

ONE PAGE SUMMARY

IT & Software > Cyber Security > Secure SDLC

Introduction to Secure SDLC

Build secure software from the ground up with Secure SDLC.

DEFINITION

Secure SDLC is a process that integrates security into software development. It ensures that security considerations are part of every phase of the software lifecycle.

KEY CONCEPTS

Phases of SDLC

The Software Development Life Cycle includes planning, design, development, testing, deployment, and maintenance.

Threat Modeling

Identifying potential threats and vulnerabilities in the design phase helps mitigate risks early.

Security Testing

Conducting tests like penetration testing and code reviews ensures that security flaws are identified and fixed.

Compliance Standards

Following regulations like GDPR or HIPAA ensures that software meets legal and security requirements.

Continuous Monitoring

Ongoing assessment of software in production helps detect and respond to security threats in real-time.

EXAMPLES

- Integrating security requirements during the design phase.
- Conducting regular security audits throughout development.
- Using automated tools for vulnerability scanning.

MEMORY TIPS

- ★ Remember 'PDTM' for Phases: Planning, Design, Testing, Maintenance.
- ★ Use 'TSC' for Threats, Security, Compliance.
- ★ Think 'Monitor to Secure' for continuous monitoring.

COMMON MISTAKES

- ✗ Ignoring security in early development stages.
- ✗ Failing to update security practices with new threats.
- ✗ Neglecting documentation of security measures.

QUICK RECAP

Secure SDLC integrates security into every phase of software development. By focusing on threat modeling, security testing, and compliance, developers can create safer applications. Continuous monitoring is essential for maintaining security post-deployment.