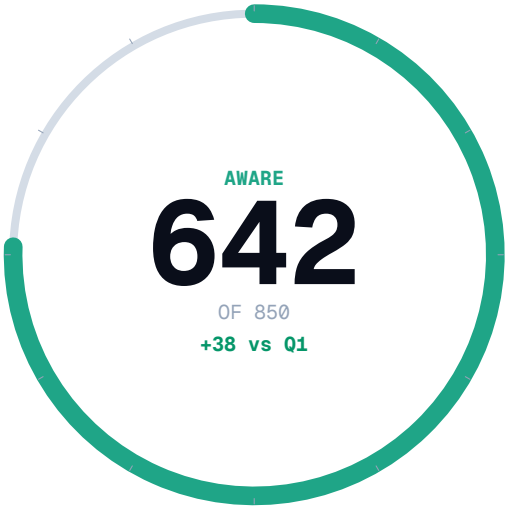
// Q2 2026 · SCORECARD

Apex Logistics — Cyber IQ

47 players across 5 departments. AWARE band, +38 since baseline. Phishing is the dominant weakness — fix it and the org clears GUARDIAN by Q3.

// EXECUTIVE TAKEAWAY

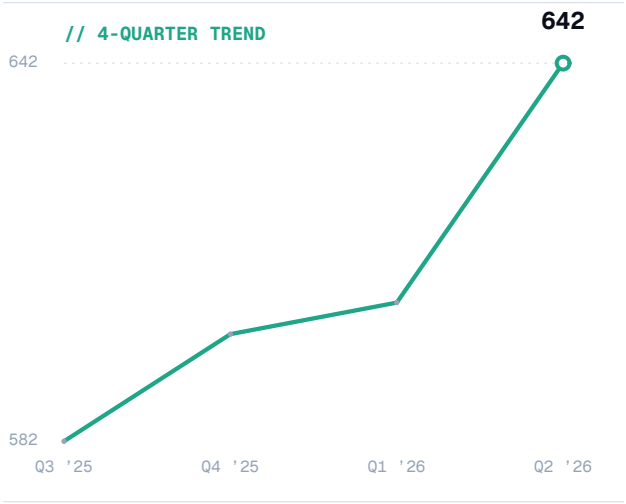
The number is moving in the right direction. Customer Success and Finance drag the org score; targeted phishing replay for those two depts unlocks ~50 score-points.



38
DELTA VS Q1

47
PLAYERS ACTIVE

89%
ENGAGEMENT



// TIER POSITION

// DEPARTMENT BREAKDOWN

DEPARTMENT	PLAYERS	SCORE	TIER LADDER	WEAKEST DOMAIN
Operations	14	612		Phishing −12 pts
Sales	11	688		Insider risk −6 pts
Engineering	9	721		APT awareness −4 pts
Customer Success	8	554		Phishing −22 pts
Finance	5	595		Ransomware −18 pts

// THREAT INTELLIGENCE

Threat-domain heatmap

Per-domain accuracy by department. Cells under 60% in amber; under 45% in red. Bold cells flag the priority interventions on page 3.

THREAT DOMAIN	OPERATIONS	SALES	ENGINEERING	CUST. SUCCESS	FINANCE
Phishing	62%	78%	84%	41%	58%
Ransomware	71%	82%	88%	64%	47%
Insider risk	69%	74%	91%	68%	70%
Malware/APT	74%	71%	87%	59%	66%
Spam / scam	85%	88%	94%	78%	80%

// TOP 3 WEAK SPOTS

#	DEPARTMENT	DOMAIN	SCORE	RISK PROFILE
1	Customer Success	Phishing	41%	**HIGH** · public-facing role · external email volume
2	Finance	Ransomware	47%	**HIGH** · financial system access · macro-laden documents
3	Customer Success	Malware/APT	59%	**MED** · frequent file attachments from prospects

// SIGNAL QUALITY

0.71 means 71% of correct answers landed in < 8 seconds across at least three sessions per player. High-confidence answers weight **1.4×** toward the org Cyber IQ Score; guess-and-check answers weight **0.6×**. The index is the truest read on whether your team is *recognising* threats versus pattern-matching the test format. Apex moved up **+0.09** this quarter as players logged repeat sessions across different threat categories.

// PLAYBOOK

Recommended actions

Three priority items mapped directly to this quarter's heatmap. Each one indexed to CIS Controls v8 + NIST CSF subcategories so it drops cleanly into your existing security programme.

#	ACTION	OWNER	ETA	MAPS TO
1	**Targeted phishing replay for Customer Success.** Five simulated phishing variants, weekly cadence over 6 weeks. Pair each with a manager-led debrief reviewing the missed cues — visual, copy, sender-domain.	**CS Lead + Sec. team**	WEEK 1	CIS 14.1 NIST PR.AT-2
2	**Finance ransomware tabletop.** Quarterly drill covering macro execution from inbound invoices. Update policy on attachment handling for AP team — disable macros on AP mailboxes by default.	**Finance Dir + CISO**	WEEK 3	CIS 10.2 NIST PR.IP-9
3	**Cross-dept manager-led replay.** Top 5 missed questions from the heatmap surfaced as Slack flashcards. Drives Cyber IQ uplift without scheduled meetings — managers nominate the format that fits their team's cadence.	**All managers**	WEEK 2	CIS 14.3 NIST PR.AT-1

// COMPLIANCE MAPPING

FRAMEWORK	COVERAGE	BAR	EVIDENCE IN THIS DEBRIEF
CIS Controls v8	3 of 18 controls		Heatmap + per-dept accuracy
NIST CSF	PR.AT-1, PR.AT-2, PR.IP-9		Per-domain quiz outcomes
ISO 27001 (Ent)	A.6.3, A.7.2.2		Tier scale + dept rollup
NIS2 (Ent)	Art. 21(2)(g)		Threat-awareness baseline

// EXPORT & INTEGRATIONS **Pro**: CSV export of every column above at cyberiq.cc/reports. PDF ships with this exact format. **Enterprise**: KnowBe4 / Proofpoint live API + webhooks; ISO 27001 + NIS2 evidence packs auto-generated quarterly.

Want this for your team?

Free for 5 players → **cyberiq.cc/games** · Reserve 14-day Pro trial · launches 1 June 2026 → **cyberiq.cc/login?intent=trial**

Methodology: *Cyber IQ is a 300–850 score derived from per-domain accuracy (weighted 0.45), confidence index (0.30), bonus objectives (0.15), and historical trend (0.10). Domain weights apply 90-day recency decay. Source data: every game session, every quiz answer. Full methodology + replication SQL at cyberiq.cc/methodology.*