TestingXperts Security Testing Capabilities

TechDefcon
www.techdefcon.com

TestingXperts
Passion For Perfection

Security Testing Services

Security Testing Services

Organisations are getting affected every day by security allied incident such as Network Intrusion, Cross Site Scripting (XSS) and DOS/DDOS attack. TestingXperts Security Test Services has effective approach to guard against the risk an organisation can face. Like, Architecture Assessment from Security point of view (Threat Modeling), Security Audit & Security Testing.

Our Services

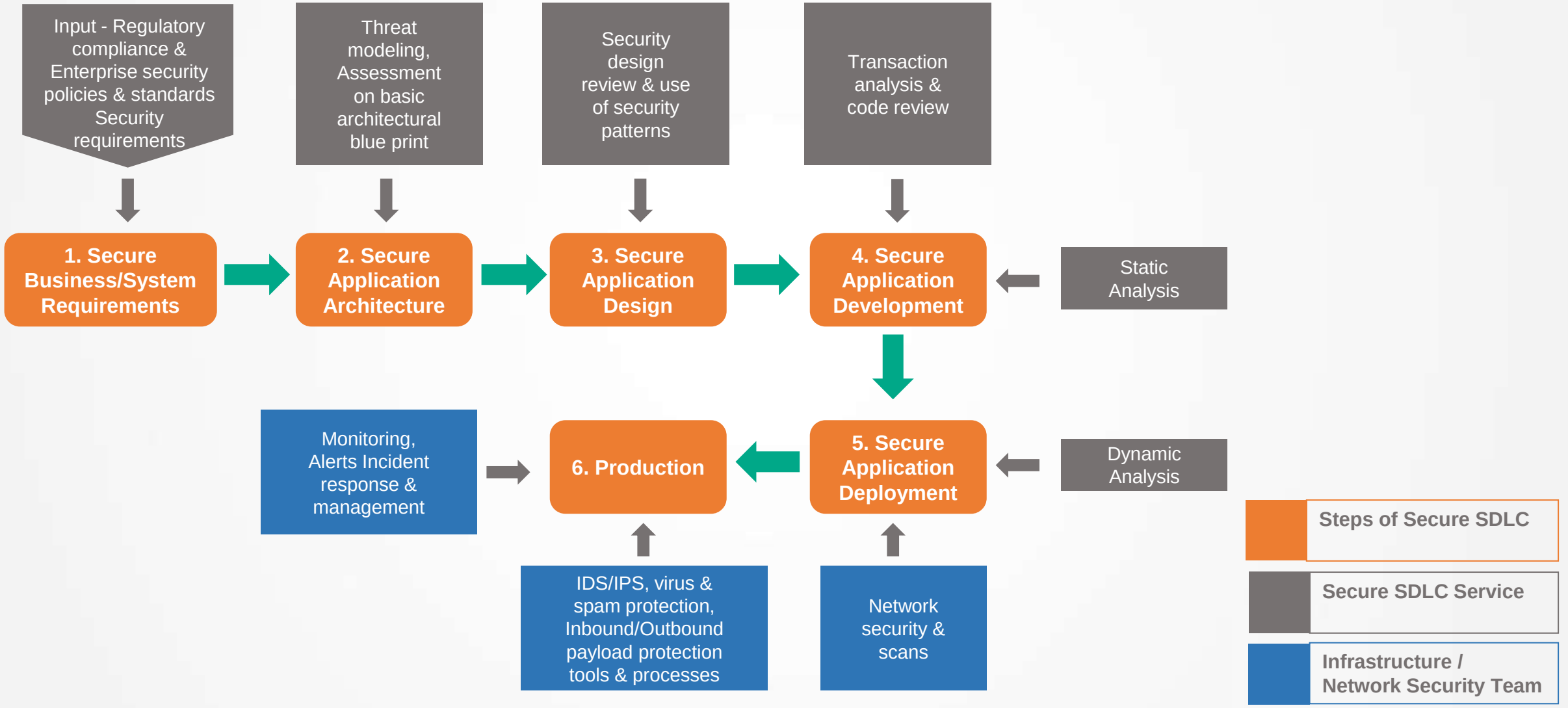
- Security Consultancy (Application level threat assessment)
- Packaged Application Security Testing
- Security Testing Center of Excellence
- Mobile Lab for Security Testing
- Threat Modelling
- Security audit
- Dynamic Analysis
- Penetration testing

TestingXperts Security Testing Advantage:

- *Pool of CEHs (Certified Ethical Hackers)*
- *Conformance with international standards including* OWASP, SANS, OSSTMM, PCI, HIPAA, FDA, SOX, etc.
- *Vendor independence coupled with deep expertise of key security technologies*
- *The report classifies each vulnerability in appropriate categories along with mitigation strategy*
- *Ensuring zero false positive with snap shot of exploitation*
- *Complete coverage of regression testing*
- *Vulnerability free application with iterative strategy for further release*
- *Supported Tools: HP Web Inspect , IBM App Scan, Acunetix, Cenzic Hailstorm, Burp Suit Pro and other open source tools*

Security Testing Strategy

Optimal strategy for Application security requires security across various activities throughout the development life cycle. Component & E2E Security is a unified solution for optimal application security, which is illustrated below:



Security Testing Process

TechDefcon TestingXperts Passion For Perfection

Security Testing

Well planned Security Testing, use of appropriate tools to identify potential vulnerabilities and security status of your applications.

Identify Critical System & Information Gathering

- Identify critical system to be assessed
- Identify the scan window
- Gather information about target
- Port Scanning
- OS fingerprinting

Tool Mapping & Scheduling

- Fine-tuning the tool for Vulnerability assessment
- Selection of plugins/ checks/ scripts
- Scheduling the Scan

Vulnerability Identification

- Scan Vulnerability on Application
- Characterisation of vulnerability

Result Analyse & Reporting

- Collect evidence
- Elimination of False positive
- Summarise and report results

Gap for Fixes

Re-testing

- Re-test the fixes and complete application
- Re-testing report
- Sign off report

Case Studies

Case Study 1 – Security Testing for a healthcare company in UK

Client:

- A leading Health care company in the area of mobile health and work in partnership with clinicians

Project Brief:

- Customer have created a new portal for NHS Innovation Challenge Prizes 2014/15
- Security Testing of newly developed application for Security loopholes

Approach / Solution:

Our Approach was to meet Information Security Industry standards like OWASP Top 10, SANS Top 15 and others at the priority:

- Primarily focused on Network transportation, Session Management, Authentication, input Validation checks
- Used commercial, Open Source tools and manual testing to meet the objective
- Prone to Man in the Middle Attack (MIM), Credentials transported in plain text, Password Policy & Critical information disclosure vulnerability were identified with a very high impact score

Challenges:

- Security testing activity finished in 5 days according to project release date
- Follow the Iterative Secure SDLC process, this includes complete security regression test with any new component that is developed

Business Benefits:

- 60% of vulnerabilities identified as critical
- Best penetration testing of the application using OWASP tools helped client obtain certification by renowned test services
- Compliance of applications with security regulations
- Reduces cost through identification of security defects at an early testing stage
- Adherence to company's internal security policies and external laws
- Integration of testing mechanisms with industry best practices such as the Open Web Application Security Project (OWASP)

Tool / Devices Used:

- HP WEB INSPECT

Case Study 2 – Security Testing for an E-Learning Application

Client:

- Client is a leading e-learning company offering efficient and customized solutions around curriculum and media development, assessments, learning solutions etc.

Business Needs:

- Client was working on implementation of the product for various end customers and was looking for thorough security testing of 2 applications:
    - Questions Authoring application for teachers
    - Assessments application for teachers and learners
- Application was on load balancing environment with SSL enabling and servers on AWS behind virtual private cloud (VPC)

Approach / Solution:

Our **Approach was to meet Information Security Industry standards** like OWASP Top 10, OSSTMM standards and others at the priority:

- Understood the application, security requirements, security assets, user roles, access levels, authentications
- Application was scanned using TX's Security testing framework based on open source tools and Burp Suite Pro and vulnerabilities were identified
- The initial testing was completed in a challenging timeline of 2 weeks to meet client's implementation timelines
- TX provided detailed recommendations on security vulnerabilities along with providing the client a demo of how various vulnerabilities could be replicated and exploited to gain unauthorised access to systems and data.

Business Benefits:

- Identified all vulnerabilities in the application including 6 critical vulnerabilities
- The report classified each vulnerability in appropriate categories, and TX suggested mitigation strategy for them enabling the client to fix the issues in quick time
- Suggested an iterative security check strategy for further releases

Tool / Devices Used:

- TX's security testing framework, Burp Suit Pro

Thank You

www.techdefcon.com
sales@techdefcon.com