Software Security Practices

• Essential Principles & Best Practices

Why Software Security Matters

• Protect sensitive data

• Prevent unauthorized access

• Ensure system reliability

• Reduce vulnerability exposure

Principle of Least Privilege

• Grant minimal necessary access

• Reduces damage from compromised accounts

• Applies to users, services, APIs

Secure Coding Practices

• Validate all inputs

• Avoid hard-coded credentials

• Use parameterized queries

• Sanitize outputs

Authentication & Authorization

• Use strong password policies

• Implement MFA

• Role-based access control

• Session management best practices

Data Protection

• Encrypt data at rest and in transit

• Use secure key management

• Avoid storing unnecessary data

Threat Modeling

• Identify potential threats early

• Map entry points and weaknesses

• Use STRIDE or similar frameworks

Security Testing

• Perform code reviews

• Use automated scanners

• Penetration testing

• Regular vulnerability assessments

Patch & Dependency Management

• Keep dependencies updated

• Monitor CVE databases

• Automate patch pipelines

Incident Response

• Prepare an IR plan

• Log and monitor activity

• Contain, eradicate, recover

• Post-incident review

Best Practices Summary

• Security by design

• Continuous monitoring

• Regular updates

• Security is everyone's responsibility