

TABLE OF CONTENTS

Chapter No.	Title	Page No.
1	Chapter 1: Introduction to Product Security	01-18
	1.1 Definition and Scope	
	1.2 Importance in Healthcare & Finance	
	1.3 Evolving Threat Landscape	
	1.4 Security vs. Compliance	
	1.5 Building a Security Culture	
	1.6 Case Studies Overview	
2	Chapter 2: Security Fundamentals	19-35
	2.1 The CIA Triad (Confidentiality, Integrity, Availability)	
	2.2 Authentication & Authorization	
	2.3 Encryption Techniques	
	2.4 Secure Coding Practices	
	2.5 Common Vulnerabilities (OWASP Top 10)	
	2.6 Security Testing Basics	
3	Chapter 3: Regulatory and Compliance Frameworks	36-52
	3.1 Overview of HIPAA	
	3.2 PCI-DSS Standards	
	3.3 SOX Compliance Requirements	
	3.4 U.S. Cybersecurity Regulations	
	3.5 Data Privacy Laws (Global Perspective)	
	3.6 Audit and Governance Practices	
4	Chapter 4: Secure Software Development Lifecycle (SSDLC)	53-69
	4.1 Phases of SSDLC	
	4.2 Threat Modeling Techniques	
	4.3 Secure Design Principles	
	4.4 Code Review Best Practices	
	4.5 DevSecOps Integration	
	4.6 Continuous Security Testing	
5	Chapter 5: Application and API Security	70-86
	5.1 Web Application Security Fundamentals	
	5.2 API Security Risks and Mitigation	
	5.3 Authentication Protocols (OAuth, SAML, etc.)	
	5.4 Session Management Best Practices	
	5.5 Microservices Security Challenges	
	5.6 Zero Trust Architecture	

6	Chapter 6: Cloud and Infrastructure Security	87-102
	6.1 Cloud Security Models (IaaS, PaaS, SaaS)	
	6.2 Shared Responsibility Model	
	6.3 Container and Kubernetes Security	
	6.4 Identity and Access Management (IAM)	
	6.5 Monitoring and Logging Strategies	
	6.6 Incident Detection and Response	
7	Chapter 7: Incident Response and Risk Management	103-120
	7.1 Incident Response Lifecycle	
	7.2 Security Operations Center (SOC)	
	7.3 Risk Assessment Techniques	
	7.4 Business Continuity Planning	
	7.5 Disaster Recovery Strategies	
	7.6 Case Studies (Healthcare & Finance)	
8	Chapter 8: Future Trends in Product Security	121-137
	8.1 AI in Cybersecurity	
	8.2 Evolution of Zero Trust	
	8.3 Quantum Security Concepts	
	8.4 Securing AI Systems	
	8.5 Emerging Threat Landscape	
	8.6 Strategic Security Roadmap	
9	Chapter 9: Security Architecture and Design Patterns	138-155
	9.1 Principles of Secure Architecture	
	9.2 Defense-in-Depth Strategy	
	9.3 Secure Design Patterns (e.g., Least Privilege, Fail-Safe Defaults)	
	9.4 Threat-Resilient System Design	
	9.5 Secure Data Flow and Trust Boundaries	
	9.6 Architecture Review and Risk Analysis	
10	Chapter 10: Human Factors and Security Awareness	156-171
	10.1 Social Engineering Attacks (Phishing, Pretexting, etc.)	
	10.2 Insider Threats and Mitigation	
	10.3 Security Awareness Training Programs	
	10.4 Secure Behavior and Developer Mindset	
	10.5 Building a Security-First Organization	
	10.6 Measuring Security Culture Effectiveness	