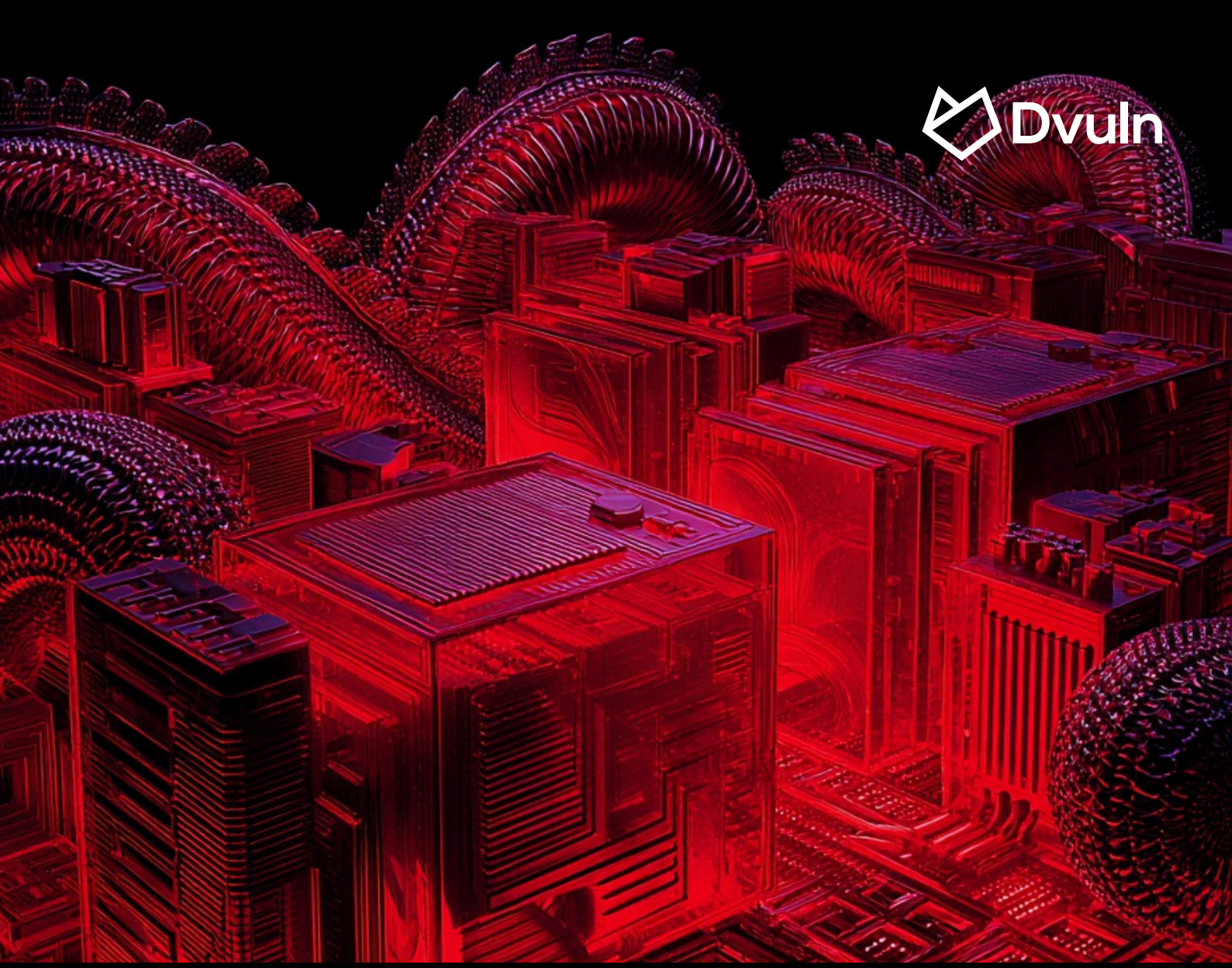

Adversary Simulation Service

Unfair Advantage, Simulated.

See what yourenvironmentlookslikethroughtheeyes of a real threat actor.

dvuln.com

What is an Adversary Simulation?

Dvulnadversarysimulationsemulate real attackerbehaviour - notjust exploits, but mindset, tradecraft, and persistence. Our operators don’t test tools. We test assumptions.

We target your business the way an actual criminal gang would

- External compromise, lateral movement, privilege abuse
- Broken MFA flows, social engineering, business process attacks
- Abuse of cloud misconfigurations, identity trust boundaries, and vendor relationships

You don’t just find weaknesses. You see the full narrative - what the attacker would do, how far they'd get, and how your people, tools, and processes would respond.

Why Organisations Use Adversary Simulations

Organisations engage Dvuln for adversary simulation when they need to:

- Validate XDR/SIEM effectiveness
- Test detection and escalation pathways
- Build realistic incident response capability
- Provide board-level assurance and visibility
- Meet uplift requirements for APRA CPS 234, Essential Eight, ISO 27001

What You Get

Each Dvuln simulation includes the following deliverables:

- Executive Summary for Leadership
- Technical Kill Chain Narrative
- Gaps in Telemetry & Response
- ATT&CK TTP Mapping
- Prioritised Remediation Plan
- Optional Purple Team & Tabletop Follow-up

Sample objectives

Compromise Core Banking Functionality via Compromised Banking Customer

Compromise National Point-of-Sales Network to Deploy Ransomware

Adversary Simulation vs. Penetration Testing

Penetration testing plays an important role in identifying technical vulnerabilities. But in high-stakes environments where reputation, financial systems, and regulatory outcomes are on the line, it is no longer sufficient.

Aspect	Penetration Testing	Adversary Simulation
Objective	Find and report technical vulnerabilities	Emulate real attacker objectives and pathways
Scope	Narrow, predefined (e.g., IP ranges, apps)	Full-spectrum (external, internal, process-level)
Met hodology	Checklist-driven (e.g., OWASP, CVE scanning)	Threat actor tradecraft (TTPs, evasion, persistence)
Detection Testing	Not typically in scope	Tests XDR, SIEM, SOC visibility and response
People & Process Coverage	Focused on technology	Includes staff, vendors, processes, physical access
Value to Executives	Compliance evidence	Realistic security narrative and decision-making insights
End State	Exploit proof-of-concept	Goal-oriented simulation (data access, lateral movement, fraud)

Case Study

Ransomware Attack on a Global Retailer

The target

A national retail chain with thousands of staff, centralised IT operations, and a high-value point-of-sale (POS) network spanning hundreds of locations. The environment included M365, Entra ID, third-party contractors, and multiple service integration platforms.

The goal

Simulate the pathways a ransomware group might take to disrupt sales operations nationally with a focus on POS compromise, identity abuse, and lateral movement through high-trust systems. The objective was to understand how quickly an attacker could move from external access to full-scale business disruption.

The attack process

Dvuln executed a staged adversary simulation mimicking real ransomware operator behaviour:

- Performed reconnaissance using legitimate marketing and enrichment tools to identify staff roles, exposed services, and vendor relationships
- Bypassed the client's enterprise identity and MFA system, using phishing and token theft to gain internal foothold
- Enumerated and mined internal fileshares for sensitive documentation, stored credentials, and onboarding packs
- Compromised the contractor portal and the corporate service desk, enabling privilege escalation and visibility into real-time ticket flows
- Masqueraded as internal support, interacting with employees across multiple sites using insider language and knowledge of active incidents
- Used this trust to pivot into the POS infrastructure, gaining physical and logical access to store networks across the country
-
-

Case Study

Ransomware Attack on a Global Retailer

The Results

The simulation demonstrated how a ransomware operator could chain together identity abuse, vendor impersonation, and business process gaps to cripple national sales operations. As a result, the client:

- Introduced segmentation and containment controls between corporate IT and retail networks
  Hardened service desk workflows with multi-factor escalation, caller validation,
- and endpoint context awareness
  Refactored contractor system access to enforce least privilege and session expiry
- Delivered clear, high-impact risk narratives to board and executive stakeholders, directly informing budget allocation and roadmap planning
-

Why Dvuln?

Dvuln

We Don’t Play Defence. We Simulate the Offence.
Dvuln is not a generic testing firm. We simulate the behaviour, mindset, and tradecraft of real adversaries - at the standard required by banks, casinos, and government.
Our work has exposed gaps in environments already passed by auditors and other providers.
We aren’t brought in to tick boxes. We’re brought in when the risk is real and failure is not an option.

CREST
SECUR ITY
TEST ING

OFFENSIVE security
OSCP

9NEWS

FINANCIAL REVIEW

The Sydney Morning Herald
INDEPENDENT. ALWAYS.

7NEWS

Daily Mail Australia