Ramasser Group

+1 (316) 882-7967

www.ramassergroup.com

ramasser.consulting@ramassergroup.com

CYBERSECURITY TRAINING COURSE OUTLINE

Course Duration: 3 Days (8 hours per day)

Day 1: Understanding Cybersecurity Fundamentals

Morning Session (2 hours)

Introduction to Cybersecurity
- Welcome and Introduction
- Definition of Cybersecurity
- Importance of Cybersecurity
- Why Cybersecurity Matters

Cyber Threat Landscape
- Understanding the Cyber Threat Landscape
- Various Types of Threats
- The Impact of Cyber Threats

Security Principles and Best Practices
- The CIA Triad: Confidentiality, Integrity, and Availability
- Defense in Depth
- Importance of Security Policies and Procedures

Practical Session (2 hours)

Practical Session - Setting up a Secure Environment
- Hands-On: Installing and Configuring a Virtual Machine
- Basic Security Configurations
- Introduction to Firewalls and Access Controls

Lunch Break (1 hour) ……

Afternoon Session (3 hours)

Types of Cyber Attacks
- Malware: What Is It and How Does It Work?
- Phishing: Recognizing and Avoiding Phishing Attacks
- Ransomware: Understanding and Defending Against It

Types of Cyber Attacks (Continued)
- Social Engineering: Manipulating the Human Factor
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks
- Intrusion and Data Breaches

Protecting Against Cyber Threats

- Using Antivirus Software and Anti-Malware Tools
- Email and Web Security Best Practices
- The Importance of User Awareness and Training
- SOC and SIEM

Homework Assignment Explanation
- Research on Recent Cyber Attacks

Online Quiz for Day 1

Day 2: Security Operations, Cryptography Vulnerabilities Management

Morning Session (2 hours)

Network and application Security Basics
- Introduction to Network Security
- Common Network Vulnerabilities
- Securing Wireless Networks
- Application Security

Cryptography Fundamentals
- Understanding Encryption and Decryption
- Symmetric vs. Asymmetric Cryptography
- Public and Private Keys Explained

Threats, Vulnerabilities & Mitigations
- Introduction to TVM
- Tools to perform Vulnerability Scanning
- Reporting and communicating to the Business
- Penetration Testing.

Practical Session - Setting Up a Secure Network
- Hands-On: Configuring a Secure Wi-Fi Network
- Implementing VPN for Secure Communication
- Introduction to Network Monitoring Tools

Lunch Break (1 hour) ……

Afternoon Session (3 hours)

Firewalls and Intrusion Detection Systems (IDS)
- Types of Firewalls: Stateful, Stateless, Application Layer
- Intrusion Detection vs. Intrusion Prevention Systems
- Configuring Firewalls and IDS

Secure Communication and Data Protection

- Exploring Secure Socket Layer (SSL) and Transport Layer Security (TLS)
- Data Encryption in Practice: When and How to Use It
- Secure File Transfer Protocols
- Principle of Secure Development.
-

Homework Assignment Explanation
- Creating a Secure Home Network Diagram

Online Quiz for Day 2

Day 3: GRC, Incident Response, and Career Pathways

Morning Session (2 hours)

Cybersecurity Policies and Compliance
- Role of Policies in Cybersecurity
- Understanding Regulatory Compliance (e.g., GDPR, HIPAA)
- Developing a Cybersecurity Policy, Directives, Standard and Procedures

Introduction to Governance in Cybersecurity
- Governance in cybersecurity.
- Governance frameworks and standards.
- Roles of executive management and the board in cybersecurity governance.

Managing Cybersecurity Risk
- Cybersecurity risk.
- Identification and assessment of cybersecurity risks.
- Explore risk management strategies and frameworks.

Introduction to Compliance and Regulatory Frameworks
- Concept of compliance.
- Overview of cybersecurity regulations and standards.
- Relationship between compliance, risk, and governance.

Incident Response and Recovery
- Preparing for Cyber Incidents: Prevention and Planning
- Incident Detection and Classification
- Developing an Incident Response Plan

Practical Session - Incident Response Simulation
- Hands-On: Simulated Cyber Incident Scenario
- Assessing and Responding to a Security Breach
- Learning from Realistic Scenarios

Lunch Break (1 hour) ……

Afternoon Session (3 hours)

Cybersecurity Career Pathways

- Different Roles in Cybersecurity: Analysts, Engineers, Ethical Hackers, etc.
- Certifications and Qualifications: *CISSP, CISM, CEH, CompTIA Security+, GIAC, Google Cybersecurity, Microsoft Cybersecurity, Cisco, EC-Council.*
- Building a Career in Cybersecurity: Networking, Skills, and Continuous Learning

Ethical Hacking and Responsible Disclosure

- Introduction to Ethical Hacking
- Reporting Vulnerabilities Responsibly
- Bug Bounty Programs: Opportunities and Challenges

Homework Assignment Explanation

- Creating a Personal Cybersecurity Development Plan

Online Quiz for Day 3

Course Conclusion and Interactions

- Recap of Key Learnings
- *Q&A Session and Course Wrap-Up*