

Managed Autonomous Pentesting (MAP)

Built to run quietly and continuously



The Problem

Too many tools. Too much noise.

Your team spends more time chasing alerts than fixing what matters.



The Shift

This is not a scanner.

Not a red team.

It works quietly in the background, surfacing only what's real.

What it Covers

We simulate real-world attacks across your web apps, APIs, endpoints, and exposed infrastructure. The system goes deeper than scanning: it tests for supply chain threats, targeted phishing over Teams as well as Slack, and impersonation attempts across dark and open web sources.

What Makes It Different



Real risk only.
No false positives.



Continuous coverage
across your stack.



Starts instantly. No
tuning or project cycles.



No extra headcount
or tools needed.



Human support when
context matters.

How it works

Deploy ➤ Simulate ➤ Validate ➤ Report

What you get

Only validated, exploitable risk, no alert fatigue, no noise. Testing runs continuously, with zero impact on your team. No scheduling. No headcount needed. When you need support, our team is ready.