

Every platform tests. Few teach in sequence.

Ten of the twenty platforms test staff by email only, with no SMS, voice or QR code lures. Where they differ most is how they teach: three run a structured curriculum.

THE FOUR JOBS

01	ADVANCED	
SIMULATE	Deepfakes of your own executives	4 of 20
02	TABLESTAKES	
REPORT	A report button in the inbox	20 of 20
03	ADVANCED WIDEST GAP	
TRAIN	A structured curriculum, taught in order	3 of 20
04	ADVANCED	
ALERT	Alerts when staff credentials appear in a breach	4 of 20

20
platforms assessed

380+
vendor-stated features

37
capabilities scored

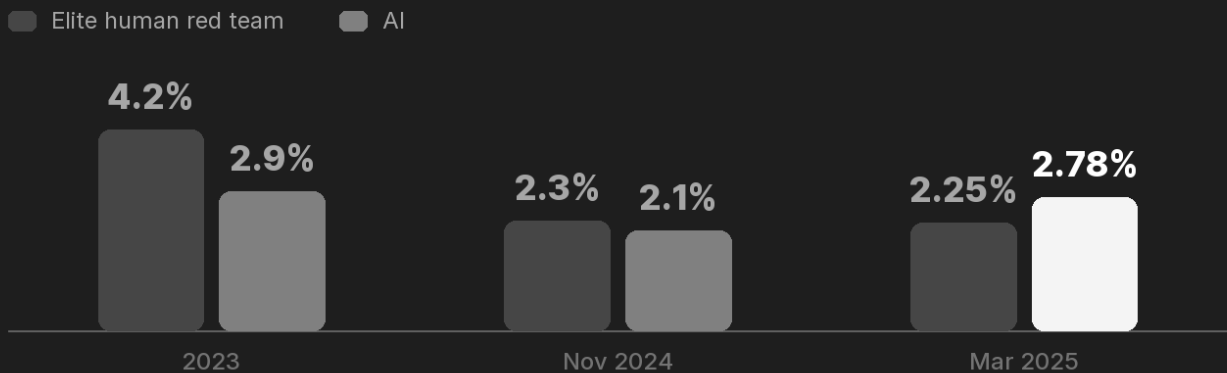
PROVENANCE

Edition 2026.1, data as at 1 October 2026. Twenty platforms assessed against 380+ vendor-stated features, normalised to 37 scored capabilities. Each job is represented by one capability rather than by the job as a whole, labelled with that capability's maturity tier; the highlighted job is the one whose capability the fewest of the twenty are credited with. The article's threat context is contributed by Parabellum, CREST-accredited offensive security specialists; the product analysis is Tekspace's own. The scoring model is on page 08.

THE LURE

In 2025, AI wrote better phishing than human experts.

SIMULATED PHISHING CLICK RATE



In one training vendor's simulations, phishing written by AI drew 31 per cent fewer clicks than its elite human red team in 2023. By March 2025 it drew 24 per cent more.

Read it for direction, not scale: these are simulated campaigns measured by click rate, run by a single vendor.

Four of the twenty platforms assessed here are credited with AI spear phishing personalisation, which builds simulations from your own org chart, names and suppliers.

The lure is now tailored by a machine. Ask whether your simulations are.

SOURCES

Click rates are Hoxhunt's published failure rates for simulations written by its elite human red team and by AI: in 2023 single-prompt AI across 2.5 million people; in November 2024 and March 2025 an AI agent, 70,000 simulations each. Source: Hoxhunt, "AI-Powered Phishing Outperforms Elite Cybercriminals in 2025", 3 April 2025. Hoxhunt is one of the 20 platforms in this assessment; its research is cited for the trend, not as an endorsement. Platform count: Tekspace Research assessment, 2026, 4 of 20 credited.

REASONABLE STEPS

After a breach, training becomes evidence.

The Privacy Act requires every organisation holding personal information to take reasonable steps to protect it. The regulator's own guidance counts staff training among those steps, and is specific about what that training should cover.

WHAT THE GUIDANCE ASKS OF TRAINING

"Does training cover recognising and avoiding 'phishing' and 'spear phishing' attacks and 'social engineering'?"

OAIC

"Is refresher training provided to your staff and does this occur on a regular basis?"

OAIC

"Tracking training undertaken and testing the understanding of relevant information security policies, both on commencement and periodically."

APRA CPG 234

"Had not seen, used, or received training on the playbooks provided and had no formal cybersecurity background or incident response training."

The Federal Court on the IT team leader in the Australian Clinical Labs breach, part of its finding that reasonable steps were not taken. The penalty, \$5.8M, was the first ever ordered under the Privacy Act.

A completion record shows that training happened. It does not show that it worked.

The next pages show which platform capabilities produce the second kind of record, and how many of the twenty hold each one.

SOURCES

Reasonable steps: Privacy Act 1988, APP 11.1. OAIC, Guide to securing personal information, "Governance, culture and training". APRA CPG 234 Information Security (June 2019), Attachment B, is guidance for APRA-regulated entities; the standard, CPS 234, does not itself mention training. Court: Australian Information Commissioner v Australian Clinical Labs Limited (No 2) [2025] FCA 1224 at [53], 8 October 2025. Penalty: OAIC media release, 9 October 2025, \$4.2M for failing to protect personal information and \$1.6M for assessment and notification failures. Not legal advice.

AI-Generated Simulation Content		20 of 20
Content Library		20 of 20
Continuous Assessment		20 of 20
In-Email Report Button		20 of 20
Interactive Training Modules		20 of 20
Performance Reporting		20 of 20
Phishing Simulation		20 of 20
Platform Customisation		20 of 20
Security Baselineing		20 of 20
Gamification		19 of 20
White-Label Branding		19 of 20
Behavioural Risk Scoring		18 of 20

put a report button in the inbox.

TEKSPACE.COM.AU/LAB • 04 / 10

Advanced Analytics & Dashboards		17 of 20
Single Sign-On		15 of 20
Adaptive Learning Engine		13 of 20
REST API Access		11 of 20
LMS & Third-Party Integration		9 of 20
Multilingual Content		9 of 20
Smishing Simulation		8 of 20
Multi-Tenant Management		7 of 20
Policy & Compliance Management		7 of 20
SIEM Integration		5 of 20

TEKSPACE.COM.AU/LAB • 05 / 10

[illegible]

FOR YOUR SHORTLIST

Questions that split the shortlist.

Six questions, each testing a capability that no more than six of the twenty platforms are credited with. Ask to see each one working, not listed.

01	Show me the curriculum a new starter follows, level by level. Tests: Structured Learning Paths	3 of 20
02	Does a click change the next simulation, with no admin? Tests: Automated Risk-Based Simulations	3 of 20
03	Can you build lures from our org chart and supplier names? Tests: AI-Powered Spear Phishing Personalisation	4 of 20
04	Where is our people's data stored? Can it be Australia? Tests: Data Sovereignty	4 of 20
05	Can reported phish and risk scores flow into our SIEM? Tests: SIEM Integration	5 of 20
06	Can you simulate a phone call, not just an email? Tests: Vishing Simulation	6 of 20

The comparison shows how the top four answer each one.

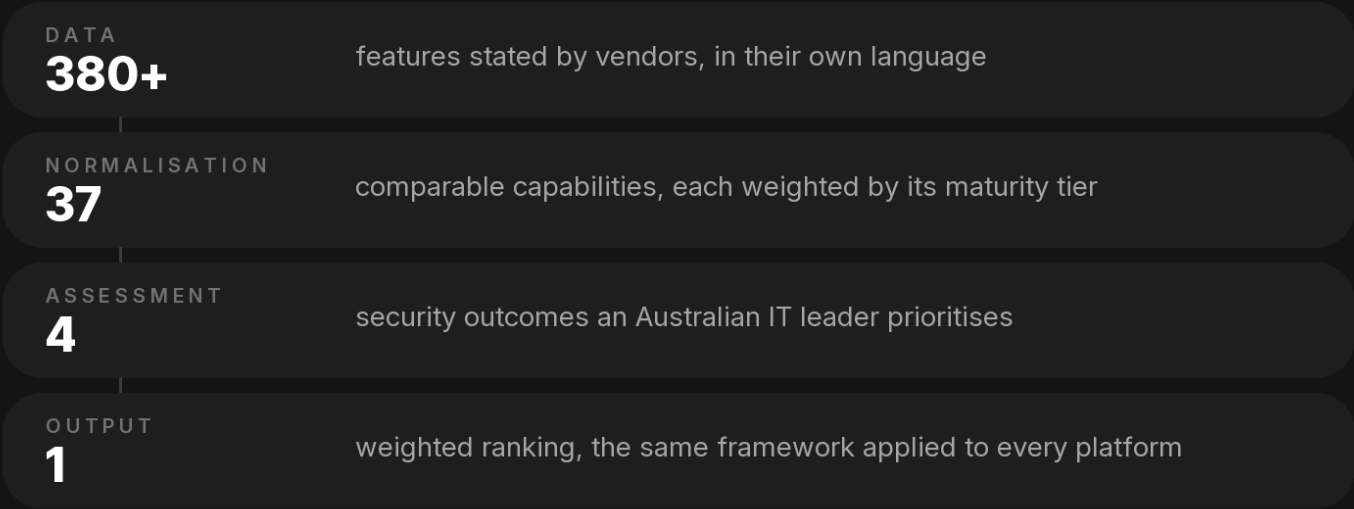
BASIS

Each question is Tekspace's framing of one scored capability, named beneath it exactly as it appears on pages 04 to 06. The count is how many of the twenty assessed platforms are credited with that capability. A platform that is not credited may still offer something similar that its documentation does not state.

HOW WE ASSESSED IT

Hundreds of claims,
thirty-seven capabilities.

Vendors name the same function in different words. Normalising what each one states into one shared list is what makes a like-for-like comparison possible at all.



THE FOUR OUTCOMES



THE THREE MATURITY TIERS

Tablestakes	expected of any platform in the category	12 · held by 18 to 20 of 20
Common	separates the middle of the market	10 · held by 5 to 17 of 20
Advanced	held by few; where platforms differ most	15 · held by 2 to 7 of 20

A platform is a tool. The program that changes behaviour around it is still yours to build.

BASIS

380+ is the count of features in the 20 platforms' enriched feature lists (389 rows) before normalisation; 37 is the scored capability set that remains after merging and de-duplication. Weighting is 12 capabilities at 1.0, 10 capabilities at 1.5, 15 capabilities at 2.5, which gives the framework maximum of 64.5. Tiers follow how many platforms hold a capability, with documented editorial overrides where the quality gap between holders matters, which is why the holder ranges overlap. Held means credited from vendor documentation, not audited.

THE 2026 RANKING

Who leads, by how much, and why.

The twenty, in the article’s rank order. The comparison gives every score, the margin between each, and what puts the top four in front.

	RANK	PLATFORM	IN THE COMPARISON	SCORE
COMPREHENSIVE	1	KnowBe4	Score, margin, 37 capabilities, head to head	
	2	Phished	Score, margin, 37 capabilities, head to head	
	3	Adaptive Security	Score, margin, 37 capabilities	
	4	Hoxhunt	Score, margin, 37 capabilities	
BROAD	5	Proofpoint ZenGuide	Score and margin	
	6	SoSafe	Score and margin	
	7	Immersive Labs	Score and margin	
	8	Barracuda Security Awareness Training	Score and margin	
	9	Infosec Infosec IQ	Score and margin	
	10	MetaCompliance	Score and margin	
	11	NINJIO	Score and margin	
	12	SANS Institute Security Awareness	Score and margin	
	13	usecure	Score and margin	
	14	Huntress Managed SAT	Score and margin	
FOCUSED	15	Mimecast Engage	Score and margin	
	16	Riot	Score and margin	
	17	Boxphish	Score and margin	
	18	CyberHoot	Score and margin	
	19	ID Agent BullPhish ID	Score and margin	
	20	Perallis Security Hacker Rangers	Score and margin	

13 of 15

advanced capabilities are held by at least one of the top four.

3 at most

advanced capabilities held by any platform below the top four.

Get the comparison

Details on the next page.

BASIS

Ranked by weighted capability score against a framework maximum of 64.5; scores are withheld from this public version. Ranks 11 and 12 share a score; their order follows the article. Company is shown first, then the product assessed where it has its own name. Brackets mark the article’s Tekspace Cyber Continuum tiers.

THE 2026 COMPARISON

See them side by side.

The public research shows the shape of the category. The comparison puts the platforms side by side: exact scores, the gaps between them, and the capabilities that make the difference.

WHAT IS IN THE COMPARISON

01

Exact scores and gaps

Every platform's weighted score, and the distance to the one ranked above it.

02

What each score is made of

Each score split into tablestakes, common and advanced, so close totals can be told apart.

03

The top four, capability by capability

All 37 capabilities for the four highest-ranked platforms, one tier to a page.

04

The top two, head to head

What each holds that the other does not, and exactly what those capabilities are worth.

20 platforms | 380+ vendor-stated features | 37 normalised capabilities | weighted scoring model

GO TO

tekspace.com.au/lab/security-awareness-training/compare

Get the comparison

Business email. The comparison opens straight away.

DISCLOSURE

The article's threat context is contributed by Parabellum, CREST-accredited offensive security specialists; the threat pages in this document and the product analysis are Tekspace's own. Tekspace maintains commercial relationships with vendors across the cybersecurity industry. These relationships do not influence the research methodology, vendor scoring or maturity tier placement documented in this assessment. All assessments reflect Tekspace's independent professional judgement based on hands-on evaluation and structured product research. This document does not constitute professional advice; organisations should conduct their own due diligence appropriate to their requirements, risk profile and regulatory obligations.