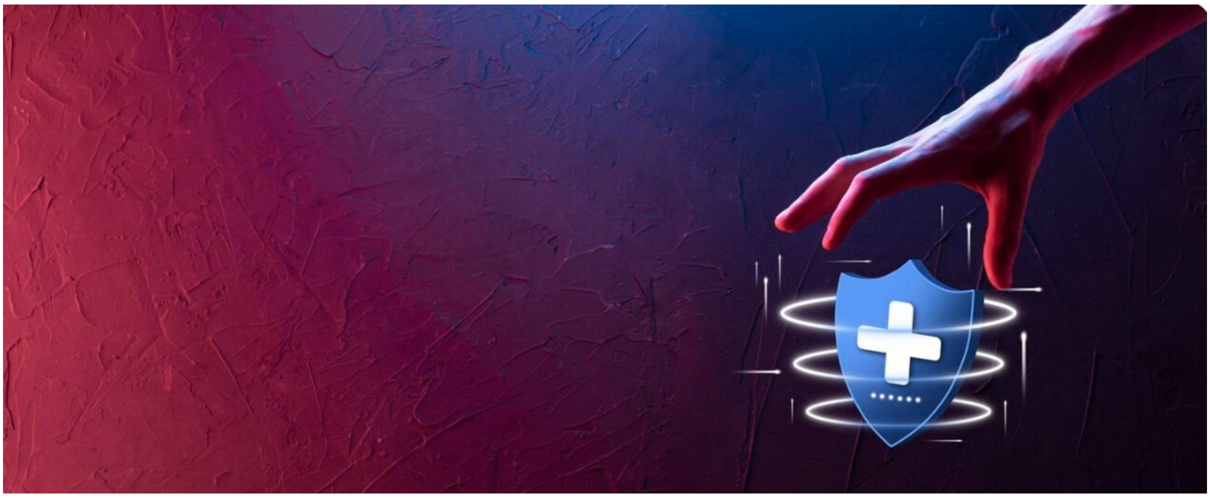

ETHICAL HACKING IN INSURANCE

(Creating Best of Minds)

Certificate in Ethical Hacking in Insurance

Course Code: BF_IP_I_0011/25

Duration: 40 Hours

Delivery Format: Hybrid

Target Audience:

- Freshers: Ideal for individuals seeking to start a career in cybersecurity, particularly in insurance, with a focus on ethical hacking.
- Professionals: Current IT professionals, security analysts, or employees in the insurance industry who want to deepen their knowledge of cybersecurity, improve risk detection, and enhance security practices.

Program Objectives:

- Understand the fundamentals of ethical hacking and its importance in the insurance sector.
- Gain hands-on experience in performing penetration testing and vulnerability assessments.
- Learn how to conduct security audits specific to insurance systems.
- Recognize common vulnerabilities in insurance-related digital infrastructures.
- Understand real-world cyber threats and develop defence strategies for the insurance industry.

Detailed Syllabus

Module 1: Introduction to Ethical Hacking in Insurance

Objective: Introduce the core concepts of ethical hacking and its relevance in the insurance industry.

Topics:

- Overview of Ethical Hacking
- The Importance of Cybersecurity in Insurance
- Key Concepts: Penetration Testing, Vulnerability Assessment, and Security Audits
- Ethical Hacking Process and Methodology
- Legal and Ethical Guidelines in Ethical Hacking

Activities:

- Discussions on the basic principles of ethical hacking.
- Case studies of cyber-attacks on insurance companies.

Assessments:

- Quiz on ethical hacking terminology and concepts.
- Short report on the importance of ethical hacking in the insurance sector.

Module 2: Penetration Testing

Objective: Provide hands-on training in penetration testing techniques within insurance systems.

Topics:

- Introduction to Penetration Testing
- Phases of Penetration Testing: Reconnaissance, Scanning, Exploitation
- Tools for Penetration Testing: Kali Linux, Metasploit, Burp Suite
- Penetration Testing in the Context of Insurance Systems
- Hands-on Exercise: Conducting a Penetration Test on a Sample Insurance Application

Activities:

- Practical exercises using penetration testing tools.
- Simulations of penetration tests on insurance applications.

Assessments:

- Assignment on conducting a penetration test and documenting findings.

- Presentation on penetration testing methodologies.

Module 3: Vulnerability Assessment

Objective: Teach how to assess and manage vulnerabilities in insurance systems.

Topics:

- Understanding Vulnerability Assessment and Its Importance in Insurance
- Vulnerability Scanning Tools: Nessus, OpenVAS
- Identifying Common Vulnerabilities in Insurance Systems
- Risk Assessment and Prioritization
- Hands-on Exercise: Running Vulnerability Scans on Sample Systems

Activities:

- Hands-on sessions with vulnerability scanning tools.
- Analyzing vulnerability reports and prioritizing remediation.

Assessments:

- Assignment on performing a vulnerability assessment and proposing solutions.
- Report on vulnerability management best practices.

Module 4: Security Audits

Objective: Train participants to conduct security audits in the insurance industry.

Topics:

- Introduction to Security Audits
- Components of a Security Audit in the Insurance Industry
- Security Standards and Compliance: GDPR, HIPAA, PCI-DSS
- Auditing Insurance Infrastructure: Networks, Applications, and Data Protection
- Hands-on Exercise: Conducting a Security Audit for an Insurance System

Activities:

- Simulations of security audit processes.
- Reviewing security standards and compliance requirements.

Assessments:

- Assignment on creating a security audit plan for an insurance company.
- Presentation on security audit findings and recommendations.

Module 5: Real-World Threats and Defence Strategies

Objective: Provide knowledge of real-world cyber threats and effective defence strategies in the insurance sector.

Topics:

- Common Cyber Threats in the Insurance Industry (Phishing, Ransomware, Data Breaches)
- Real-World Case Studies of Cyber Attacks on Insurance Companies
- Defence Mechanisms and Best Practices
- Incident Response and Recovery Procedures
- Hands-on Exercise: Developing a Security Plan for an Insurance Firm

Activities:

- Analyzing case studies of cyber-attacks on insurance firms.
- Developing incident response and recovery plans.

Assessments:

- Case study analysis and presentation on a real-world cyber-attack.
- Project: Creating a comprehensive security plan for an insurance company.