PROOF OF CONCEPT — CUSTOMER DOCUMENTATION PACK

Zimperium MAPS Mobile Application Protection Suite

A structured, engineer-led Proof of Concept framework covering qualification, scoping, technical prerequisites, test cases, success criteria and sign-off — delivered by SecureCentral, an authorised value-added partner for Zimperium across Australia, New Zealand, Singapore, Malaysia and Indonesia.

DOCUMENT	APPLIES TO	TYPICAL DURATION	CLASSIFICATION
SC-ZIM-MAPS-POC v1.0	**zScan · zShield · zKeyBox · zDefend**	**2 weeks**	**Confidential — Customer & Partner**

How to use this pack. Sections 1–4 are read-only briefing material for the prospect. Sections 5–8 are completed jointly by the SecureCentral Solutions Engineer and the customer during the Discovery call. Sections 9–11 are the fillable forms that must be returned before licence keys and SDK artefacts are issued. Section 12 is the closure and sign-off record.

Contents

1 Zimperium MAPS at a glance
2 POC objective, scope & out-of-scope
3 POC process & timeline
4 Roles, responsibilities & RACI
5 Qualification questionnaire (mandatory)
6 Technical prerequisites checklist
7 POC test cases
8 Threat detection & handling action matrix
9 Form A — End User (Customer) Details
10 Form B — Application for POC
11 Form C — Reseller / Partner Details
12 Success criteria, closure & sign-off
13 Appendix — glossary & contacts

1 · Zimperium MAPS at a glance

Zimperium **MAPS (Mobile Application Protection Suite)** secures the mobile applications you build and publish — across the full lifecycle, from source code through to apps running on untrusted consumer devices. It comprises four complementary modules:

zScan — Discover

Automated static/binary analysis of your compiled app. Surfaces privacy, compliance and coding vulnerabilities (OWASP MASVS/MASTG, PCI MPoC, GDPR) inside CI/CD, before release.

zShield — Protect

Hardening / shielding of the app binary: code obfuscation, anti-tamper, anti-debug, anti-reverse-engineering and integrity checks. No source code changes required.

zKeyBox — Secure

White-box cryptography. Keys are never present in the clear in memory or at rest, protecting secrets, tokens and payment credentials even on a compromised device.

zDefend — Detect & Respond

Embedded on-device SDK with machine-learning runtime protection (RASP). Detects device, network, malware and app-level attacks and triggers configurable responses in real time.

Why a POC matters. The objective of a MAPS POC is **not** to deliver production-grade protection. It is to give your engineering and security stakeholders evidence-based confidence that MAPS integrates cleanly with your build pipeline, detects the threats you care about, and triggers the response actions your risk policy requires — with acceptable performance and size overhead.

2 · POC objective, scope & out-of-scope

ITEM	DEFINITION
Primary objective	Validate that Zimperium MAPS meets the customer's security requirements for the nominated mobile application(s), within an agreed time-box.
In scope	☐ Validate application of code protection capabilities (zShield) ☐ Validate zDefend detection and integration capabilities ☐ Validate zScan vulnerability scan output on the target binary ☐ Validate zKeyBox white-box crypto (OPTIONAL — only if keys/secrets in scope) ☐ Validate console visibility, threat telemetry and reporting
Out of scope	✗ Third-party penetration testing or red-team engagement ✗ Production release / app-store submission of a protected build ✗ Performance benchmarking beyond indicative size & start-up measurement ✗ Custom feature development or unreleased roadmap items ✗ Integration to SIEM/SOAR beyond a single sample webhook (unless agreed in Form B)
Time-box	Standard 2 weeks from kickoff. Extensions require written agreement from SecureCentral and Zimperium.
Environment	Non-production build variant, Zimperium SaaS console tenant provisioned by SecureCentral, physical test devices supplied by the customer.

3 · POC process & timeline

Step 0 — Scoping & Discovery ALL STAKEHOLDERS

Complete Section 5 qualification questionnaire. Agree timelines and scope, align resources, assess current state, confirm success criteria. Forms A, B and C submitted.

Step 1 — zDefend ENGINEERING

zDefend introduction · threat workshop · review of integration requirements and capabilities · SDK embedded into the target app · console tenant walk-through.

Step 2 — zScan & zShield ENGINEERING + SECURITY

zScan introduction, scan of target app(s), review of findings. zShield introduction, protection applied to target app(s), build process validated and repeatable.

Step 3 — Validation / Testing ENGINEERING + SECURITY

Independent execution of the Section 7 test cases on customer devices. Evidence captured (screenshots, console events, logs). Implementation review.

Step 4 — Closure ALL STAKEHOLDERS

Gather POC results, validate open success criteria, communicate outcome to stakeholders, sign-off in Section 12, commercial proposal issued by SecureCentral.

Agreed schedule

TARGET DATE	STAGE	PARTICIPANTS	STATUS
	Step 0: Scoping & Discovery	All stakeholders	
	Step 1: zDefend	Engineering	
	Step 2: zScan / zShield	Engineering, Security	
	Step 3: Validation / Testing	Engineering, Security	
	Step 4: Closure & sign-off	All stakeholders	
	Weekly sync cadence (day/time)	Core team	

4 · Roles, responsibilities & RACI

ROLE	ORGANISATION	NAME / CONTACT	RACI
Executive sponsor	Customer		Accountable
Security lead / CISO delegate	Customer		Responsible
Mobile engineering lead	Customer		Responsible
DevOps / build owner	Customer		Responsible
QA / test lead	Customer		Consulted
Outsourced dev partner (if any)			Consulted
Solutions Engineer (POC owner)	SecureCentral		Responsible
Account Manager	SecureCentral		Informed
Reseller / Implementation partner			Consulted
Vendor Sales Engineer	Zimperium		Consulted

5 · Qualification questionnaire MANDATORY BEFORE POC APPROVAL

To be completed by the SecureCentral Solutions Engineer with the customer. A POC will not be scheduled until Q1–Q9 are answered. Answers directly determine module selection, SDK variant and effort.

1 Why are you looking for a mobile app security solution? Is there a security incident or urgency driving this?

Establishes the compelling event, budget owner and realistic timeline.

☐ Active / recent security incident ☐ Fraud or account-takeover losses ☐ App cloning, repackaging or piracy
☐ Regulatory / compliance mandate ☐ Penetration test or audit finding ☐ Customer or board requirement
☐ Proactive security uplift ☐ App-store or scheme requirement (e.g. PCI MPoC)

DETAIL — INCIDENT DESCRIPTION, DRIVING DEADLINE, CONSEQUENCE OF NO ACTION

Urgency: ☐ Critical (<30 days) ☐ High (this quarter) ☐ Medium (next 2 quarters) ☐ Exploratory

2 Are you doing outsourced development?

Determines who receives the SDK, NDA coverage, IP handling and who must attend technical sessions.

☐ No — fully in-house ☐ Yes — fully outsourced ☐ Hybrid — in-house + vendor

DEVELOPMENT PARTNER NAME(S)

COUNTRY / LOCATION OF DEV TEAM

WHO OWNS THE SOURCE CODE & SIGNING KEYS?

CAN THE PARTNER JOIN POC TECHNICAL SESSIONS? (Y/N)

3 Native vs hybrid development?

Drives which zDefend SDK variant and which zShield protection profile are used.

☐ Native Android (Kotlin / Java) ☐ Native iOS (Swift / Objective-C) ☐ Hybrid / cross-platform
☐ Mixed — native + embedded web views

4 If hybrid — which framework and which exact version?

e.g. React Native v0.82, Flutter 3.24, Cordova, Ionic/Capacitor, Xamarin/.NET MAUI, Unity, NativeScript. Version compatibility must be confirmed with Zimperium before kickoff.

☐ React Native ☐ Flutter ☐ Cordova / Ionic / Capacitor ☐ .NET MAUI / Xamarin ☐ Unity ☐ NativeScript ☐ Other

FRAMEWORK

EXACT VERSION (E.G. V0.82)

MINIMUM OS SUPPORTED (ANDROID API / IOS)

BUILD SYSTEM (GRADLE / XCODE / CI TOOL & VERSION)

> **Action:**
> SecureCentral to confirm framework/version support with Zimperium engineering **prior** to Step 1. Unsupported versions may require an upgrade or a native-wrapper approach.

5 Which platform is the focus — Android, iOS or both?

Determines artefact requirements, number of test devices and POC effort.

☐ Android only ☐ iOS only ☐ Both (recommended)

ANDROID — MIN / TARGET API LEVEL

IOS — MIN DEPLOYMENT TARGET

TEST DEVICES AVAILABLE (MODEL / OS / ROOTED OR JAILBROKEN?)

DISTRIBUTION CHANNEL (PLAY / APP STORE / MDM / ENTERPRISE)

6 What are the test cases for the POC?

The standard MAPS test-case set is
provided by SecureCentral
— see Section 7. Customer may add up to five bespoke cases.

☐ Accept SecureCentral standard test cases (Section 7) ☐ Standard set + customer-specific additions (list below)

CUSTOMER-SPECIFIC TEST CASES (MAX 5)

7 Which threats are you detecting today, and what is the handling mechanism when a threat is detected?

e.g. rooting / jailbreak, hooking (Frida, Xposed), malware, emulator, debugger, screen sharing, tampering. Example: threat = rooting/jailbreak → handling action = shut down the app. Complete the matrix in Section 8.

☐ No detection today ☐ In-house/home-grown checks ☐ Open-source library (e.g. RootBeer)
☐ Another commercial RASP vendor

CURRENT TOOLING / VENDOR (IF ANY)

KNOWN GAPS OR BYPASSES EXPERIENCED

→
Complete the full threat & handling action matrix in Section 8.

8 Do you want to implement custom handling actions in this POC, or use the SDK "No-Code" action?

No-Code = zDefend shuts the app down and redirects to a browser page showing a URL you configure — zero development effort. Custom = your app handles the threat callback in code (logout, step-up auth, disable features, alert SOC).

☐ **Option A — No-Code only** (shut down + redirect to configured URL)

☐ **Option B — Custom in-app handling** (developer implements threat callbacks)

☐ **Option C — Both** (No-Code first, then selected custom actions)

IF NO-CODE — REDIRECT URL TO DISPLAY

IF CUSTOM — DEV EFFORT AVAILABLE (PERSON-DAYS)

> SecureCentral recommendation: start with
> **Option A (No-Code)**
> to prove detection quickly with no code change, then layer custom handling for the two or three highest-risk threats.

9 **Can you leverage Zimperium's next-gen app protection by uploading your APK and Xcarchive with dSYM to the SaaS platform for protection?**

zShield protection is applied by uploading the compiled artefact to the Zimperium SaaS console. Android requires the ***APK/AAB*** *; iOS requires the* ***.xcarchive including dSYM*** *for symbolication and protection. If SaaS upload is blocked by policy, on-premises / self-hosted options must be discussed before kickoff.*

☐ Yes — SaaS upload approved ☐ Yes, but approval pending (owner / date below)

☐ No — data residency or policy restriction

ANDROID ARTEFACT AVAILABLE (APK / AAB) — Y/N	IOS .XCARCHIVE WITH DSYM AVAILABLE — Y/N

REQUIRED DATA RESIDENCY (E.G. AU, SG, EU, US)	APPROVER NAME & EXPECTED APPROVAL DATE

> **Blocker risk:**
> If artefacts cannot be uploaded, the zShield portion of the POC cannot proceed in standard form. Escalate to SecureCentral to evaluate alternative deployment models.

Qualification outcome

ASSESSMENT	RESULT
Compelling event confirmed	☐ Yes ☐ No
Technical feasibility confirmed	☐ Yes ☐ No ☐ Pending Zimperium confirmation
Budget & decision process identified	☐ Yes ☐ No
Resources committed by customer	☐ Yes ☐ No
POC recommendation	☐ Proceed ☐ Proceed with conditions ☐ Defer ☐ Decline

6 · Technical prerequisites checklist

All items must be **COMPLETE** before Step 1 begins. Owner "C" = Customer, "SC" = SecureCentral, "Z" = Zimperium.

✓	REF	PREREQUISITE	OWNER	STATUS / DATE
☐	PR-01	Mutual NDA executed between customer, SecureCentral and Zimperium	C / SC	
☐	PR-02	POC scope, success criteria and end date agreed and documented (Sections 2 & 12)	All	
☐	PR-03	Target application(s) identified and named	C	
☐	PR-04	Named resources assigned and committed (Section 4)	C	
☐	PR-05	Weekly sync scheduled with calendar invites issued	SC	
☐	PR-06	Zimperium console tenant provisioned; customer users invited and MFA enrolled	SC / Z	
☐	PR-07	POC evaluation licence keys issued	SC / Z	
☐	PR-08	Android build artefact available (unsigned or debug-signed APK/AAB)	C	
☐	PR-09	iOS `.xcarchive` including `dSYM` available	C	
☐	PR-10	Approval obtained to upload artefacts to the Zimperium SaaS platform (Q9)	C	
☐	PR-11	Signing certificates / provisioning profiles available to re-sign protected builds	C	
☐	PR-12	Build pipeline access or a documented manual build procedure	C	
☐	PR-13	Physical test devices ready: ≥1 clean + ≥1 rooted Android, ≥1 clean + ≥1 jailbroken iOS	C	
☐	PR-14	Network egress permitted from devices/build hosts to Zimperium cloud endpoints	C	
☐	PR-15	Test accounts / test data available in a non-production backend	C	
☐	PR-16	Threat & handling action matrix completed (Section 8)	C / SC	
☐	PR-17	No-Code redirect URL confirmed (if Option A or C selected in Q8)	C	
☐	PR-18	Change/security approval for installing an instrumented build on test devices	C	
☐	PR-19	Outsourced dev partner briefed and under NDA (if applicable — Q2)	C	
☐	PR-20	Forms A, B and C completed, signed and returned to SecureCentral	C / Reseller	

7 · POC test cases **PROVIDED BY SECURECENTRAL**

Standard MAPS validation set. Record result as Pass / Fail / N-A and attach evidence (screenshot, console event ID, log extract). Cases marked **OPTIONAL** apply only where the relevant module is in scope.

A · zScan — application vulnerability discovery

ID	TEST CASE	EXPECTED RESULT	RESULT	EVIDENCE
TC-01	Upload target binary to zScan and run a full scan	Scan completes; findings report generated		
TC-02	Review findings mapped to OWASP MASVS / MASTG categories	Findings categorised with severity, description and remediation guidance		
TC-03	Verify detection of hard-coded secrets / API keys in the binary	Embedded secrets identified with file and location context		
TC-04	Export report (PDF/JSON) and confirm CI/CD-consumable output	Report exports successfully; API/plugin integration demonstrated		

B · zShield — application hardening

ID	TEST CASE	EXPECTED RESULT	RESULT	EVIDENCE
TC-05	Upload APK/AAB and .xcarchive+dSYM; apply zShield protection	Protected artefact produced and downloadable		
TC-06	Re-sign, install and smoke-test the protected build	App installs and core user journeys function normally		
TC-07	Decompile / reverse-engineer protected vs unprotected build (e.g. jadx, Hopper)	Protected build shows obfuscated symbols and unreadable logic vs baseline		
TC-08	Attach a debugger to the protected app	Anti-debug triggers; app terminates or blocks attachment		
TC-09	Tamper with the binary and re-sign with a different key, then launch	Integrity check fails; app refuses to run		
TC-10	Measure app size delta and cold start-up delta vs baseline	Overhead within agreed threshold (record actual values)		
TC-11	Repeat protection step inside the customer build pipeline	Process is repeatable and automatable via CLI/API		

C · zDefend — runtime detection & response

ID	TEST CASE	EXPECTED RESULT	RESULT	EVIDENCE
TC-12	Embed zDefend SDK into target app and build successfully	Build succeeds; SDK initialises and app registers in console		
TC-13	Launch app on a **rooted** Android device	Root detected; configured handling action executes; event in console		
TC-14	Launch app on a **jailbroken** iOS device	Jailbreak detected; configured handling action executes; event in console		
TC-15	Run app on an emulator / simulator	Emulator detected and reported		
TC-16	Attach dynamic instrumentation / hooking framework (Frida, Xposed, Cydia Substrate)	Hooking detected; action executes; event in console		
TC-17	Attempt runtime debugging of the app	Debugger detected and reported		
TC-18	Install a known-malicious / risky test app on the device	Malware or risky app detected (device-scope detection)		
TC-19	Route traffic through a proxy with a rogue CA (MITM simulation)	MITM / untrusted certificate detected; action executes		
TC-20	Attempt screen capture / screen sharing while app is in the foreground	Screen sharing or overlay attack detected per policy		
TC-21	Install a repackaged / re-signed copy of the app	App integrity / repackaging violation detected		
TC-22	Trigger a threat with the device **offline** (airplane mode)	Detection and action occur on-device; event queued and synced on reconnect		
TC-23	**No-Code action test:** configure shut-down + redirect to a specified URL, then trigger root/jailbreak	App terminates and the device browser opens the configured URL — with no code change		
TC-24	**Custom action test:** implement an in-app callback (e.g. force logout, block feature) OPTIONAL	Custom handler fires on the threat event as specified in Section 8		
TC-25	Change threat policy in console and confirm dynamic update on device	Updated policy applies without an app rebuild or redeploy		
TC-26	Validate telemetry forwarding to SIEM/webhook OPTIONAL	Threat events delivered to the nominated endpoint in expected format		
TC-27	False-positive check: run the app normally on clean devices for the agreed period	No spurious threat events raised during normal use		

D · zKeyBox — key protection OPTIONAL

ID	TEST CASE	EXPECTED RESULT	RESULT	EVIDENCE
TC-28	Integrate zKeyBox and perform an encrypt/decrypt or sign operation	Cryptographic operation succeeds using white-box protected keys		
TC-29	Inspect memory and binary for key material during operation	No key material recoverable in the clear		

E · Console, reporting & operations

ID	TEST CASE	EXPECTED RESULT	RESULT	EVIDENCE
TC-30	Review the threat dashboard and per-event forensic detail	Events show device, OS, app version, threat type, severity and timestamp		
TC-31	Apply role-based access control for security vs engineering users	Roles enforce correct visibility and permissions		
TC-32	Generate an executive summary / compliance report for the POC period	Report generated and exportable for stakeholder review		

8 · Threat detection & handling action matrix

For each threat, record what is detected **today**, whether it is **in scope** for the POC, and the **required handling action**. Handling action key: **SD** = shut down · **SD+URL** = shut down and redirect to configured URL (No-Code) · **ALERT** = log/alert only · **LOGOUT** = force session termination · **RESTRICT** = disable sensitive features · **STEPUP** = require step-up authentication · **CUSTOM** = customer-defined in-app callback.

#	THREAT	DETECTED TODAY?	IN POC SCOPE	REQUIRED HANDLING ACTION	NOTES
1	**Rooting (Android)**	☐ Yes ☐ No	☐	e.g. SD+URL	
2	**Jailbreak (iOS)**	☐ Yes ☐ No	☐	e.g. SD+URL	
3	Hooking frameworks (Frida, Xposed, Substrate)	☐ Yes ☐ No	☐		
4	Debugger attachment	☐ Yes ☐ No	☐		
5	Emulator / simulator execution	☐ Yes ☐ No	☐		
6	App tampering / repackaging / cloning	☐ Yes ☐ No	☐		
7	Malware / risky apps on device	☐ Yes ☐ No	☐		
8	Man-in-the-middle / rogue certificate	☐ Yes ☐ No	☐		
9	Unsafe / rogue Wi-Fi network	☐ Yes ☐ No	☐		
10	Screen sharing / screen recording / overlay attacks	☐ Yes ☐ No	☐		
11	Accessibility-service abuse / remote access trojans	☐ Yes ☐ No	☐		
12	Keylogger / input capture	☐ Yes ☐ No	☐		
13	Developer options / USB debugging enabled	☐ Yes ☐ No	☐		
14	Out-of-date or unpatched OS	☐ Yes ☐ No	☐		
15	Phishing / malicious URL access	☐ Yes ☐ No	☐		
16	Other: _____	☐ Yes ☐ No	☐		

Worked example. Threat: *Rooting or Jailbreak detected* → Handling action: *Shut down the application and redirect the user to* `https://example.com/security-notice` → Implementation: **zDefend No-Code action**, configured in the console with no developer effort.

9 · Form A — End User (Customer) Details

Completed by the end-user organisation. Required for licence registration, deal registration and Zimperium POC approval.

A1 · Organisation

REGISTERED LEGAL ENTITY NAME

TRADING NAME (IF DIFFERENT)

COMPANY REGISTRATION NO. (ABN / ACN / UEN / NPWP / SSM)

INDUSTRY SECTOR

COUNTRY / COUNTRIES OF OPERATION

WEBSITE

EMPLOYEE COUNT

APPROX. MOBILE APP MONTHLY ACTIVE USERS

REGISTERED BUSINESS ADDRESS

A2 · Primary business contact

FULL NAME

JOB TITLE

BUSINESS EMAIL

MOBILE / PHONE

A3 · Technical contact (console & SDK access)

FULL NAME

JOB TITLE

BUSINESS EMAIL

MOBILE / PHONE

A4 · Security / compliance contact

FULL NAME

JOB TITLE

BUSINESS EMAIL

MOBILE / PHONE

A5 · Procurement & decision process

BUDGET OWNER / APPROVER

INDICATIVE BUDGET RANGE

TARGET DECISION DATE

PURCHASING ROUTE

Existing controls in place: ☐ MDM / UEM ☐ MTD ☐ WAF / API gateway ☐ SIEM / SOC ☐ Fraud platform ☐ None

COMPLIANCE DRIVERS (E.G. APRA CPS 234, ESSENTIAL EIGHT, MAS TRM, PCI DSS / MPOC, ISO 27001, PDPA, GDPR)

A6 · Declaration

I confirm the information provided is accurate, that I am authorised to request this evaluation on behalf of the organisation named above, and that evaluation software will be used solely for internal assessment during the agreed POC period in accordance with Zimperium's evaluation terms and SecureCentral's Terms & Conditions and Privacy Policy.

SIGNATURE	NAME & TITLE	DATE

10 · Form B — Application for Proof of Concept

B1 · Target application

APPLICATION NAME

CURRENT VERSION

ANDROID PACKAGE ID

IOS BUNDLE ID

APP TYPE (CONSUMER / EMPLOYEE / PARTNER)

SENSITIVE DATA HANDLED (PII, PAYMENTS, HEALTH, CREDENTIALS)

BRIEF DESCRIPTION OF THE APP AND ITS BUSINESS CRITICALITY

B2 · Technology profile LINKS TO Q3-Q5

ATTRIBUTE	CUSTOMER RESPONSE
Native or hybrid	☐ Native Android ☐ Native iOS ☐ Hybrid ☐ Mixed
Framework (if hybrid)	
Exact framework version (e.g. React Native v0.82)	
Platform focus	☐ Android ☐ iOS ☐ Both
Min / target Android API level	
Min iOS deployment target	
Build system & CI/CD tooling	
Third-party SDKs that may conflict (e.g. other RASP, obfuscators)	
Outsourced development? (Q2)	☐ No ☐ Yes — partner:

B3 · Modules requested

✓	MODULE	PURPOSE FOR THIS POC	PRIORITY
☐	**zScan**	App vulnerability & compliance scanning	☐ Must ☐ Should ☐ Could
☐	**zShield**	Binary hardening, obfuscation, anti-tamper	☐ Must ☐ Should ☐ Could
☐	**zDefend**	Runtime threat detection & response (RASP)	☐ Must ☐ Should ☐ Could
☐	**zKeyBox**	White-box cryptography / key protection	☐ Must ☐ Should ☐ Could

B4 · Handling action approach LINKS TO Q8

☐ **Option A** — No-Code only: shut down + redirect to URL ☐ **Option B** — Custom in-app handling ☐ **Option C** — Both

NO-CODE REDIRECT URL

CUSTOM ACTIONS REQUIRED (LIST)

B5 · SaaS artefact upload LINKS TO Q9

QUESTION	RESPONSE
Approval to upload APK/AAB to Zimperium SaaS	☐ Yes ☐ Pending ☐ No
Approval to upload .xcarchive incl. dSYM to Zimperium SaaS	☐ Yes ☐ Pending ☐ No
Data residency requirement	
Secure transfer method preferred	☐ Console upload ☐ API ☐ Other:

B6 · Drivers, scope and schedule

REASON FOR EVALUATION / COMPELLING EVENT (Q1)

URGENCY & REQUIRED COMPLETION DATE

TEST CASES: ☐ STANDARD SET (SECTION 7) ☐ STANDARD + ADDITIONS

SUCCESS CRITERIA THE CUSTOMER WILL MEASURE (SECTION 12)

REQUESTED START DATE

REQUESTED END DATE

WEEKLY SYNC DAY/TIME

B7 · Customer authorisation

CUSTOMER SIGNATURE

NAME & TITLE

DATE

B8 · SecureCentral use only

FIELD	ENTRY
POC reference number	SC-ZIM-POC-
Solutions Engineer assigned	
Account Manager	
Deal registration submitted to Zimperium (ID / date)	
Evaluation licence issued (date / expiry)	
Framework/version compatibility confirmed with vendor	☐ Yes ☐ No — date:
Approval decision	☐ Approved ☐ Approved with conditions ☐ Declined

11 · Form C — Reseller / Partner Details

Completed by the reseller or implementation partner sponsoring this opportunity. Required for deal registration, margin protection and POC resourcing. Leave blank if the opportunity is transacted directly with SecureCentral.

C1 · Reseller organisation

RESELLER LEGAL ENTITY NAME

COMPANY REGISTRATION NO. (ABN / UEN / NPWP / SSM)

COUNTRY / TERRITORY

WEBSITE

SECURECENTRAL PARTNER TIER

EXISTING PARTNER ID (IF ANY)

REGISTERED BUSINESS ADDRESS

C2 · Reseller contacts

SALES CONTACT — NAME & TITLE

SALES CONTACT — EMAIL & PHONE

TECHNICAL CONTACT — NAME & TITLE

TECHNICAL CONTACT — EMAIL & PHONE

C3 · Opportunity & deal registration

FIELD	ENTRY
End-user account name	
Opportunity owner at reseller	
Estimated licence quantity (apps / MAU)	
Estimated deal value & currency	
Expected close date	
Competing solutions being evaluated	
Deal registration status	☐ Submitted ☐ Approved ☐ Not yet submitted

C4 · Capability & POC involvement

☐ Zimperium sales accreditation held ☐ Zimperium technical accreditation held ☐ Mobile app development capability
☐ DevSecOps / CI-CD capability ☐ Managed security services / SOC ☐ Local first-line support capability

FIELD	ENTRY
Reseller resources committed to the POC	
Role in POC	☐ Lead ☐ Co-deliver with SecureCentral ☐ Observer
Post-POC services to be provided by reseller	
Training or enablement required from SecureCentral	

C5 · Reseller declaration

I confirm the details above are accurate, that this opportunity is genuine and that our organisation will comply with SecureCentral and Zimperium partner programme terms, including confidentiality and evaluation-software handling obligations.

RESELLER SIGNATURE	NAME & TITLE	DATE

12 · Success criteria, closure & sign-off

Agreed success criteria

REF	SUCCESS CRITERION	MEASURE / THRESHOLD	MET?
SC-01	zShield protection successfully applied and protected build runs correctly		☐ Y ☐ N
SC-02	Reverse engineering of the protected build demonstrably harder than baseline		☐ Y ☐ N
SC-03	zDefend detects all in-scope threats from the Section 8 matrix		☐ Y ☐ N
SC-04	Required handling actions execute correctly (No-Code and/or custom)		☐ Y ☐ N
SC-05	zScan findings reviewed and considered actionable by engineering		☐ Y ☐ N
SC-06	Size and performance overhead within agreed threshold		☐ Y ☐ N
SC-07	No material false positives during normal use		☐ Y ☐ N
SC-08	Integration effort acceptable and repeatable in the build pipeline		☐ Y ☐ N
SC-09	Console visibility and reporting meet security team requirements		☐ Y ☐ N
SC-10	Customer-specific criterion		☐ Y ☐ N

Closure checklist

✓	CLOSURE ACTIVITY	OWNER	DATE
☐	All test cases executed and evidence collected	SC / Customer	
☐	POC results report produced and issued	SecureCentral	
☐	Findings and open items reviewed with stakeholders	All	
☐	Executive read-out delivered	SecureCentral	
☐	Commercial proposal and licensing model issued	SC / Reseller	
☐	Production rollout plan and timeline drafted	All	
☐	Evaluation licences decommissioned or converted	SecureCentral	
☐	POC artefacts and test builds removed from devices	Customer	

POC outcome

☐ **Successful** — proceed to commercial proposal ☐ **Successful with conditions** — see notes

☐ **Extended** — revised end date recorded ☐ **Unsuccessful** — reasons documented

OUTCOME SUMMARY & AGREED NEXT STEPS

CUSTOMER — NAME, TITLE, DATE

SECURECENTRAL SE — NAME, DATE

RESELLER — NAME, DATE

13 · Appendix — glossary & contacts

Glossary

TERM	MEANING
MAPS	Mobile Application Protection Suite — Zimperium's app-security suite
RASP	Runtime Application Self-Protection
MTD	Mobile Threat Defense — device-side protection (complementary to MAPS)
No-Code action	Console-configured response (shut down + redirect to URL) requiring no development effort
dSYM	iOS debug symbol bundle required alongside the .xcarchive
MASVS / MASTG	OWASP Mobile Application Security Verification Standard / Testing Guide
Hooking	Runtime code manipulation via frameworks such as Frida or Xposed

Contact SecureCentral

SecureCentral Global Pty Ltd

A Pioneer Infotech Company · ISO/IEC 27001 certified
ACN 690 139 872 · ABN 45 690 139 872
Email: info@securecentral.com.au
Mobile: +61 424 135 693
Web: www.securecentral.com.au
Support portal: support.securecentral.net

Regional coverage

Australia · New Zealand · Singapore · Malaysia · Indonesia
12+ years in APAC distribution · 8 markets served

SecureCentral is an authorised value-added partner for Zimperium in Asia Pacific, providing solution consulting, POC delivery, localised enablement and regional first- and second-line managed support.

Zimperium, zScan, zShield, zKeyBox, zDefend and MAPS are trademarks of Zimperium, Inc. Module capabilities and test cases described here reflect SecureCentral's standard POC methodology; final scope is confirmed with Zimperium during Step 0.