*10 Best Practices for Secure Software Development –*

1. *Threat Modelling for Secure Software Development - Threat modelling involves analysing the software architecture and identifying potential security threats and vulnerabilities. This helps in designing the software with security in mind and implementing the necessary security controls.*
2. *Secure Software Coding - Developers must adhere to secure coding practices, such as input validation, secure data storage, and secure communication protocols. Secure coding practices help to prevent common security vulnerabilities such as SQL injection, cross-site scripting, and buffer overflow attacks.*
3. *Code Review - Code review involves reviewing the code written by developers to identify potential security issues. This helps in detecting and correcting security vulnerabilities early in the development process.*
4. *Testing - Regular security testing, including penetration testing and vulnerability scanning, can help identify potential security weaknesses in the software.*
5. *Secure Configuration Management - Configuration management ensures that software systems are deployed with secure configurations. This includes configuring access controls, network settings, and other security-related settings to reduce the risk of unauthorized access.*
6. *Access Control - Access control ensures that only authorized personnel can access the software system. This includes implementing user authentication and authorization mechanisms.*
7. *Regular Updates and Patches - Regular software updates and patches help to address security vulnerabilities and reduce the risk of security breaches. It is important to stay up to date with security patches and updates for all software components.*
8. *Security Training - Developers and other personnel involved in the software development process should receive regular security training to ensure that they understand the importance of security and the best practices.*
9. *Incident Response - Organizations should have a well-defined incident response plan in place to respond to security incidents.*
10. *Continuous Monitoring - Continuous monitoring helps in detecting and responding to security incidents in real time. This includes monitoring system logs, network traffic, and user behavior for any signs of security breaches.*