

**Deloitte.**



**Powering growth  
through smart cyber**  
You build. We secure.

For Private circulation only

Risk Advisory ●





## About

Deloitte's Product Security Testing helps clients identify vulnerabilities in their products by assisting them throughout the product development life cycle from a security standpoint. Our experienced cyber professionals and well-equipped security labs are a one-stop solution for Product Security Testing, which provides guidance, stability, and security needed to confidently deploy enterprise products.

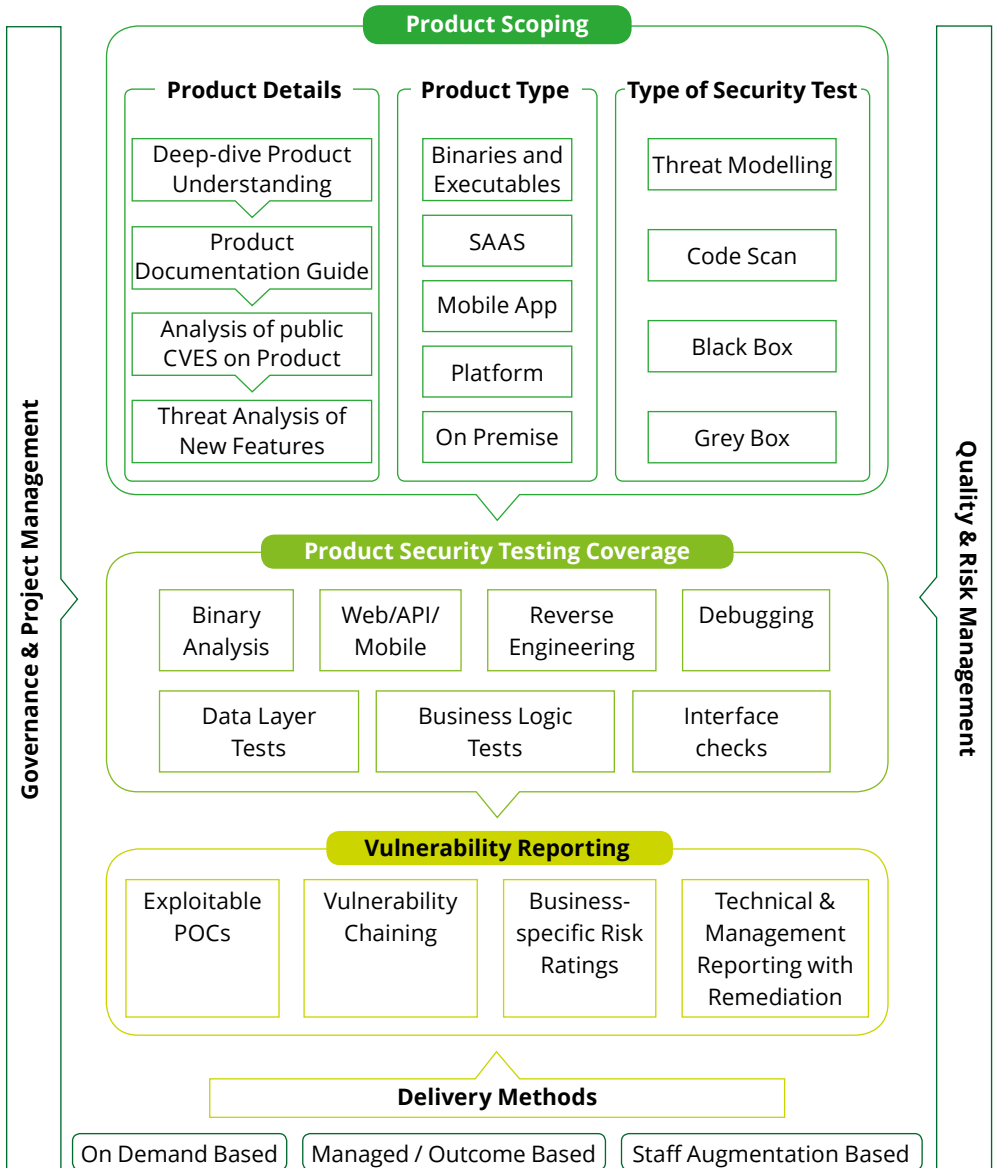
## Typical challenges in Product Security Testing

-  **Blind Spot while Scoping** The size and complexity of the product leads to "blind spots" during scoping and coverage when traditional security testing approach is followed.
-  **Standard Threats & Risks** No two product security testing plans are alike as each product has a unique threat profile and faces different risks.
-  **Knowledge of Product** Complete functional and technical knowledge about the product does not usually get translated into effective product security testing strategy and execution.
-  **Skill Sets** Product Security Testing requires various skill sets to work together; this is not always possible.

## Benefits

-  Deep product knowledge by referring to documentation such as security guides, installation guides, and administration guides that helps us understand the product and conduct threat analysis.
-  Beyond the scope of conventional penetration testing; vulnerability chaining to highlight the exploitability factor, eliminates edge cases and identification of security issues in third-party or open-source packages.

# Our Product Security Testing framework



## Case Study 1

Large multinational product-based company – Security assessment of their flagship cloud-based learning management solution (LMS)

### Client



Leading multinational product-based company; one of the world's largest rich internet application development with annual revenue close to US\$ 7.3B.

The client engaged Deloitte to:

- Perform security assessment of their flagship cloud-based LMS that consists of a modern rich internet web solution and mobile apps (iOS and Android based) powered by more than 700 APIs
- Evaluate the security posture of this SAAS solution deployed on Amazon EC2
- Provide effective and implementable remediation solutions for the identified vulnerabilities and exploits

### What we did



- Performed a deep-dive manual web application security assessment that led to the uncovering of 61 impactful vulnerabilities
- Focused on uncovering security vulnerabilities that are related to business logic flaws, privilege escalation, and user roles authentication and authorisation
- Identified and remediated highly impactful vulnerabilities in mobile apps; this was done by following the custom mobile Pentesting methodology developed by Deloitte

### Outcomes/ Impact



- Most of the reported vulnerabilities (>60%) were classified as zero day in nature and immediate fixes were rolled out considering their criticality and impact.
- Authorisation-based security flaws helped the client take a relook at the configured gateway and consistently apply rules across incoming service calls.
- Although the solution underwent multiple security assessments by internal teams and external Pentesting vendors, the client appreciated the depth of coverage and the quality of security bugs uncovered.

## Case Study 2

Large multinational product-based company – Security assessment of their legacy application development product

### Client



Leading multinational product-based company; one of the world's largest rich internet application development with annual revenue close to US\$ 7.3B.

The client engaged Deloitte to:

- Perform security assessment of their legacy application development product
- Binary executables, development platform and applications developed and deployed on this solution were in scope
- Evaluate the latest threats affecting this legacy product that has been in the market for over a decade
- Provide effective and implementable remediation for the identified vulnerabilities and exploits

### What we did



- Performed a deep-dive product security assessment that led to the uncovering of more than 40 zero day vulnerabilities
- Conducted assessments, including binary analysis, reverse engineering, vulnerabilities detection (with respect to open-source and third packages within the solution), attack surface analysis, and deep-dive web Pentesting
- Identified and remediated exploitable critical vulnerabilities

### Outcomes/ Impact



- Immediate fixes were rolled out considering the criticality and impact of the discovered vulnerabilities.
- Bypass with respect to inherent security controls and filters was implemented within the product; this helped the client take a relook at the configurations and profiles.
- Although the solution underwent multiple security assessments by internal teams, security researchers, and external Pentesting vendors, the client appreciated the depth of coverage and the quality of security bugs uncovered.

# Contacts

**Rohit Mahajan**

President – Risk Advisory  
rmahajan@deloitte.com

**Shree Parthasarathy**

Partner  
sparthasarathy@deloitte.com

**Gaurav Shukla**

Partner  
shuklagaurav@deloitte.com

**Maninder Bharadwaj**

Partner  
manbharadwaj@deloitte.com

**Santosh Jinugu**

Director  
sjinugu@deloitte.com

Product Security



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.