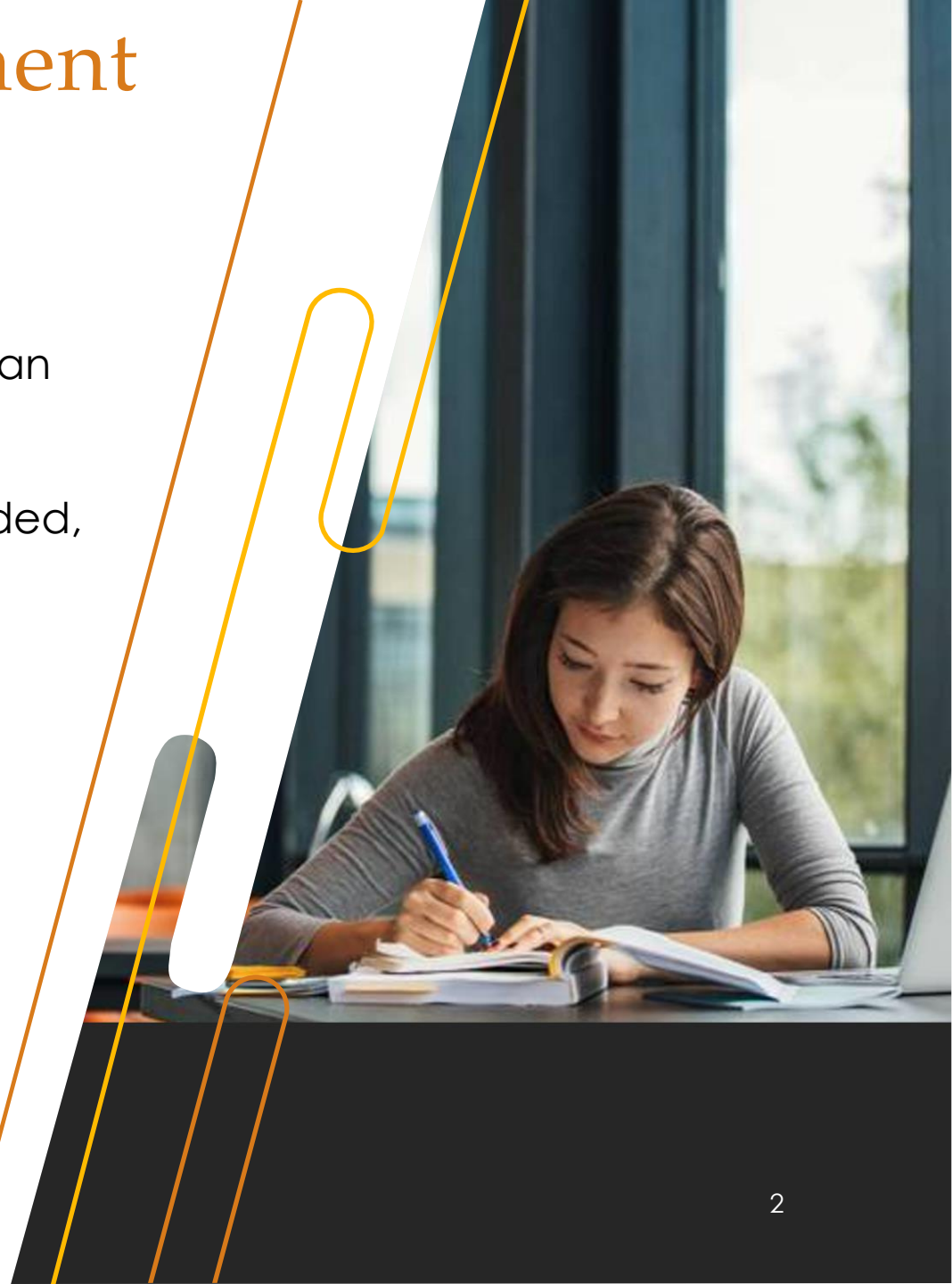
Cybersecurity and risk management

Training Methodology

- Digital Point is a global classroom. All classes are featured online (No recorded version). Students around the 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.
- Class Notes and Labs for each class

Contact Us

Phone: 1-703-652-9640 | 226-972-1877
Web: https://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 job outlook in information security is projected at 33% (2023-33), much faster than the average for all other occupations. The number of Cybersecurity jobs in 2023 was. 180,770. Obtaining work in this industry can mean a great income, job security, and advancement potential.

The Highest-Paid Cybersecurity Jobs:

- Application Security Engineer: This cybersecurity role tops the list with an average salary range that falls between $100,000 and $210,000
- Network Security Analyst: Another of the highest-paid cybersecurity jobs, Network Security Analysts make, on average, between $90,000 and $150,000.
- Cybersecurity Specialist/Analyst: The annual average wage 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.
- Security Risk Management Specialist: This role nets an average salary range of $120,000 to $220,000.

Cybersecurity and risk management

Benefits of the Course:

- Better Job Opportunities: If you are looking for a new job completing 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 IT industry.

Prerequisites:

- A bachelor's degree in any background
- You must have good presentation skills

Course Duration: (4 months, 6 hours/week)

Cybersecurity and risk management

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 the world can join this online live class.
- The course is very interactive and has lots of lab practice.
- We help you with Resume preparation, Interview preparation, and before and after job support
- Students can repeat the same program one time 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 and Unix/Linux
Module 3 Networking Fundamentals, Active Directory and DNS
Module 4 Power Shell Scripting, Batch and Shell Scripting
Module 5 Incident, Problem and Change Management Process

Module 6 Infrastructure Lab setup

- Lab setup on Laptop/desktop
  - Installation of Virtual Machine
  - Build Active Directory and Kali Linux
- Lab setup on AWS
- Lab setup on Azure

Module 7 Cybersecurity Framework and Standards

- NIST Cybersecurity Framework (CSF)
- ISO/IEC 27001
- CIS Critical Security Controls (CIS Controls)
- COBIT (Control Objectives for Information and Related Technologies)
- PCI-DSS (Payment Card Industry Data Security Standard)
- HIPAA (Health Insurance Portability and Accountability Act)
- MITRE ATT&CK Framework

Course Curriculum

Phase 2: Cybersecurity and Risk Management

Module 8: Communication and Network Security

- Assess and implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to the design
- Wireless Network Security
- Remote Access Network Security

Module 9: Identity and Access Management

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Federated identity with a third-party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle
- Implement authentication systems

Module 10: Encryption and Cryptography Management

- Principles of encryption
- Symmetric and asymmetric key management
- Data encryption at rest and in transit condition
- Encryption key management
- Common encryption algorithms

Course Curriculum

Phase 2: Cybersecurity and Risk Management

Module 11: Asset Management Security

- Assess and implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to the design
- Wireless Network Security
- Remote Access Network Security

Module 12: Identity and Access Management

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Federated identity with a third-party service
- Implement and manage authorization mechanisms
- Manage the identity and access provisioning lifecycle
- Implement authentication systems

Module 13: Encryption and Cryptography Management

- Principles of encryption
- Symmetric and asymmetric key management
- Data encryption at rest and in transit condition
- Encryption key management
- Common encryption algorithms

Course Curriculum

Phase 2: Cybersecurity and Risk Management

Module 14: Software Development Security

- Understand and integrate security in the Software Development Life Cycle (S-SDLC)
- Understand and integrate security in the DevOps Model (DevSecOps)
- Identify and apply security controls in software development ecosystems
- Assess the effectiveness of software security
- Assess the security impact of acquired software
- Define and apply secure coding guidelines and standards

Module 15: Risk Management

- Security governance principles
- Governance, Risk and Compliance (GRC)
- Security policy, standards, procedures, and guidelines
- Regulatory Laws and Compliance
- Business continuity (BC) and Disaster Recovery
- Risk Assessment, treatment and remediation, exception/exemption
- Risk Calculation
  - Risk Identification
  - Threat Identification
  - Vulnerability Identification
- Impact Analysis
- Likelihood Analysis
- Risk Mitigation
- Risk Response Strategies

Course Curriculum

Phase 2: Cybersecurity and Risk Management

Module 16: Configuration Management

- Securing and hardening Windows OS
- Securing and hardening Unix/Linux OS
- Securing and hardening Database Technologies
- Securing and hardening Windows Network and appliances
- Securing and hardening Cloud Technologies

Module 17: Security Assessment and Testing

- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data (e.g., technical and administrative)
- Analyze test output and generate the report
- Conduct or facilitate security audits.

Course Curriculum

Phase 3: Labs

Module 18: Network and Infrastructure Penetration Test

- Properly plan and prepare for an enterprise penetration test
- Scan in-scope environments using best-of-breed tools to identify systems and targets
- Understand the environment via efficient methods of gaining situation awareness to identify additional targets and attack paths
- Use privilege escalation techniques to elevate access on Windows or Linux systems or Active Directory itself
- Crack passwords using modern tools and techniques to extend or escalate access
- Use Command and Control (C2, C&C) frameworks to manage and manage compromised hosts remotely
- Attack the Active Directory domains and forests used by most organizations
- Execute multiple Kerberos attacks, including Kerberoasting, Golden Ticket, and Silver Ticket attacks
- Execute Entra ID password spray attacks
- Execute commands in Azure using compromised credentials
- Develop and deliver high-quality reports that communicate the accurate business risk stemming from the discovered flaws and misconfiguration

Module 19: Application Penetration Test

- Apply OWASP's methodology to web application penetration tests to ensure they are consistent, reproducible, rigorous, and under quality control.
- Install and Configure Burp suite.
  - Brute-force
  - Command injection
  - Cross-Site Request Forgery (CSRF)
  - File Inclusion
  - File upload
  - Insecure CAPTCHA
  - SQL injection

Course Curriculum

Phase 4: Real-World project

Module 20: 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 5: Real-World project

Module 21: Real-world Job Interview Preparation

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

Thank you

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

Web: https://training.digitalpoint.tech

Email: admin@digitalpoint.tech