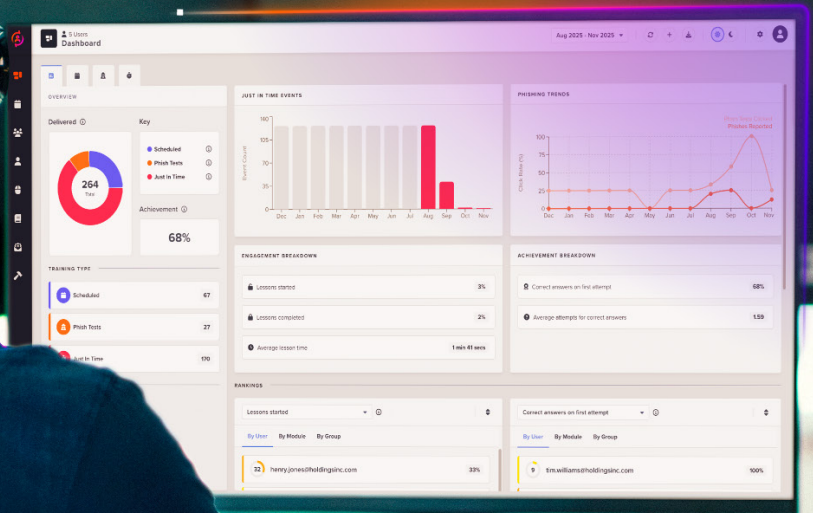


DARKTRACE

Why Security Awareness Training is Broken

...and how to fix it



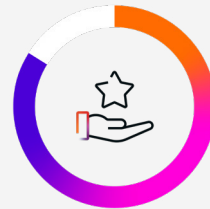
At a glance

Humans sit on the front line of organizational defense, yet the security awareness training (SAT) that employees receive is measured by completion rather than behavior change.

As a result, training doesn't translate to retention or real-world decision-making – it's a check-box exercise.

This eBook outlines a strategic shift from static, one-size-fits-all training to adaptive human defense: a feedback-loop approach that unifies user awareness and real-time protection.

By aligning coaching to live user behavior and measurable risk, organizations can strengthen resilience, protect productivity, and turn their workforce into a dynamic layer of defense.



84% of organizations measure SAT success through completion rates

(NIST Awareness Effectiveness Study, Forrester 2025)



<2% Improvement on failure rates after standard phishing training

UCSD (2025). Understanding the Efficacy of Phishing Training in Practice. Proceedings of the 2025 IEEE Symposium on Security and Privacy.

Why traditional security awareness training doesn't work

Why are we here?

If training worked, the fallout from behavior-related risk would be declining. **It isn't.**



Billions spent annually on security awareness
~\$7B market and growing



Reported losses continue to skyrocket
average cost of a breach
\$4.4M in 2025



AI-powered scams are accelerating
97% of organizations reporting
AI-related security incidents



Phishing, social engineering, and human error remain top breach drivers
Human element involved
in 68% of data breaches

Why isn't it working?

01 IT'S DESIGNED TO CHECK A BOX



Annual or quarterly sessions



Completion rates
= "success"



Optimized for audit defensibility,
not behavior change



Training data never feeds
back into security controls

02 IT DOESN'T REFLECT THE REALITY OF THREATS



Unrealistic, "defanged"
phishing simulations



Based on threats already
blocked by email filters



No exposure to personalized,
AI-driven, cross-channel attacks

03 IT BLAMES USERS



Measures failure
more than progress



Punishes mistakes instead
of reinforcing learning



Little or no support to improve
response in the moment of risk



Positions people as liabilities,
not as a critical layer of defense

04 IT CAN'T PROVE IMPACT



Click rates
≠ risk reduction



Coaching stays static
even as risk signals change



Defenses don't adapt based on
who clicks, reports, or struggles



ROI?
Unclear at best.

It's time for a different model

The shift from compliance training to human defense

The new era of human defense is built on a feedback loop: performance, learning, and strategy continuously informing one another.



01 Human performance

Goal: Measurable reduction in human-driven security incidents while capturing behavioral data to drive smarter coaching and appropriate controls.



02 Human learning & skill building

Goal: Build progressive capabilities that convert users from passive participants into security ambassadors that actively strengthen security posture.



03 Strategy & visibility

Goal: Convert human risk into a managed, quantifiable business risk, enabling leaders to prioritize defense investments and reduce exposure.

TRADITIONAL SAT

Annual	✗
Generic	✗
Reactive	✗
Siloed	✗
Ineffective measurement	✗

ADAPTIVE HUMAN DEFENSE

Continuous	✓
Realistic	✓
Personalized	✓
Measurable	✓
Integrated	✓

Intelligent learning vs. check-box training

The bottom line? Static, compliance-focused programs don't reduce real-world risk.

What's needed

Continuous, adaptive, behavior-driven learning, based around:



01 Live email analysis

Behavioral modeling of all communication in real time
Signals: tone, relationships, anomalies, authentication, routing patterns



02 Training & simulations

Real-time coaching triggered by risky user actions
Simulations adapt to real threats and user behavior



03 Awareness activity metrics

Track engagement, risk, and behavior—not just completion
Insights build dynamic user risk profiles



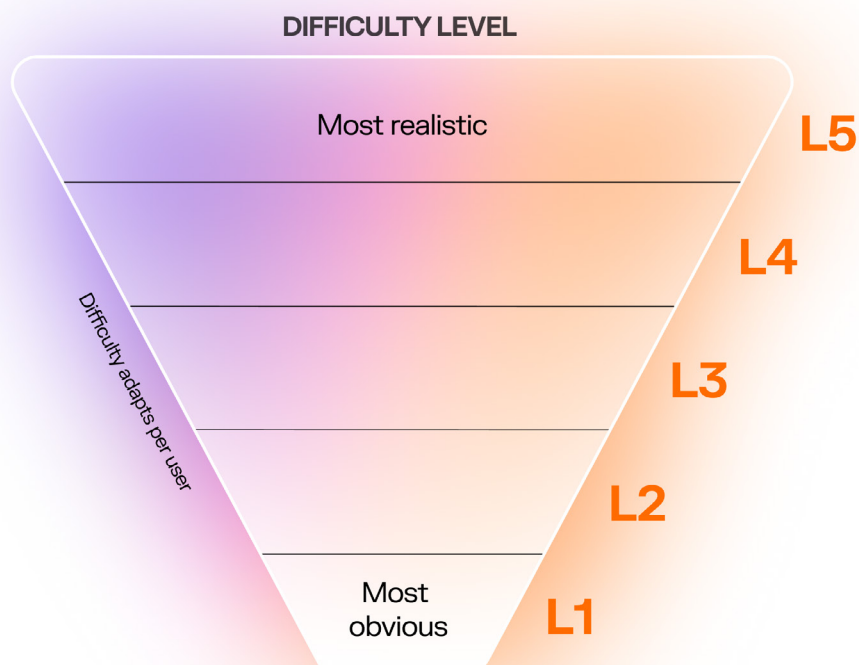
04 Context-based inbox actions

Protections adapt based on individual user risk
Reduces noise, improves prioritization, strengthens response



Realistic simulations that transfer to real-world learning

To actually build skills, phishing simulations should evolve from low to high difficulty:



What's needed

1. Realistic phishing simulations



AI-generated phishing scenarios
tailored to each user and role



Difficulty adapts automatically based on performance;
immersive tests integrate into real communications

2. Adaptive difficulty



Learners advance through increasingly
challenging scenarios according to performance



Skill growth is measured
and reinforced over time

3. Profiles & insights



Individual and group
performance metrics



Risk analysis based on integrated metrics from
SAT tool plus email security for a complete view

Training intelligence that strengthens security – and delivers on ROI

Unifying training and email protection

The goal is a security culture that strengthens each employee's real-world resilience while simultaneously improving the protective controls around them, **allowing you to:**

- ✓ **Quantify correlation** between human performance and reduced human exposure
- ✓ **Drive a positive security culture** that rewards good behavior such as reporting
- ✓ **Communicate program value** to the board with confidence

What's needed

01 Analytics that measure risk

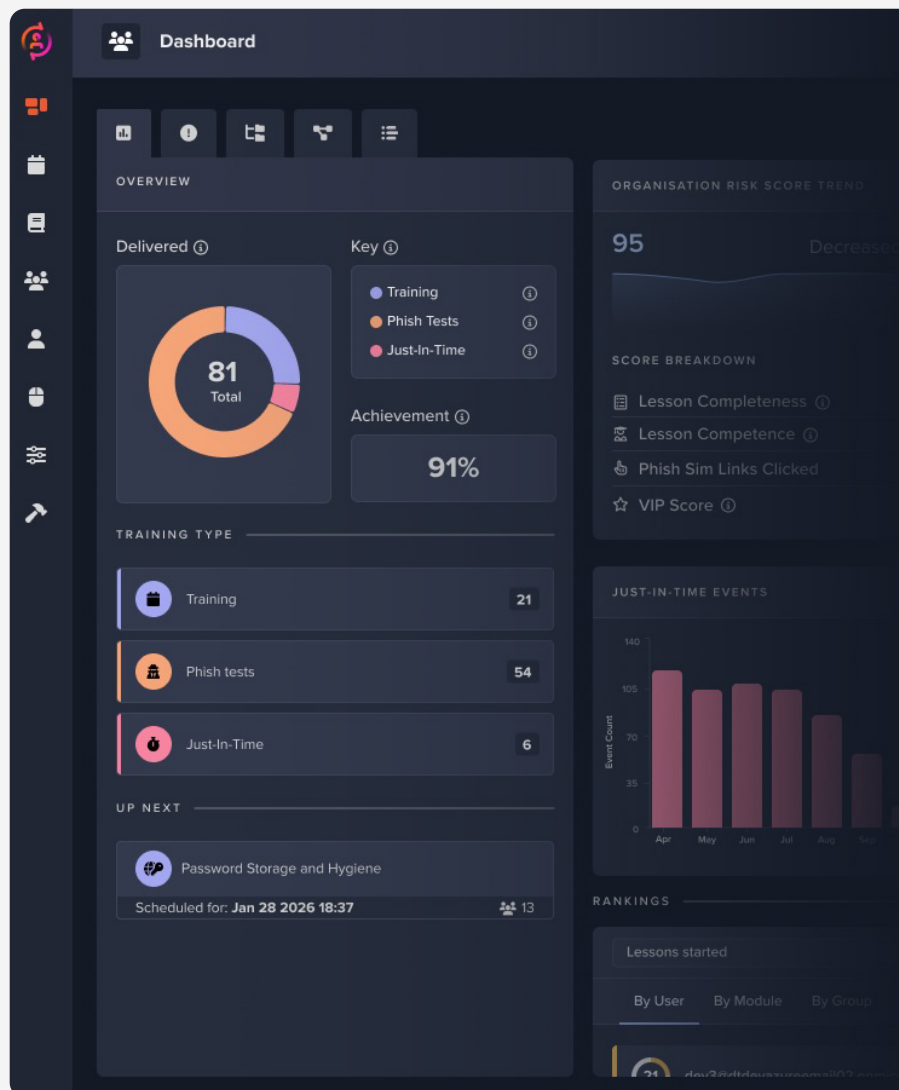
- Dashboards with session stats, risk scores, and month-over-month trends across users, groups, and the organization
- Board-ready metrics that convert performance data into defensible views of human risk (with VIP context)

02 Data access without barriers

- Export your data anywhere - integrate metrics into existing security, GRC, and reporting workflows

03 Integrated, closed-loop defense

- Bi-directional integration with email security, where people and threats interact most
- Telemetry flows both ways so coaching and controls adapt as users and threats evolve



Adaptive human defense, purpose-built for the modern workforce

Any SAT program can deliver training — but training alone is no longer enough. In organizations facing AI-powered threats, static, non-personalized programs cannot keep pace.

True risk reduction requires personalized, in-the-moment security coaching, where behavior and detection continuously inform and strengthen each other. Threats target humans. Make them your strongest line of defense. Darktrace is defining a new standard in human risk management.

Let's recap the benefits



True risk reduction that minimizes successful phishing



A **modern**, AI-driven security culture powered by dynamic, user-specific learning



Measurable behavior change, not just completion rates



Seamless integration with your existing security stack for closed-loop protection



Demonstrable ROI with board-ready metrics and defensible reporting



Check out

Darktrace / Adaptive Human Defense
solution brief



Download brief



Get a demo

Try Darktrace / Adaptive Human Defense
in your environment



Book a demo

