

Ravindu Fernando

Application Security Consultant · Colombo, Sri Lanka · GMT+5:30

I assess how well your web, API and mobile applications are protected, show you exactly where the gaps are, and give you a prioritised plan to close them.

RAVINDUFERNANDO.PAGES.DEV



230+

applications onboarded to WAAP

5

enterprise security programmes delivered

6

areas covered in every assessment

4

markets: Sri Lanka, South Asia, GCC, APAC

01 / HOW I WORK

01 Assess

I audit your applications and the security capabilities you already have: edge, APIs, code, monitoring, mobile and governance. Evidence, not questionnaires.

02 Recommend

You get a prioritised plan: what to fix first, what it costs, what risk it removes, and what can wait.

03 Execute, case by case

If you want help delivering, I scope it case by case: the expertise and manpower it needs, the timeline, and who is best placed to do it — your team, a partner or Innov8's AppSec unit.

02 / WHAT EVERY ASSESSMENT COVERS

01 Edge & WAAP

Is hostile traffic stopped before it reaches your applications?

WAF / WAAP coverage and blocking mode · Bot and abuse controls · DDoS readiness · Origin exposure and bypass paths

03 Vulnerabilities & exposure

Are you fixing the weaknesses an attacker would actually use?

Scanner coverage and credentialed scanning · SAST / DAST in the pipeline · Prioritisation beyond CVSS (CTEM) · Time to remediate by owner

05 Mobile apps

Can your customer app defend itself on a device you do not control?

In-app protection and RASP · Anti-tamper and anti-hooking · OWASP MASVS-aligned testing · Runtime threat telemetry

02 API security

Do you know every API you expose, and who can call it?

API inventory and shadow APIs · Schema enforcement · Authentication and object-level authorisation · OWASP API Top 10 (2023)

04 Monitoring & visibility

Would your SOC see an application attack while it is happening?

Security log coverage · SIEM integration and pipeline health · Detections for application attacks · Alert ownership

06 Governance & maturity

Is application security owned, measured and funded?

Ownership and policy · OWASP SAMM v2 maturity score · NIST CSF 2.0 alignment · Roadmap and budget

AppSec maturity assessment	Scored baseline, gap analysis, 12–24 month roadmap, board summary	2–3 weeks	Fixed fee
Application architecture review	Threat model, control coverage map, prioritised fixes	1–3 weeks	Fixed fee
WAAP & API protection assessment	Coverage gaps, bypass paths, migration or tuning plan	2–4 weeks	Fixed fee
Mobile app security assessment	Mobile threat model, protection policy, MASVS test plan	1–2 weeks	Fixed fee
Exposure management (CTEM) assessment	Prioritisation model, validation approach, owner playbook, metrics	2–4 weeks	Fixed fee
Executive briefing or team workshop	Plain-language risk briefing or hands-on workshop	1/2–1 day	Fixed fee
Fractional AppSec advisor	Roadmap governance, vendor and design reviews, escalation support	Monthly	Retainer

04 / TRACK RECORD

112

APPLICATIONS
MIGRATED**Cloud WAAP migration at enterprise scale**

Banking · A leading Sri Lankan private bank · F5 Distributed Cloud. Moved roughly 112 web applications and APIs to cloud web application and API protection in waves, from monitoring to blocking.

120

APPLICATIONS
PROTECTED**WAAP, API security and advanced bot protection**

Manufacturing · A global apparel group headquartered in Sri Lanka · Imperva. Deployed web application, API and advanced bot protection across around 120 applications for a multinational manufacturing group.

T1

BANK VULNERABILITY
PROGRAMME**Vulnerability management modernisation**

Banking · A Tier-1 Sri Lankan commercial bank · Tenable Security Center. Upgraded the vulnerability management platform and deployed web application scanning to cover the application layer.

RASP

IN-APP PROTECTION
LIVE**Mobile application runtime protection**

Banking · A leading private bank's mobile app · Zimperium. Rolled out in-app protection for a customer banking app, tuning policies and supporting SDK integration with the bank's developers.

SIEM

TELEMETRY PIPELINE

WAAP security telemetry into the SOC

Banking · A leading Sri Lankan private bank · F5 > Logstash > Trellix SIEM. Integrated WAAP security logs into the bank's SIEM through Logstash and resolved pipeline backpressure so events arrive reliably.

05 / PLATFORMS DEPLOYED AND OPERATED IN PRODUCTION

F5 Distributed Cloud · Imperva · Zimperium · Veracode · Tenable · Qualys · RidgeBot · Datadog · Trellix · Logstash

06 / CURRENT ROLE

Head of the Application Security Business Unit, Innov8 (Pvt) Ltd

Consulting is independent and vendor-neutral. When implementation, licences or managed services are needed and Innov8 is the right fit, the BU can deliver; this is always disclosed.

Start with a free 30-minute call.

ravindufernando.pages.dev/contact · Colombo, Sri Lanka