SymphonyAI Summit Inc.

Technical Security Assessments – Standard Operating Procedures

November 2023

Contents

Introduction

Purpose

This Standard Operating Procedure has been developed to define the procedure for technical security assessments as mentioned in the below scope provided by the EY team to SymphonyAI Summit Inc.

This document includes steps to perform the quarterly and half-yearly assessment as mentioned in the below scope and reporting for SymphonyAI Summit Inc to help ensure that an appropriate level of security is maintained. EY shall help identify vulnerabilities in the below defined scope and prioritize vulnerability mitigation efforts to mitigate information security risks.

This is a confidential document and should only be shared with employees, temporary employees and third-party contractors contracted to provide services to client.

Scope

This procedure is applicable to the Pentest activities performed by the EY team for SymphonyAI Summit Inc. The activities covered as part of this procedure is given scope as below:

- ❑ Internal & External Network VA/PT
    - ❑ Production IPs
    - ❑ Non-production IPs
- ❑ Web Applications and APIs VA/PT
- ❑ Think Client Penetration Testing
- ❑ Mobile Application Penetration Testing
- ❑ Reporting
- ❑ Remediation Testing

Introduction

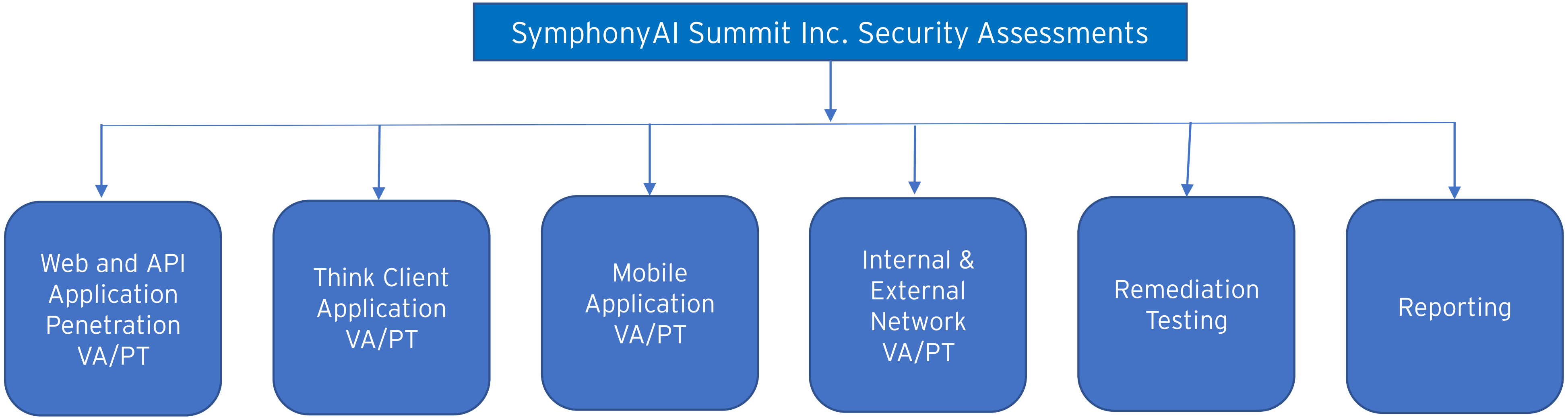
Definitions

- Vulnerability Assessment: Vulnerability assessment is a process of identifying and evaluating potential weaknesses and security flaws in a system, network, or application to assess their susceptibility to threats and attacks.
- Penetration Testing: Penetration testing is a proactive cybersecurity approach that involves authorized hackers simulating real-world attacks on a system or network to uncover vulnerabilities and assess its security posture.
- Remediation Testing: Remediation testing is a follow-up assessment conducted after addressing vulnerabilities identified in a previous security assessment, ensuring that the fixes or mitigations effectively resolve the issues and enhance overall security.
- Inventory: List of all the network IP addresses of all devices/nodes, IP addressing scheme used and maintained by SymphonyAI Summit Inc.

Introduction

Currently as part of the SymphonyAI Summit Inc. security assessments, EY conducts quarterly Web, API, Mobile, Thick client Penetration testing and half-yearly internal & external VA/PT and issues detailed penetration testing reports for the same. These reports contain vulnerabilities which are classified based on criticality and SymphonyAI Summit Inc. specific requirements.

The activities performed as part of the SymphonyAI Summit Inc. security assessments is depicted below:


SymphonyAI Summit Inc. Security Assessments
Web and API Application Penetration VA/PT
Think Client Application VA/PT
Mobile Application VA/PT
Internal & External Network VA/PT
Remediation Testing
Reporting

The process for performing these services are provided in subsequent slides.

1. Web Application and APIs VA/PT Approach

- Perform a Black box and Grey Box Penetration Testing exercise, targeting in scope assets
- The Penetration Testing exercise follow the OWASP top 10 approach and consisted of the activities listed in the table below

Activity	Description	Objective	Procedure
I	Information gathering	▪ Understand the application and underlying technologies used	▪ Identify information accessible in public domain such as search engines. ▪ Perform initial discovery of the application to obtain URLs.
II	Application foot printing	▪ Identify entry fields, login pages, attack surfaces	▪ Based on the information gathered, a profile of the target is made, also known as a 'footprint'. ▪ Identify the main entry points to the application and create a footprint of the application. ▪ Explore and obtain platform/software versions of underlying infrastructure.
III	Vulnerability analysis & exploitation	▪ Identify vulnerabilities and perform proof of concept exploitation	▪ Conduct vulnerability scans on the application as an unauthenticated user. ▪ Manual test of the application will be performed to identify the logic flaws in the application which can lead to security compromises. ▪ Cross verifies the vulnerabilities identified by automated scanners to eliminate false positives ▪ Conduct tests to identify OWASP top ten categories of vulnerabilities ▪ Perform controlled exploitation to assess the true impact of the vulnerabilities identified by using: • Published software exploits • Fuzzers and brute forcers • Web application exploitation frameworks

1. Web Application and APIs VA/PT Approach (cont.)

OWASP Top Ten – Web and API Application Penetration Exercise

#	Web Based OWASP Top 10	API Based OWASP Top 10
1	Broken Access Control	Broken Object Level Authorization
2	Cryptographic Failures	Broken Authentication
3	Injection	Broken Object Property Level Authorization
4	Insecure Design	Unrestricted Resource Consumption
5	Security Misconfiguration	Broken Function Level Authorization
6	Vulnerable and Outdated Components	Unrestricted Access to Sensitive Business Flows
7	Identification and Authentication Failures	Server Side Request Forgery
8	Software and Data Integrity Failures	Security Misconfiguration
9	Security Logging and Monitoring Failures	Improper Inventory Management
10	Server-Side Request Forgery	Unsafe Consumption of APIs

1. Web Application and APIs VA/PT Process

INPUT

- Inventory from stakeholder

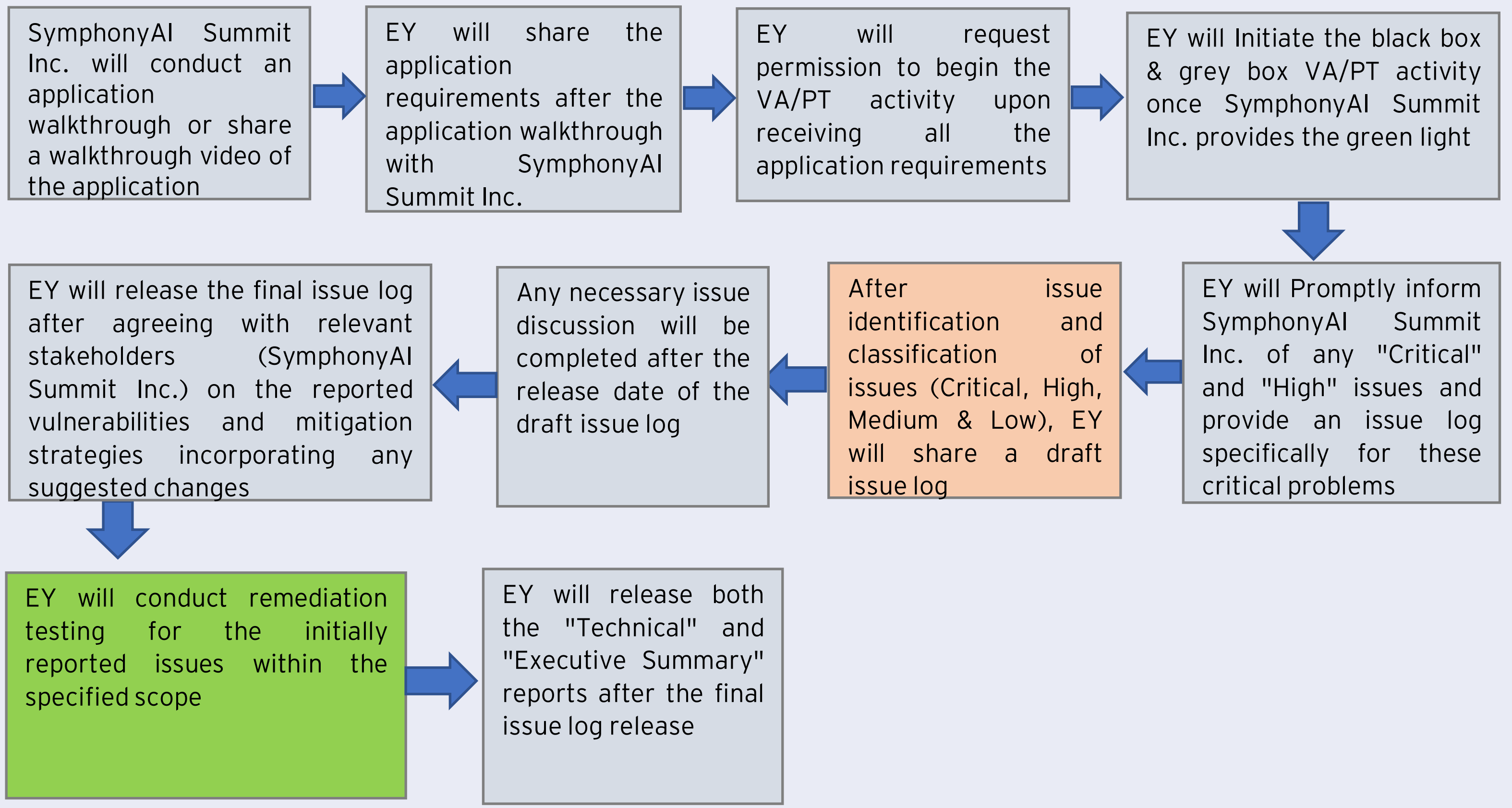
TRIGGER:

- Every Quarter

TOOLS & ENABLERS:

- Nessus Professional
- Burp Suite Pro
- Kali Linux
- TestSSL
- Metasploit, etc.

PROCESS



SymphonyAI Summit Inc. will conduct an application walkthrough or share a walkthrough video of the application

EY will share the application requirements after the application walkthrough with SymphonyAI Summit Inc.

EY will request permission to begin the VA/PT activity upon receiving all the application requirements

EY will Initiate the black box & grey box VA/PT activity once SymphonyAI Summit Inc. provides the green light

EY will Promptly inform SymphonyAI Summit Inc. of any "Critical" and "High" issues and provide an issue log specifically for these critical problems

After issue identification and classification of issues (Critical, High, Medium & Low), EY will share a draft issue log

Any necessary issue discussion will be completed after the release date of the draft issue log

EY will release the final issue log after agreeing with relevant stakeholders (SymphonyAI Summit Inc.) on the reported vulnerabilities and mitigation strategies incorporating any suggested changes

EY will conduct remediation testing for the initially reported issues within the specified scope

EY will release both the "Technical" and "Executive Summary" reports after the final issue log release

Output

- Final Issue Log
- Final Technical Report
- Final Executive Summary Report

Note:

- SymphonyAI Summit Inc. to ensure no change in application during the penetration testing.

🟧 Issue Identification and classification

🟩 Remediation Testing

2. Thick Client Application VA/PT Approach

- Perform a Black box and Grey Box Penetration Testing exercise, targeting in scope assets
- The Penetration Testing exercise follow the OWASP top 10 approach and consisted of the activities listed in the table below

Activity	Description	Objective	Procedure
I	Application walkthrough	▪ Understand the functionality of the application.	▪ Analyze the traffic exchanged between the client and the server to understand the under-the-hood behaviour of the application. ▪ Application’s data storage mechanism (whether encrypted, plain text etc.) was understood.
II	Reverse Engineering	▪ Obtain the source code from the application file ▪ Gather cached information ▪ Identify flaws in application related files exposed to the users ▪ Memory Analysis	▪ Decompiling the application file and analysing the exposed functions for vulnerabilities and unauthorized access. ▪ Perform tests with respect to the known vulnerabilities associated with the thick Client and the technology used. ▪ Extract and review sensitive information stored in Logs, files, Registries and Memory.
III	Vulnerability scan and exploitation	▪ Identify the flaws in the application. ▪ Attempt exploitation of the identified flaws to demonstrate the impact of the identified vulnerabilities and elimination of possible false positives	▪ Perform application vulnerability scans with scan policies aimed at detecting thick client Application weaknesses and OWASP top ten vulnerabilities. ▪ Perform manual tests to review the following aspects of the application: ▪ Authentication ▪ Authorization / Access Control ▪ Input Validation ▪ Storage of sensitive information , Informational Messages ,Transmission security ▪ Perform vulnerability linkage by using identified flaws in tandem to achieve significant level of unauthorized access.

2. Thick Client Application VA/PT Process

INPUT

- Inventory from stakeholder

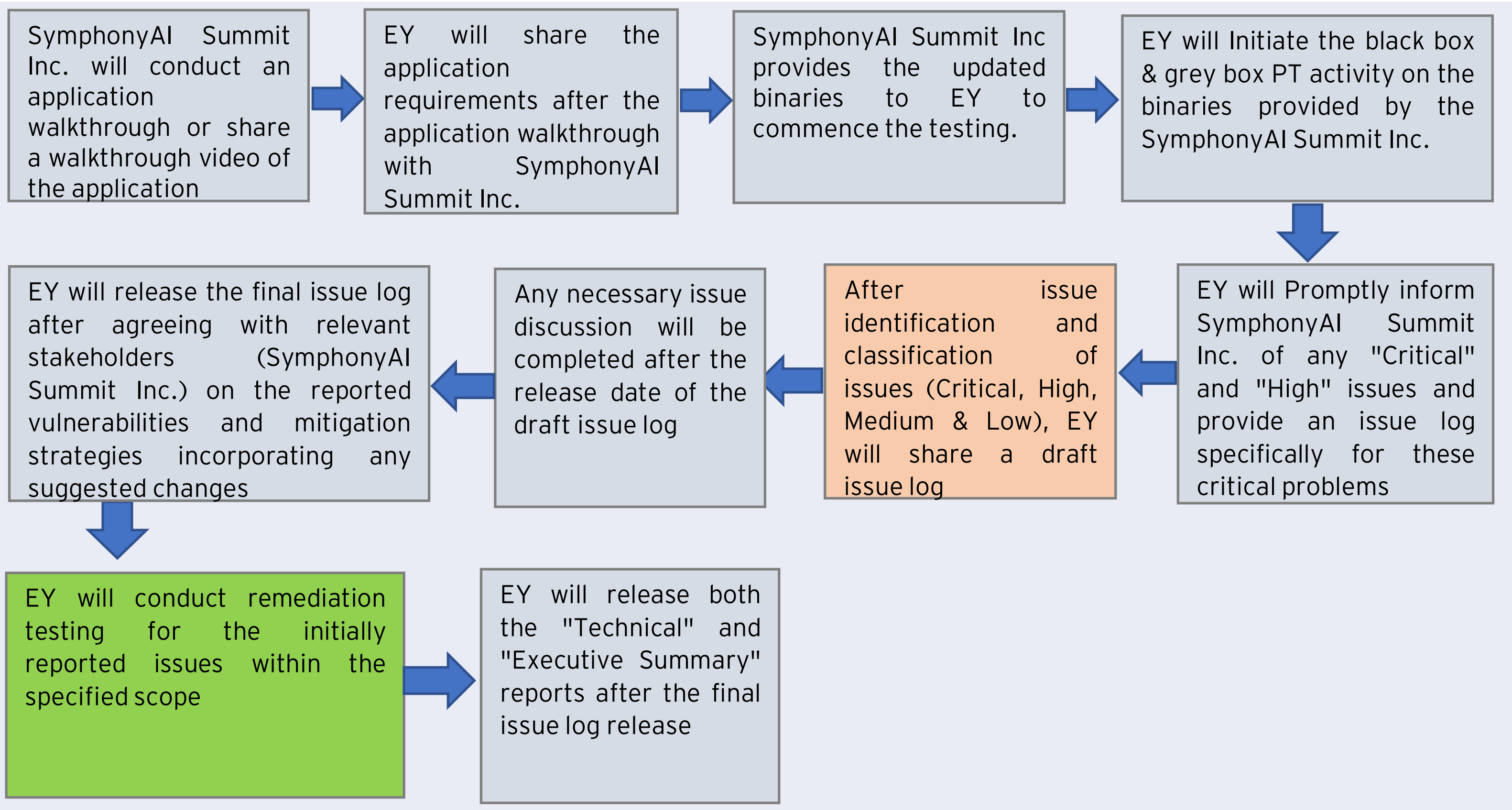
TRIGGER:

- Every Quarter

TOOLS & ENABLERS:

- CFF Explorer
- dnSpy
- JetBrains Dotpeek
- Wireshark
- tcpdump,
- Burp Suite Pro ,etc.

PROCESS



SymphonyAI Summit Inc. will conduct an application walkthrough or share a walkthrough video of the application

EY will share the application requirements after the application walkthrough with SymphonyAI Summit Inc.

SymphonyAI Summit Inc provides the updated binaries to EY to commence the testing.

EY will Initiate the black box & grey box PT activity on the binaries provided by the SymphonyAI Summit Inc.

EY will Promptly inform SymphonyAI Summit Inc. of any "Critical" and "High" issues and provide an issue log specifically for these critical problems

After issue identification and classification of issues (Critical, High, Medium & Low), EY will share a draft issue log

Any necessary issue discussion will be completed after the release date of the draft issue log

EY will release the final issue log after agreeing with relevant stakeholders (SymphonyAI Summit Inc.) on the reported vulnerabilities and mitigation strategies incorporating any suggested changes

EY will conduct remediation testing for the initially reported issues within the specified scope

EY will release both the "Technical" and "Executive Summary" reports after the final issue log release

Output

- Final Issue Log
- Final Technical Report
- Final Executive Summary Report

Note:

- SymphonyAI Summit Inc. to ensure no change in application during the penetration testing.

Issue Identification and classification

Remediation Testing

3. Mobile Application VA/PT Approach

- Perform a Black box and Grey Box Penetration Testing exercise, targeting in scope assets
- The Penetration Testing exercise follow the OWASP top 10 approach and consisted of the activities listed in the table below

Activity	Description	Objective	Procedure
I	Emulation	▪ Setup test environment	▪ Setup testing environment using emulation tools such as: ▪ Android emulator (Eclipse) and the corresponding Android SDK ▪ iPhone emulator (XCode) and the corresponding iOS API ▪ Tunnel traffic through local HTTP proxy tool ▪ Identify work around for SSL enabled applications ▪ Create/ obtain required test data in the application
II	Discover	▪ Understand the application	▪ Reverse engineer the mobile binary to identify sensitive data resident on the mobile device and any key access controls embedded in client-side code ▪ Understand the basic business functionality of the application to identify possible entry and exit points of information ▪ Identify application's data stores (at rest, in transit or on display) and sensitivity ▪ Document the initial observations to be used as input during the testing phase
III	Vulnerability Analysis & Exploitation	▪ Identify and exploit vulnerabilities	▪ Based on the observations in the discovery phase, formulate test cases and carry out the security testing for the following: ▪ Weak server-side controls ,Insecure data storage ,Insufficient transport layer protection ▪ Unintended data leakage, Poor authorization and authentication ▪ Security decisions via untrusted inputs, Improper session handling ▪ Improper platform usage and Client code quality

3. Mobile Application VA/PT Approach (cont.)

OWASP Top Ten – Mobile Security Penetration Exercise

#	Mobile Application Based OWASP Top 10
1	Platform Misuse
2	Lack of data Storage Security
3	Insecure Communication
4	Insecure Authentication
5	Insufficient Cryptography
6	Insecure Authorization
7	Client Code Quality
8	Code Tampering
9	Reverse Engineering
10	Extraneous Functionality

3. Mobile Application VA/PT Process

INPUT

- Inventory from stakeholder

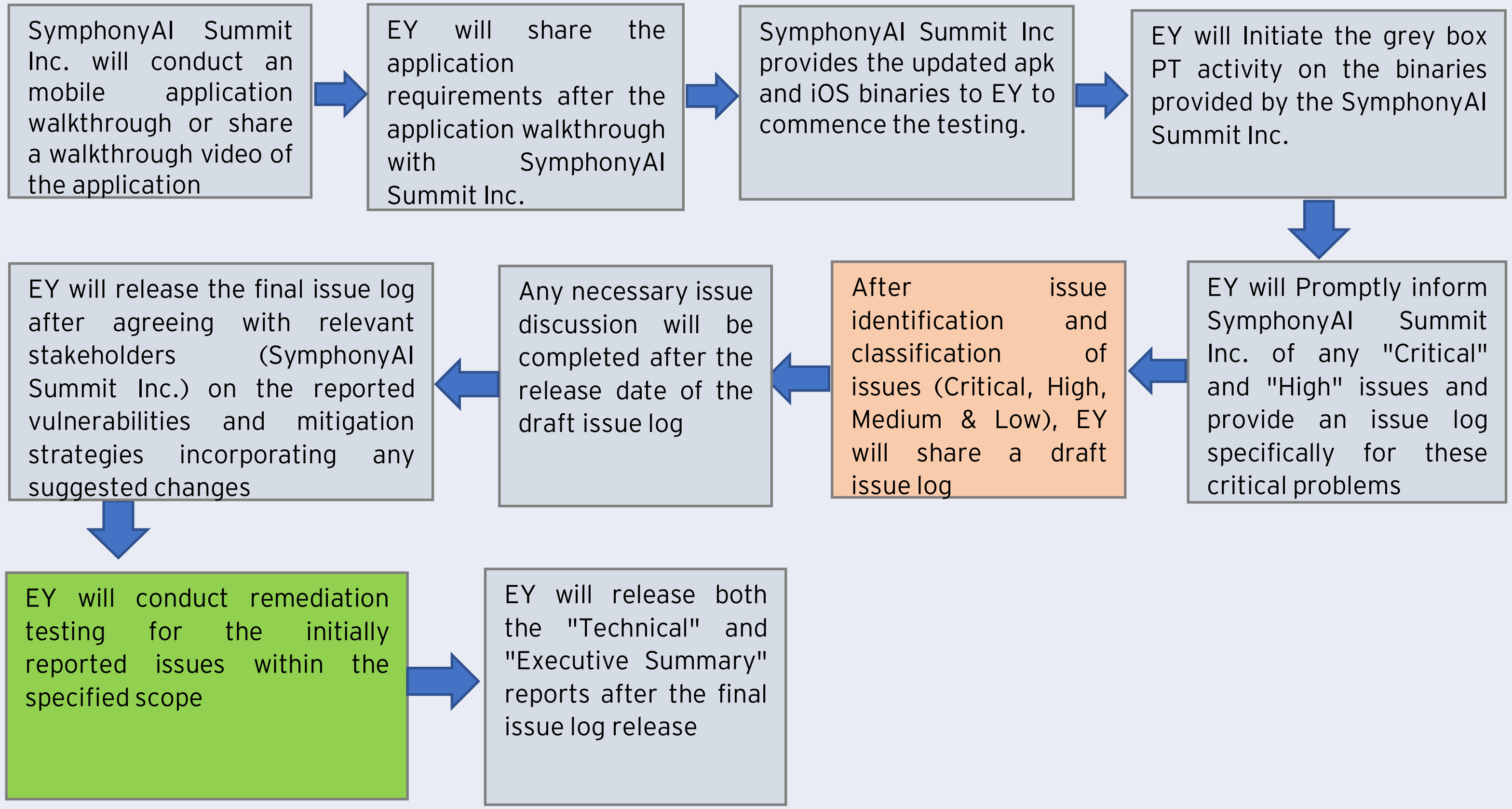
TRIGGER:

- Every Quarter

TOOLS & ENABLERS:

- Frida
- MobSF
- Ghidra
- Wireshark
- Burp Suite Pro ,etc.

PROCESS



SymphonyAI Summit Inc. will conduct an mobile application walkthrough or share a walkthrough video of the application

EY will share the application requirements after the application walkthrough with SymphonyAI Summit Inc.

SymphonyAI Summit Inc provides the updated apk and iOS binaries to EY to commence the testing.

EY will Initiate the grey box PT activity on the binaries provided by the SymphonyAI Summit Inc.

EY will Promptly inform SymphonyAI Summit Inc. of any "Critical" and "High" issues and provide an issue log specifically for these critical problems

After issue identification and classification of issues (Critical, High, Medium & Low), EY will share a draft issue log

Any necessary issue discussion will be completed after the release date of the draft issue log

EY will release the final issue log after agreeing with relevant stakeholders (SymphonyAI Summit Inc.) on the reported vulnerabilities and mitigation strategies incorporating any suggested changes

EY will conduct remediation testing for the initially reported issues within the specified scope

EY will release both the "Technical" and "Executive Summary" reports after the final issue log release

Output

- Final Issue Log
- Final Technical Report
- Final Executive Summary Report

Note:

- SymphonyAI Summit Inc. to ensure no change in application during the penetration testing.

Issue Identification and classification

Remediation Testing

4. Internal & External Network VA/PT Approach

- Perform a Black box Penetration Testing exercise, targeting in scope assets
- The Penetration Testing exercise follow the OWASP top 10 approach and consisted of the activities listed in the table below

Activity	Description	Objective	Procedure
I	Basic footprint checks	▪ Identify whether the specified hosts are responding to ICMP & UDP requests	▪ Check whether the hosts are responding to ICMP Echo Request. ▪ Perform Trace route.
II	Services Scan	▪ Determine the attack surface exposed by each of the target asset.	▪ Perform a TCP and UDP scan for common services. ▪ Deduce application and version details of the listening services where applicable.
III	Vulnerability Assessment	▪ Identify vulnerabilities in the services identified during the previous activity	▪ Retrieve system information by querying SNMP, NetBIOS, finger, or other listening services. ▪ Perform vulnerability scan targeting the services. ▪ Perform vulnerability linkage by exploring the possibility of using identified flaws in tandem to achieve significant level of unauthorized access.
IV	Exploitation	▪ Retrieve system information ▪ Gain access to the systems and to deduce the business and technical risk	▪ Use public exploit frameworks such as the Metasploit framework and publicly available/custom scripts to perform controlled exploitation on the vulnerabilities identified. ▪ Employ manual checks or manual exploitation techniques wherever feasible. ▪ Use the exploited systems as a vantage point to gain more privileges or access more resources within the sensitive systems/ networks.

4. Internal & External Network VA/PT Process

INPUT

- Inventory from stakeholder

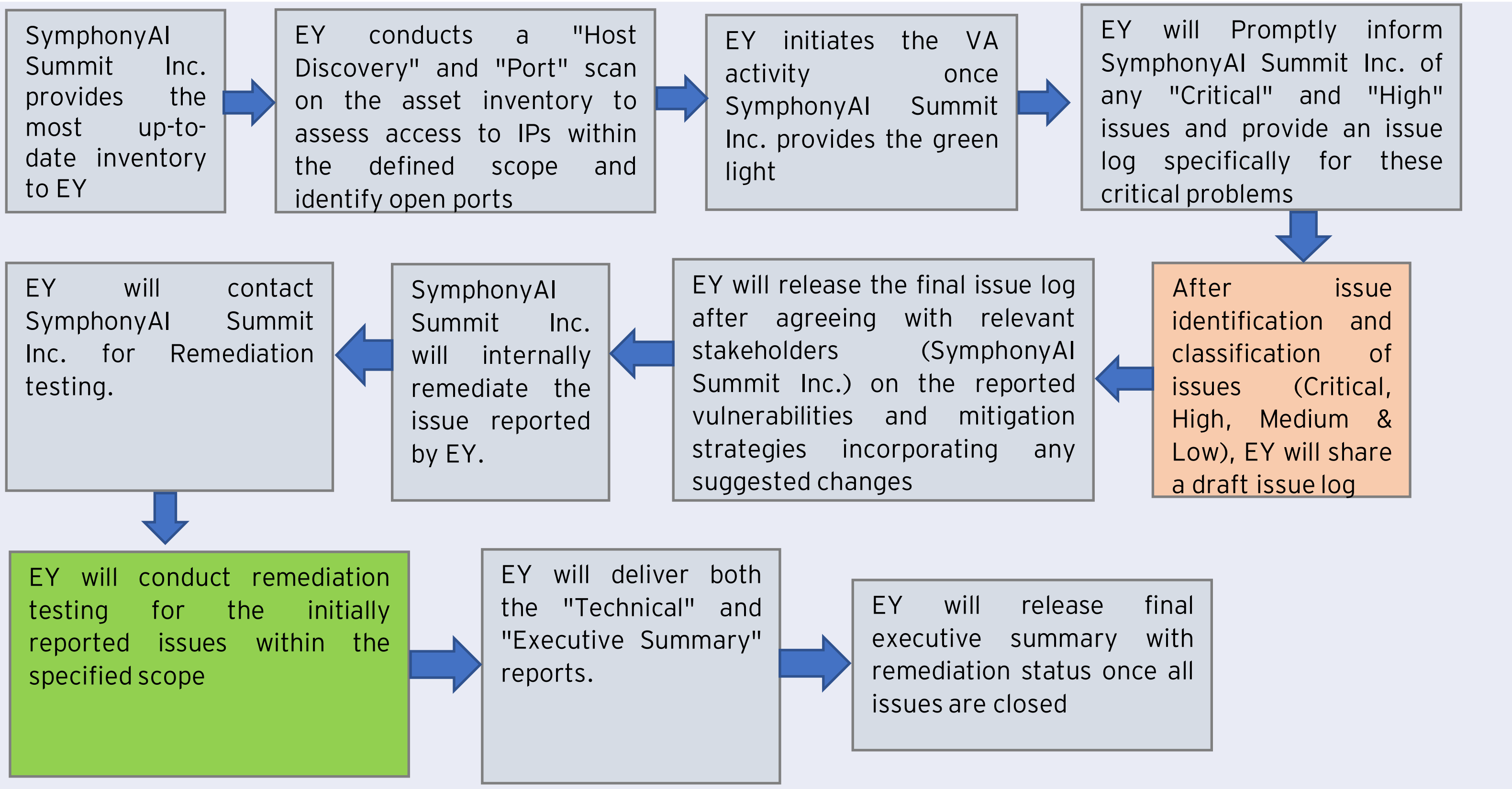
TRIGGER:

- Every Six month

TOOLS & ENABLERS:

- Nessus Professional
- Nmap
- Kali Linux
- TestSSL
- SSHScan
- Metasploit, etc.

PROCESS



SymphonyAI Summit Inc. provides the most up-to-date inventory to EY

EY conducts a "Host Discovery" and "Port" scan on the asset inventory to assess access to IPs within the defined scope and identify open ports

EY initiates the VA activity once SymphonyAI Summit Inc. provides the green light

EY will Promptly inform SymphonyAI Summit Inc. of any "Critical" and "High" issues and provide an issue log specifically for these critical problems

After issue identification and classification of issues (Critical, High, Medium & Low), EY will share a draft issue log

EY will release the final issue log after agreeing with relevant stakeholders (SymphonyAI Summit Inc.) on the reported vulnerabilities and mitigation strategies incorporating any suggested changes

SymphonyAI Summit Inc. will internally remediate the issue reported by EY.

EY will contact SymphonyAI Summit Inc. for Remediation testing.

EY will conduct remediation testing for the initially reported issues within the specified scope

EY will deliver both the "Technical" and "Executive Summary" reports.

EY will release final executive summary with remediation status once all issues are closed

Output

- Final Issue Log
- Final Technical Report
- Final Executive Summary Report

Note:

- SymphonyAI Summit Inc. to ensure reachability of in-scope IPs and respective open ports from scanning machine

Issue Identification and classification

Remediation Testing

5. Remediation Testing

INPUT

- List of identified issues in the initial VA/PT activity
  - Web Application and API VA/PT
  - Think Client Web Application Penetration Testing
  - Mobile Application Penetration Testing
  - Internal & External Network VA/PT

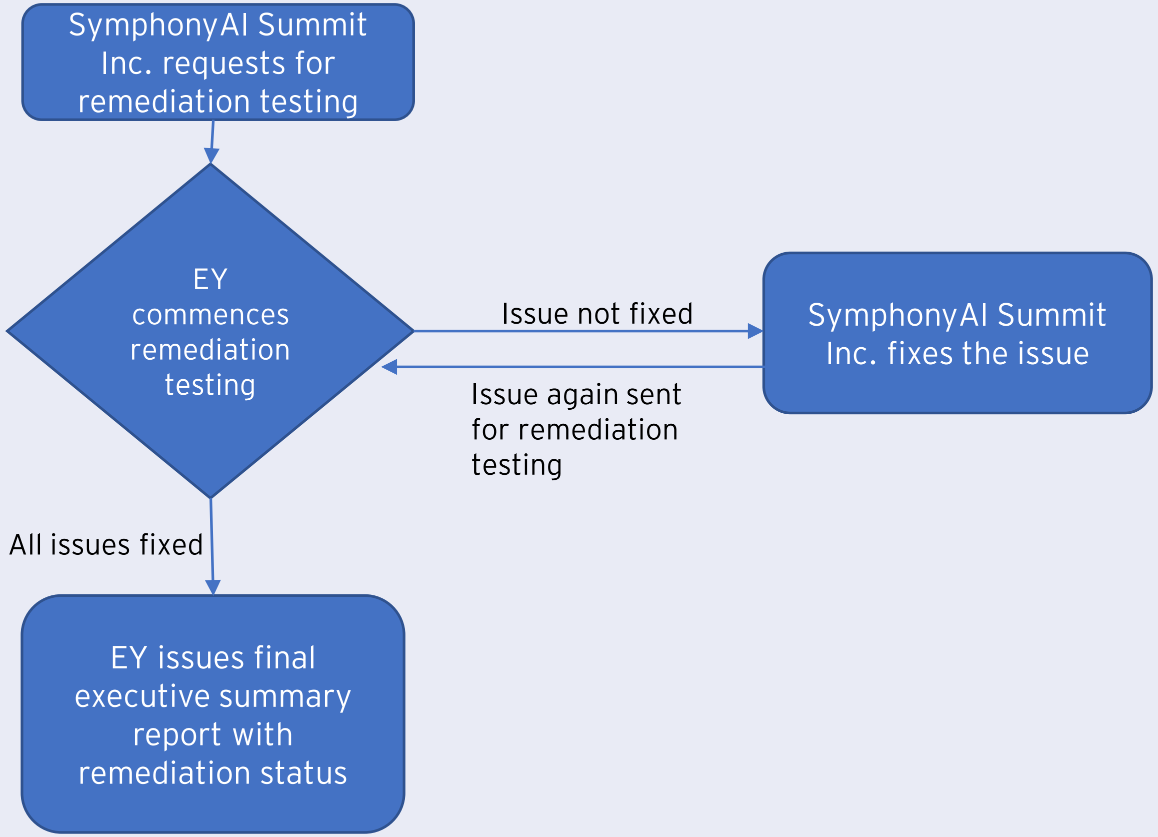
TRIGGER:

- Remediation testing request raised by stakeholders

TOOLS & ENABLERS:

- Burp Suite Pro, Nessus Professional, NMAP etc.

PROCESS



SymphonyAI Summit Inc. requests for remediation testing

EY commences remediation testing

Issue not fixed

SymphonyAI Summit Inc. fixes the issue

Issue again sent for remediation testing

All issues fixed

EY issues final executive summary report with remediation status

Output

- Final executive summary report with remediation status

Note:

- EY will perform up to one round of remediation testing

6. Reporting

INPUT

- Asset Inventory
- Application details

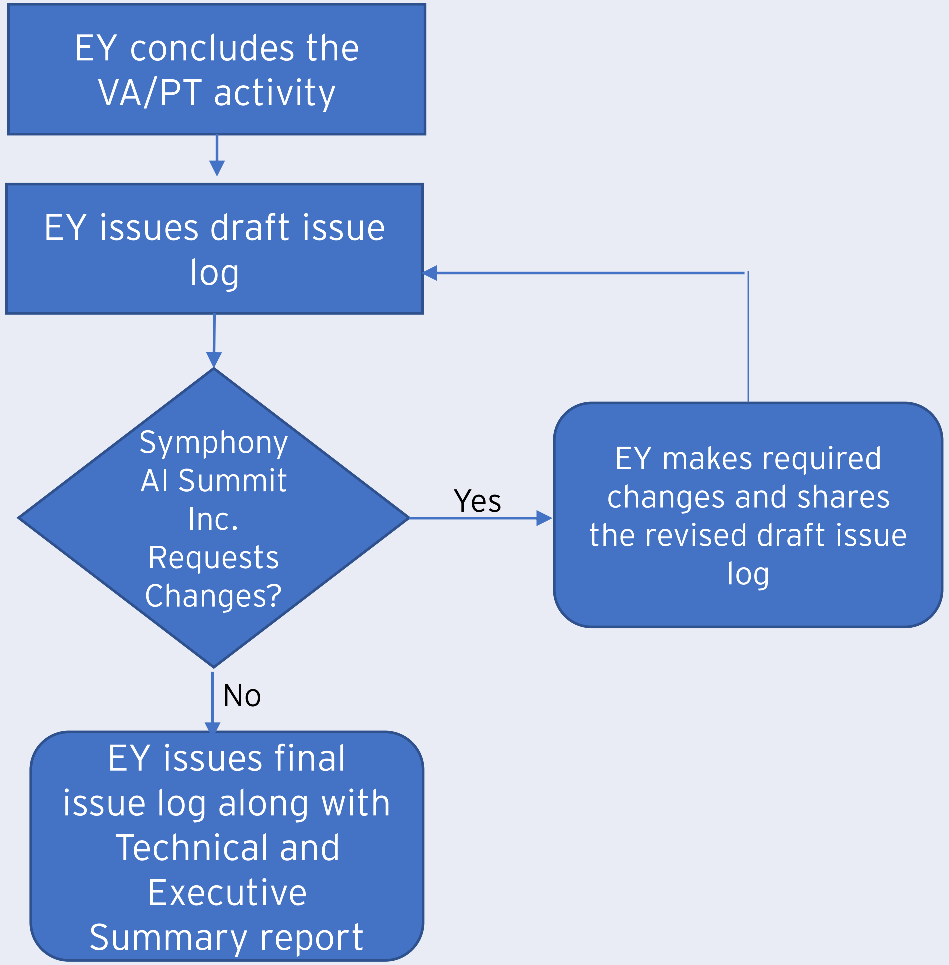
TRIGGER:

- VA/PT activity completion

TOOLS & ENABLERS:

- EY Standardized Report Template
- Email for report delivery

PROCESS


EY concludes the VA/PT activity
EY issues draft issue log
Symphony AI Summit Inc. Requests Changes?
Yes
EY makes required changes and shares the revised draft issue log
No
EY issues final issue log along with Technical and Executive Summary report

Output

- Final issue log
- Technical report
- Executive summary report

Note:

- The report will be discussed with SymphonyAI Summit Inc. on specific issues, if requested

Annexure – Basis of Risk Ratings

Risk Rating	CVSS Score	Level of severity
Critical	**9.0-10.0**	➢ **Probability of occurrence**: Exploit techniques are well known and the circumstances under which the attack may occur are very common ➢ **Impact**: Vulnerability noted on the affected IT asset can be exploited to obtain remote privileged or unprivileged access, and/or cause severe impact to system operations and organization as a whole ➢ **Ease of exploitation**: Exploit techniques can be easily obtained and executed by unskilled attackers
High	**7.0-8.9**	➢ **Probability of occurrence**: Exploit techniques are well known and the circumstances under which the attack may occur are very common ➢ **Impact**: Vulnerability noted on the affected IT asset can be exploited to obtain remote privileged or unprivileged access, and/or cause severe impact to system operations ➢ **Ease of exploitation:** Exploit techniques can be easily obtained and executed by unskilled attacker
Medium	**4.0-6.9**	Vulnerability noted on the affected IT asset / hosted application: ➢ **Probability of occurrence**: Exploit techniques are known and the circumstances under which the attack may occur are common ➢ **Impact**: Vulnerability noted on the affected IT asset can be exploited to obtain limited user privileges or network level access ➢ **Ease of exploitation:** Exploit techniques can be easily obtained and executed by persons with general computer security knowledge
Low	**0.1-3.9**	▸ **Probability of occurrence**: The vulnerability is rarely exploited, or exploitation may not be practical in usual scenarios ▸ **Impact**: Vulnerability may lead to information disclosures without any specific access to affected systems. Exploitation may not have significant impact on the company from a business or reputation standpoint. ▸ Ease of Exploitation: Requires highly skilled hackers or state-sponsored resources for exploiting this vulnerability noted on the affected IT asset / hosted application:

Annexure – Basis of Risk Ratings Contd..

Risk Rating Parameters

Parameters	Description
Probability of occurrence	Probability of occurrence defines the possibility of the vulnerabilities being exploited in public or within the corporate environment
Impact	Impact indicates the extent to which a successful attack can affect the organization's technical and business landscape
Ease of exploitation	Indicates how easily vulnerabilities can be exploited i.e., by a beginner or a skilled attacker