Yalantis

SECURITY APPROACH

SECURITY SERVICES

SECURITY TESTING	Identify vulnerabilities and weaknesses in a product from both technical and business logic perspectives. Proactively minimize the possible impact on the business.
SECURE SOFTWARE DEVELOPMENT (S-SDLC)	The implementation of security practices and controls into the software development process and software operation. Ensures the security of the product at all stages of its development and operation from the very beginning.
SECURITY COMPLIANCE	Compliance with security standards and regulations like ISO 27001, PCI DSS, HIPAA, GDPR assures customers of product security and provides access to new markets.

SECURITY SOFTWARE DEVELOPMENT AUDIT

1. **Architecture Review:**
   - Evaluate the software design and identify potential security threads.
   - Assess maturity of security controls and risk mitigation measures.
2. **Secure Development Practices:**
   - Examine development processes to ensure adherence to secure development practices.
   - Assess CI/CD process, version control and change management practices.
3. **Business Continuity and Disaster Recovery Review:**
   - Analyze critical processes, systems and data and identify potential vulnerabilities.
   - Evaluate and test your disaster recovery processes (e.g. backup recovery, incident response plans) to identify gaps.
4. **Data Storage and Encryption:**
   - Assess data storage practices to ensure sensitive data is adequately protected on production.
   - Evaluate data encryption methods for data in transit and at rest.
5. **Authentication and Authorization Assessment:**
   - Evaluate the effectiveness of authentication mechanisms and access controls.
   - Verify user roles and permissions to prevent unauthorized access.
6. **Third-Party Integrations:**
   - Review security of third-party integrations for security.
   - Validate the secure integration of external APIs.

SECURITY TESTING

1. **Vulnerability Scanning:**
   - Instrumental scanning of the infrastructure for known vulnerabilities
   - Identify weaknesses and misconfigurations
2. **Web and Mobile Security Testing:**
   - Test for common web application vulnerabilities like XSS and CSRF.
   - Evaluate the security of mobile applications against potential threats.
3. **Penetration Testing:**
   - Perform simulated attacks to exploit potential vulnerabilities in the application.
   - Evaluate business logic to identify flaws and possible fraudulent activity
4. **Cloud Audit**
   - Instrumental scanning of the infrastructure for known vulnerabilities
   - Identify weaknesses and misconfigurations
5. **Source Code Review:**
   - Analyze the application's source code for security vulnerabilities to identify coding errors, injection points, and sensitive data handling issues
   - Assess 3rd party components for known vulnerabilities
6. **Reporting and Recommendations:**
   - Provide detailed reports for both the audit and testing phases.
   - Include a prioritized list of identified vulnerabilities and recommendations for remediation.

Yalantis

THANK YOU

Thanks for considering Yalantis. Visit our website **yalantis.com** or drop a message at **hello@yalantis.com** if you're curious to find out more about us, our services, and the technologies we use.