CISO CYBER
HUMAN + AI

COMPLIMENTARY GUIDE

USING AI TO ENHANCE PENETRATION TESTING

What to automate, what to keep human, and how to brief your board. A practical field guide from the analysts at CISO Cyber.

INTRODUCTION

THE ECONOMICS OF TESTING ARE UPSIDE DOWN

Attack surfaces have exploded, cloud, SaaS, APIs, identity and supply chain, but the classic penetration test has not kept up. A fixed number of consultant-days can only reach so far, so scope gets narrowed until the test fits the budget rather than the risk.

The result is a snapshot of a fraction of your environment, delivered weeks later in a PDF that few executives read. Meanwhile attackers automate reconnaissance across everything you own, continuously, and only need to be right once.

This guide sets out where AI genuinely helps, where human judgement stays essential, what the new economics look like, and the questions to put to any provider. It closes with a scoping checklist and a one-page board briefing you can use straight away.

01 · THE PROBLEM

WHY TRADITIONAL TESTING IS BREAKING

Testing on a fixed block of days forces a trade-off: narrow the scope, or blow the budget. Either way, whole parts of the estate go unlooked-at. Modern environments change weekly, so a point-in-time test is stale almost as soon as it lands.

Automated tooling alone is not the answer either. Scanners flag noise, miss business logic, and cannot chain small issues into the kind of real-world breach that actually matters to a board.

> **"The question isn't human or AI. It's how to put a machine's reach behind a specialist's judgement."**

02 · WHERE AI HELPS

THREE PLACES AI EARNS ITS KEEP

Used well, AI removes the grunt work that eats a tester's week, freeing specialists for the creative attacks that actually matter. Three areas deliver most of the value.

RECON	Map the full attack surface (assets, subdomains, exposed services, identities) in hours, not days, with nothing quietly left out of scope.
TRIAGE	Cluster and rank thousands of signals so analysts start with the findings most likely to be exploitable, instead of reading everything twice.
REPORTING	Draft clear, consistent write-ups with remediation steps, so human time goes into the finding rather than the formatting.

03 · WHERE HUMANS STAY ESSENTIAL

MACHINES FLAG. SPECIALISTS EXPLOIT.

AI is a force multiplier, not a replacement. Chaining flaws into a real breach, understanding what a finding means for your business, and standing behind the result: that stays human.

The creative leap from "this looks odd" to "here is how I would own your domain" is exactly where experienced red-teamers earn their keep, and where black-box automation quietly fails. Accountable sign-off by a named senior analyst is the difference between a report and a rubber stamp.

04 · THE ECONOMICS

BROADER COVERAGE, FASTER, FOR LESS

When AI absorbs recon, triage and drafting, a senior analyst's hours go where they are worth most. You get wider coverage and faster turnaround, at a lower price than a traditional test.

TRADITIONAL

Fixed days. Narrowed scope. A snapshot in time. Report weeks later.

HUMAN + AI

Full coverage. Findings in hours. A continuous option. Around 30% lower cost.

3×	<2h	30%
ATTACK SURFACE COVERED	TO FIRST VALIDATED FINDING	LOWER COST, TYPICAL

05 · CHOOSING A PROVIDER

FIVE QUESTIONS TO ASK

1. Which parts are automated, and which are done by a named senior analyst?
2. Where does our data go, and is it kept sovereign in Australia?
3. Do findings come with remediation guidance and a free retest?
4. Can testing run continuously, or is it still a once-a-year snapshot?
5. Will the report make sense to both engineers and the board?

WORKSHEET

PROVIDER SCOPING CHECKLIST

Take this to your next provider conversation. Tick what they can evidence, not just what they claim.

- ☐ **Named senior lead.** A specific, accredited analyst is accountable for the engagement and signs the report.
- ☐ **Full asset coverage.** External, internal, cloud, web, API and identity are all in scope, or the exclusions are stated in writing.
- ☐ **Sovereign data handling.** Test data and findings stay onshore in Australia, with clear retention and deletion terms.
- ☐ **Manual exploitation.** Findings are validated by hand, not just scanner output, with proof of exploitability.
- ☐ **Remediation and retest.** Every finding carries fix guidance, and a retest of fixes is included, not billed again.
- ☐ **Two-audience reporting.** One report that engineers can act on and a board can understand.
- ☐ **Continuous option.** Testing can move from a yearly snapshot to always-on coverage if you want it.
- ☐ **Fixed, transparent price.** Scope, timing and cost are agreed up front, with no surprise line items.

ONE-PAGER

BRIEFING YOUR BOARD

Four lines to open the conversation, and the numbers that back them up.

Our coverage is partial.
Fixed-day testing leaves parts of the estate unexamined between engagements.

Attackers are already automated.
They probe continuously; an annual snapshot cannot keep pace.

Human + AI closes the gap.
Machine reach for coverage, senior judgement for the findings that matter.

It costs less, not more.
Wider coverage and faster results, at around 30% below a traditional test.

BOOK A PEN TEST ASSESSMENT

SEE IT ON YOUR OWN SYSTEMS

Fixed scope, senior analysts, AI-accelerated coverage, board-ready results. We respond within one business day.

EMAIL
hello@cisocyber.com.au

PHONE
1300 CISO AU

OFFICES
Sydney · Melbourne · Canberra