Applied Cybersecurity Training Course

Professional Development Training Course Outline

Category	Information Technology	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's world, organizations must be prepared to defend against threats in cyberspace. Decision makers must be familiar with the basic principles and best practices of cybersecurity to best protect their enterprises. In this course, experts from academia, the military, and industry share their knowledge to give participants the principles, the state of the practice, and strategies for the future.

Sessions will address information security, ethical and legal practices, and mitigating cyber vulnerabilities. Participants will also learn about the process of incident response and analysis. The content is targeted at ensuring the privacy, reliability, and integrity of information systems.

The majority of the course (about 75%) is geared toward participants at the decision-making level who need a broad overview, rather than those who are already deeply immersed in the technical aspects of cybersecurity (software development, digital forensics, etc.), although both groups will find the course valuable.

Cybersecurity is a very large subject, and therefore this course is only intended to cover the basics of the current leading and pressing cybersecurity topics. The result is that we can cover many different approaches. We cover the introduction of a topic and after the fundamentals, you can explore further on your own. The goal is for participants to understand the utility of each topic, not to become specialists in any one subject.

Programme Curriculum

Applied Cybersecurity Training Course

Introduction

In today's highly connected world, applied cybersecurity is critical for safeguarding digital assets, protecting sensitive information, and ensuring operational continuity. With the rise of cyber threats, ransomware attacks, and data breaches, organizations must equip their teams with practical cybersecurity skills that go beyond theoretical knowledge. Applied Cybersecurity Training Course bridges the gap between cybersecurity theory and real-world implementation, helping participants develop hands-on expertise in defending networks, systems, and applications against evolving cyber risks.

The course covers a wide spectrum of critical areas, including network security, ethical hacking, cyber risk management, vulnerability assessment, incident response, and compliance frameworks. Participants will gain practical experience through live simulations, real-world case studies, and hands-on labs to ensure they can apply cybersecurity principles in complex environments. This program is essential for IT professionals, security officers, risk managers, and anyone committed to fortifying their organization's digital defenses.

Course Duration

5 days

Course Objectives

1. Apply network security best practices to protect organizational infrastructure.
2. Conduct vulnerability assessments and penetration tests effectively.
3. Develop and execute a comprehensive incident response plan.
4. Strengthen endpoint security and identity management systems.
5. Implement cloud security controls and compliance strategies.
6. Analyze and mitigate advanced persistent threats (APTs).
7. Employ ethical hacking techniques to identify system weaknesses.
8. Manage third-party and supply chain cyber risks proactively.
9. Apply SIEM solutions for real-time threat detection and analysis.
10. Navigate cybersecurity laws and regulatory frameworks like GDPR, HIPAA, and CCPA.
11. Develop business continuity plans integrated with cybersecurity strategies.
12. Leverage AI-driven cybersecurity solutions for predictive threat mitigation.
13. Build a cyber-resilient organizational culture through awareness programs.

Organizational Benefits

1. Strengthened cyber defense infrastructure across all departments.
2. Improved risk management and threat mitigation capabilities.
3. Reduced vulnerability to cyberattacks and data breaches.
4. Enhanced compliance with global cybersecurity regulations.
5. Increased customer trust and brand reputation.
6. Improved incident response times and effectiveness.
7. Cost savings through prevention of cyber incidents.
8. Empowered employees with hands-on cybersecurity skills.
9. Proactive adaptation to emerging cybersecurity threats.
10. Greater strategic alignment between IT and business objectives.

Target Audience

- IT Security Professionals
- Network Administrators
- Cybersecurity Analysts
- Risk Management Officers
- Compliance Managers
- Incident Response Teams
- System and Cloud Architects
- Government and Law Enforcement Officers

Course Outline

Module 1: Fundamentals of Applied Cybersecurity

- Key principles and frameworks of cybersecurity
- Cyber threat landscape and types of attacks
- Case Study: Anatomy of a ransomware attack
- Security policies and governance models

- Building a cybersecurity culture in organizations

Module 2: Network Security & Defense Strategies

- Firewalls, VPNs, IDS/IPS systems
- Secure network architecture design
- Case Study: Network breach in a financial institution
- Wireless network security best practices
- Zero Trust Networking principles

Module 3: Vulnerability Assessment & Ethical Hacking

- Vulnerability scanning methodologies
- Hands-on penetration testing techniques
- Case Study: How vulnerabilities led to major data breaches
- Red teaming and blue teaming exercises
- Using tools like Nessus, Metasploit, and Burp Suite

Module 4: Cloud Security Management

- Cloud security frameworks (AWS, Azure, Google Cloud)
- Case Study: Data leakages in cloud environments
- Implementing Identity and Access Management (IAM)
- Shared responsibility model in cloud services
- Cloud-native security controls and encryption

Module 5: Incident Response and Crisis Management

- Building an incident response team (IRT)
- Developing and testing incident response playbooks
- Case Study: Coordinated response to a phishing campaign
- Digital forensics basics and evidence handling
- Post-incident reporting and learning

Module 6: Regulatory Compliance and Risk Management

- Overview of GDPR, HIPAA, CCPA, ISO 27001 standards
- Risk management methodologies (NIST, CIS controls)
- Case Study: Compliance failures and consequences
- Conducting risk assessments and audits
- Building a cybersecurity compliance roadmap

Module 7: Emerging Technologies and Cyber Threats

- AI and machine learning in cybersecurity
- IoT security vulnerabilities and solutions
- Case Study: Cyber risks in smart devices
- Blockchain security fundamentals
- Quantum computing and its cybersecurity implications

Module 8: Business Continuity and Cyber Resilience

- Integrating cybersecurity into business continuity plans
- Crisis communication strategies during cyberattacks
- Case Study: Business recovery after a major cyber event
- Developing resilient IT infrastructures
- Conducting regular cybersecurity drills and simulations

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com