KPMG Assurance and Consulting Services LLP
Embassy Golf Links Business Park
Pebble Beach, B Block, 1st & 2nd Floor,
No. 13/2, Off Intermediate Ring Road
Bengaluru 560 071 India

Telephone: +91 80 6833 5000
Fax: +91 80 6833 6999
Web: www.kpmg.com/in
Email: indiawebsite@kpmg.com

Date: 30-June-2022

Cloud Based Assessment Completion for the Year 2022 (H1)

Symphony Summit AI is focused on building next generation of artificial intelligence and machine learning applications across multiple verticals and is backed by SymphonyAI. Symphony Summit had approached KPMG for Infrastructure Vulnerability Assessment and Penetration Testing (Cloud Based Assessment) of the identified IP addresses.
This letter is a confirmation for completion of the Vulnerability Assessment and Penetration Testing activity carried out at the ITARC LAB, KPMG - Bangalore.

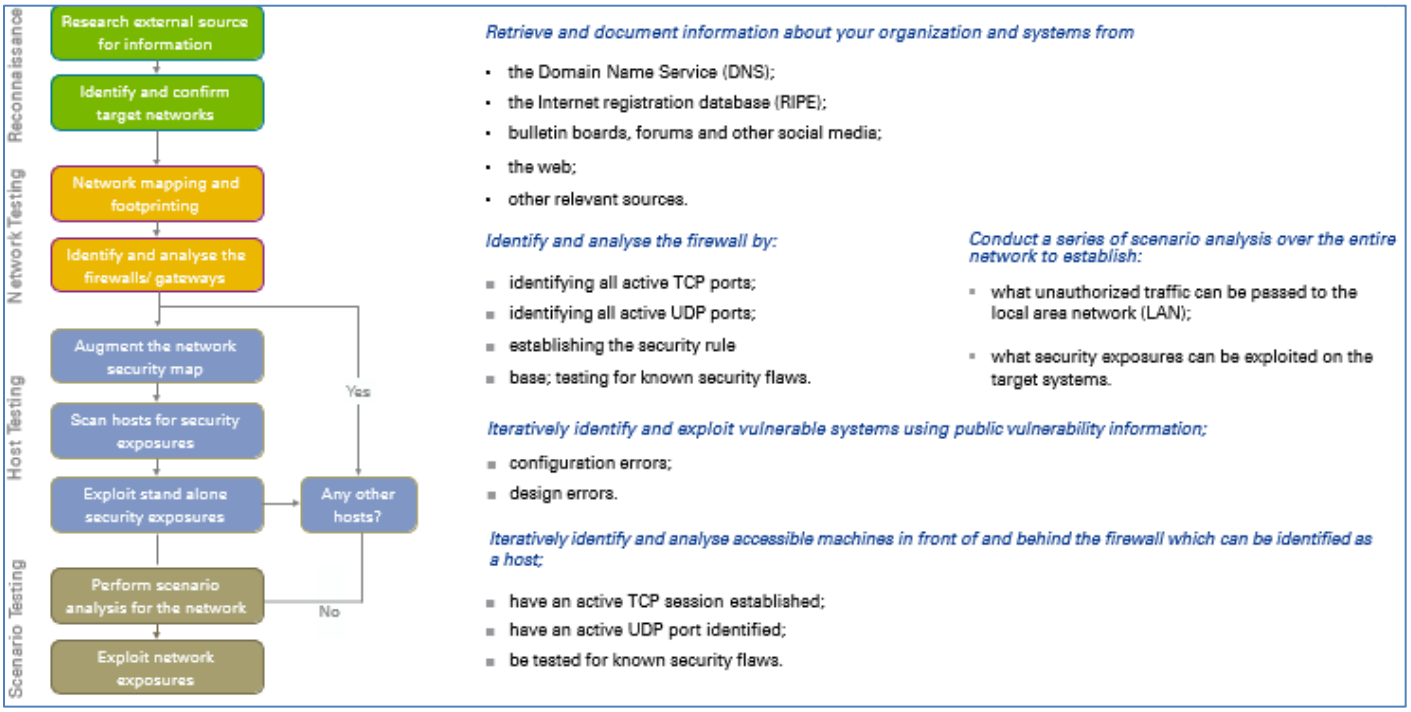
Scope of Work					
Hosting Provider	Microsoft Azure				
Identified Zones for VAPT Activity	Azure Central India Production Datacenter (ss_ci_prd_ea) Azure Southeast Asia and Production Datacenter (ss_sea_prd_ea) Azure North Central US Production Datacenter (ss_ncus_prd_ea) Azure West Europe Production Datacenter (ss_we_prd_ea) Azure East Australia Production Datacenter (ss_eas_prd_ea) IDN Production Datacenter Azure Staging Datacenter (ss_global_staging_ea) Azure Pre-Prod Datacenter (ss_global_preprod_ea) Azure Global Edge Datacenter (ss_global_edge_ea) Azure Global Corp Datacenter (ss_global_corp_ea) Azure Global POC Datacenter (ss_global_poc_ea)				
Type of Security Testing	Vulnerability Assessment and Penetration Testing (VAPT)				
Brief Methodology of Testing	KPMG Conducted an external non-intrusive penetration test by simulating a destructive attack from the Internet, identifying system weaknesses and with an intention to exploit them to gain access to the system and other confidential resources.				
Initial Test Dates	15th April to 24th April 2022	**Retest Dates**	27th June 2022	**Testing Location**	Bangalore India

During our security testing activity, total of 9 issues were observed in the Production Environment and 10 issues were observed in the Non-Production Environment in the in-scope IP addresses for testing.

KPMG Vulnerability Assessment and Penetration Testing Methodology

To facilitate the provision of security services, we have designed an illustrative approach that identifies the most serious risks and security flaws first and then focuses on less obvious areas as the project proceeds.

Sample illustration stating our approach and methodology for conducting security testing activity is as below.



Disclaimers:

1. This report has been prepared exclusively by KPMG for Summit IT Solutions Private Limited ("Client") based on the terms of the Contract with the Client.
2. The responsibility of the application performance is solely with the Client's management and reader of the Summary report should exercise its own due diligence with respect to the details under this Summary.
3. The information covered in the Summary is not intended to address the circumstances of any particular individual or entity and no recipient should act on the contents herein without appropriate professional advice.
4. In connection with our report or any part thereof, KPMG does not owe duty of care (whether in contract or in tort or under statute or otherwise) to any person or party to whom the report is circulated to and KPMG shall not be liable to any party who uses or relies on this report. KPMG thus disclaims all responsibility or liability for any costs, damages, losses, liabilities, expenses incurred by such third party arising out of or in connection with the report or any part thereof.
5. By reading our report, the reader of the report shall be deemed to have accepted the terms mentioned hereinabove.