Secure SDLC
Adoption & Implementation

Hack2Secure
INSPIRE • INDUCE • INNOVATE
Secure Software Development Life Cycle [SSDLC or Secure SDLC] is a systematic and structured concept to integrate Security at every phase of Development Life Cycle. Ensuring security in a product from scratch, not only helps to adhere with required compliances but can also assist in implementing Security Controls at Low Cost.

### How it Helps?

- **Resiliency - Built-In Security Controls**
- **Security Assurance and Compliance**
- **Early Identification of Security Risk**
- **Awareness of Potential Engineering Challenges**
- **Low Vulnerability Mitigation Cost**
- **Measurable Risk Management**
Training, Awareness & Skill Assessment

“There is only one way to keep your product plans safe and that is by having a Trained, Aware and a Conscientious workforce”

Kevin Mitnick. ‘The Art of Deception’

Key Highlights

- Vendor Independent
- Assessments
- Hands-On / Case Studies
- Customizable
- Industry Aligned
- Role Based Programs

Training Programs

- Secure Software Development Life Cycle (Secure SDLC)
- Web Application Security Testing
- Advanced Application Security Testing
- Secure Application Coding Practices
- Handling Application Security Incidents
- Cyber Security Foundation

For more details
www.hack2secure.com/training

Secure SDLC - Certification Programs

To Schedule SWADLP Exam
www.personvue.com/hack2secure
Building Software Security Requirements

Without System Requirements, System will fail.
Without Secure System Requirement, Organizations will.

- Capturing Security Requirements
- Ensuring Product Security Baseline
- Set-up Measureable Risk Definition
- Building Security Checklist
- Define Security Quality Gates
- Align with Security Maturity Models
- Standards, Compliance & Regulations

Software Security Baseline Evaluation

Ensuring “Must-Have” Security Controls & Features, aligned with Industry Recommended Best Practices and Compliance Needs
Secure Design & Threat Modeling

Treat Security as an Integral part of Overall System Design

NIST SP 800-27: “Engineering Principles for Information Technology Security”

Attack Surface Evaluation
Threat Modeling
Identify & Prioritize Controls
Documentation

Threats are NOT Vulnerabilities
Threats Live Forever,
They are Attackers Goal

Security Centric Framework - STRIDE
Risk/Asset Centric Framework - PASTA
Integrated Scoring System - CVSS

Secure Implementation & Coding

Secure Coding Practices
- SEI CERT
- OWASP

Secure Code Review
- CWE Top 25 Programming Errors
- Static & Dynamic Code Analysis

Safeguards & Countermeasures
- Software Assurance Reference Dataset (SARD) | NIST
Key Highlights

- **Risk Based Testing**
  - Scoped according to Attack Surface

- **Grey Box Analysis**
  - Design & Implementation Level Flaws

- **In-depth Assessment**
  - Detailed Test Plan across SDLC
  - Manual & Automated Analysis

- **Customizable Components**
  - According to Software Type & Use Cases

- **Scoped as per Business Needs**
  - Security Baseline Evaluation
  - In-Depth Penetration Testing
  - OWASP Testing Guide based Evaluation
  - End-to-End Software Security Assessment

- **Dedicated Security Testing Lab**

- **Detailed Reporting**
  - Technical & Executive Reports
  - Intermediate Updates [On Demand]

- **Scoped Re-Testing of Identified Vulnerabilities**

For More details: https://goo.gl/mmxY82

www.hack2secure.com | info@hack2secure.com
Software Security - Review & Response

Security in Maintenance Phase

- Final Security Review Plan
- Auditing & Compliance Review
- Vulnerability Assessment
- Penetration Testing
- Incident Handling Plan
- Deployment and Procurement Risk

Security in Maintenance Phase

- Security Patch Management
- 3rd Party Library Upgrade
- Secure Software Disposal
- Security Escalation and Risk Measurement

www.hack2secure.com | info@hack2secure.com
Secure SDLC: Consultation

Security Programs across SDLC phases

- Optimize existing Development Process
- Industry Standard Framework alignment
- Scoped per Business Requirements
- Phases & Measurable Approach
- Compliance and Standard needs

Phase 1
- Pre-Assessment (Process Maturity Evaluation)
- Design & Propose Framework
- Define Security Roadmap

Phase 2
- Define Security Compliance & Standard Requirements
- Plan, Design & Develop Security Policies & Practices
- Building Checklist, Define Measurable Gates

Phase 3
- Business and Industry Security alignment
- SSDLC Framework alignment

Phase 4
- Security Controls - Implementation
- Testing Lab & Tools Deployment

Phase 5
- Awareness Campaign
- Case Study Generation
Hack2Secure excels in “Information Security” Domain and offers customised IT Security programs including Training & Services. These programs are designed by industry experts and tailored as per business needs, assisting students, professionals and companies with knowledge, tools and guidance required to be at forefront of a vital and rapidly changing IT industry.

Training & Certification

Hack2Secure ensures delivery of intensive, immersion security training sessions designed to master practical steps necessary for defending systems against the dangerous security threats.

- Role based Customized Training Sessions, aligned with Business Requirements
- Vendor Independent & Industry Aligned Content
- Recognized Global Assessment of skills with PearsonVUE

Services

Hack2Secure offers Information Security Professional Services to provide ways to stay ahead of Security Threats through adaptive and proactive Security methods like

- **Security Audit & Assessment**
  - Application Security Testing
  - IT Security Audit, Configuration Review
  - Vulnerability Assessment, Penetration Testing

- **Secure SDLC as a Service**
  - Process Adoption & Implementation
  - Standard & Framework Alignment
  - Secure Design Review: Threat Modeling
  - Secure Code Analysis: White/Grey Box Pen-Testing
  - Security Testing, Review & Response Plan

- **Cyber Security Consultation**
  - Start-Up Advisory
  - CyberSec Gap Analysis
  - InfoSec Risk Management
  - Incident Management
  - Compliance Alignment
  - Virtual CISO (vCISO) as a Service

Partner Program

- Global Training Partner Program

Connect With Us

M: +91 900 81 78676 | E: info@hack2secure.com

Schedule Meeting: https://calendly.com/hack2secure