



AI-Assisted Security Testing

Our vision for AI-assisted
cyber defence



What it is:

A solution to accelerate security testing through AI, guided by human expertise

**Application Security
& Penetration
Testing Teams**



**Technology /
Application Owners**



**CISOs / Security
Leaders**



Why it matters

Threat actors are using AI to exploit vulnerabilities faster. Traditional testing can be quick but limited, or thorough but costly. AI-assisted testing combines speed with human judgement to expand coverage, validate findings and help organisations act on material risks sooner.

**Detect more vulnerabilities, prioritise
material risks and remediate them faster.**

What it does: **Expand testing coverage and improve risk decisions**

Increase testing coverage

Assess more of the attack surface while specialists focus on complex risks.

Validate findings with greater confidence

Reduce false positives and prioritise risks by exploitability and business impact.

Test more frequently

Retest fixes, track remediation and see whether risk is reducing.

Benefits

- Faster identification of vulnerabilities
- Clear, business-relevant risk insights
- Greater confidence in remediation outcomes
- More specialist focus on risk judgement

How it works: Turn security testing into better risk decisions

Input

The tester defines authorised targets, testing boundaries and approval limits.

Action

AI uses approved testing tools within defined guardrails.

Output

Specialists receive evidence, reproduction steps and draft findings for validation.

Impact

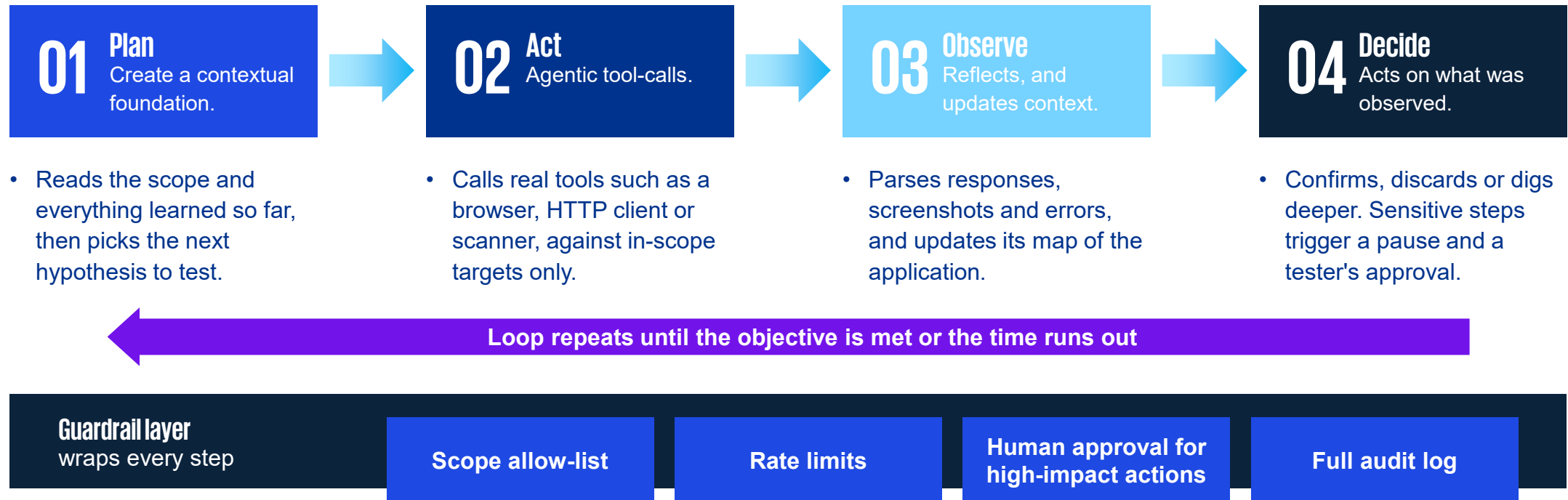
Focus on business impact, risk judgement and remediation priorities.

The screenshot displays a web-based interface for configuring a security test. It features a top navigation bar with tabs: Project, Asset, Instructions, Modules, Identities, and Rules & Launch. The main content area is divided into two primary sections: 'Step 2: Define Target Asset' and 'Step 4: Vulnerability Modules (19/19 Active)'. 'Step 2' includes a text input for 'Target Root URL' with a placeholder 'https://example.com or http://testasp.vulnweb.com/' and a 'New Target URL' button. 'Step 4' shows a grid of 12 vulnerability modules, each with a checkbox and a brief description. A 'Previous' button is located at the bottom left. A separate window in the foreground shows a table of results with columns for 'SEVERITY' and 'VULNERABILITY TITLE'.

SEVERITY	VULNERABILITY TITLE
CRITICAL	Unauthenticated Access to Secrets/Credentials Endpoint
CRITICAL	BFLA: /api/spawn allows unauthenticated remote command execution as root
CRITICAL	BFLA: /grpc/os.OsService/RunCommand allows unauthenticated remote command execution via gRPC
CRITICAL	Server-Side Template Injection (SSTI) in /api/render
CRITICAL	Remote Code Execution via dot Template Injection on /api/render
CRITICAL	XML External Entity (XXE) Injection — Arbitrary File Read via POST /api/metadata
CRITICAL	Database Connection String with Credentials Exposed via /api/config
CRITICAL	Sensitive File Disclosure — /etc/shadow Readable via XXE

How AI-assisted security testing works

A reasoning model plans the next step, calls specialised subagents, reads the result and decides again, all inside a scope the engagement lead defines.



How AI and security specialists work together

AI expands the testing coverage. Security specialists validate the findings and make the final risk decisions.



KPMG's approach: AI-powered testing, guided by specialists

We combine AI-powered scale with specialist judgement.

AI expands the speed and coverage of testing. Our specialists validate the findings, prioritise material risks and guide remediation.

AI-powered speed & scale

- Use AI to **accelerate reconnaissance, test-case generation, code analysis, and vulnerability discovery.**
- Test more assets and increase coverage across **applications, APIs, cloud and infrastructure.**

Risk-led intelligence

- Move beyond a list of vulnerabilities.
- Correlate findings with **business criticality, exploitability, regulatory exposure and potential impact** so leadership knows what needs attention first.

Human + AI expertise

- Combine **AI-driven testing with experienced security professionals** who validate findings, reduce false positives and provide context that automated tools cannot.

From finding to fixing

- Connect security testing directly to remediation.
- Provide **actionable recommendations, track remediation** and **use recurring testing** to demonstrate whether the **organisation's risk posture** is actually improving.

Stage1

Enable

...people to adopt Gen AI tools and build AI foundations to capture first wave of productivity

Stage2

Embed

...AI into workflows, products, services and value streams to deliver greater value

Stage3

Evolve

...business models and industry ecosystems with AI to re-define your company

Explore a more responsive security testing

Discover how AI can expand testing coverage, validate findings and accelerate risk-based action.

Consider a demo if your organisation is:

- Moving beyond annual or release-based testing
- Testing complex applications, workflows and access controls
- Improving how vulnerabilities are prioritised, remediated and retested

Request a demo to see AI-assisted security testing in action.



Gavan Kingdon

**Director, Cyber,
KPMG in Singapore**

gavankingdon@kpmg.com.sg



KPMG Services Pte. Ltd.

© 2026 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

General disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

Document Classification: KPMG Public