

YOUR PEOPLE ARE THE TARGET

A security aware workforce protects the enterprise.
Build readiness before attackers test your defenses

Simulate

Measure

Train

Prove It



91%

of breaches start with a phishing attack

Real

attack scenarios - not generic test emails

Proven

reduction in human risk - measurably, over time

THE REALITY

Attackers Don't Hack Systems Anymore, They Manipulate Human Assets

Perimeter defenses, firewalls, and endpoint tools protect your infrastructure. But no technology can prevent an employee from clicking a convincing link, submitting credentials on a fake login page, or approving a fraudulent request.

Attackers know this. That's why social engineering now leads the majority of successful breaches and why security awareness training that happens once a year, in a classroom, simply doesn't change behavior under real attack conditions.



Risk Is Invisible Without Measurement

Without simulation, you have no idea which teams, roles, or individuals carry the highest human risk in your organization.

Awareness Alone Isn't Enough

A policy document or annual training session doesn't prepare employees for the convincing, context-aware attacks they face today.

People Are The Primary Target

Attackers specifically craft campaigns to exploit human trust, urgency, and authority not technical vulnerabilities.

THE SOLUTION

TechOwl Phishlens - turn your employees into the strongest shield of your organization.

TechOwl Phishlens is an intelligent phishing simulation and human risk management platform. It goes beyond awareness training to continuously test, measure, and improve how your people respond to real-world social engineering attacks. Every simulation is an opportunity to identify risk before attackers do and every failure becomes an immediate, targeted learning moment that changes behavior for good.

01

SIMULATE

Launch realistic, targeted phishing campaigns tailored to your teams, roles, and the tactics attackers actually use.

02

MEASURE

MEASURETrack susceptibility by person, team, and department. See where your human risk actually lives, not where you assume it does.

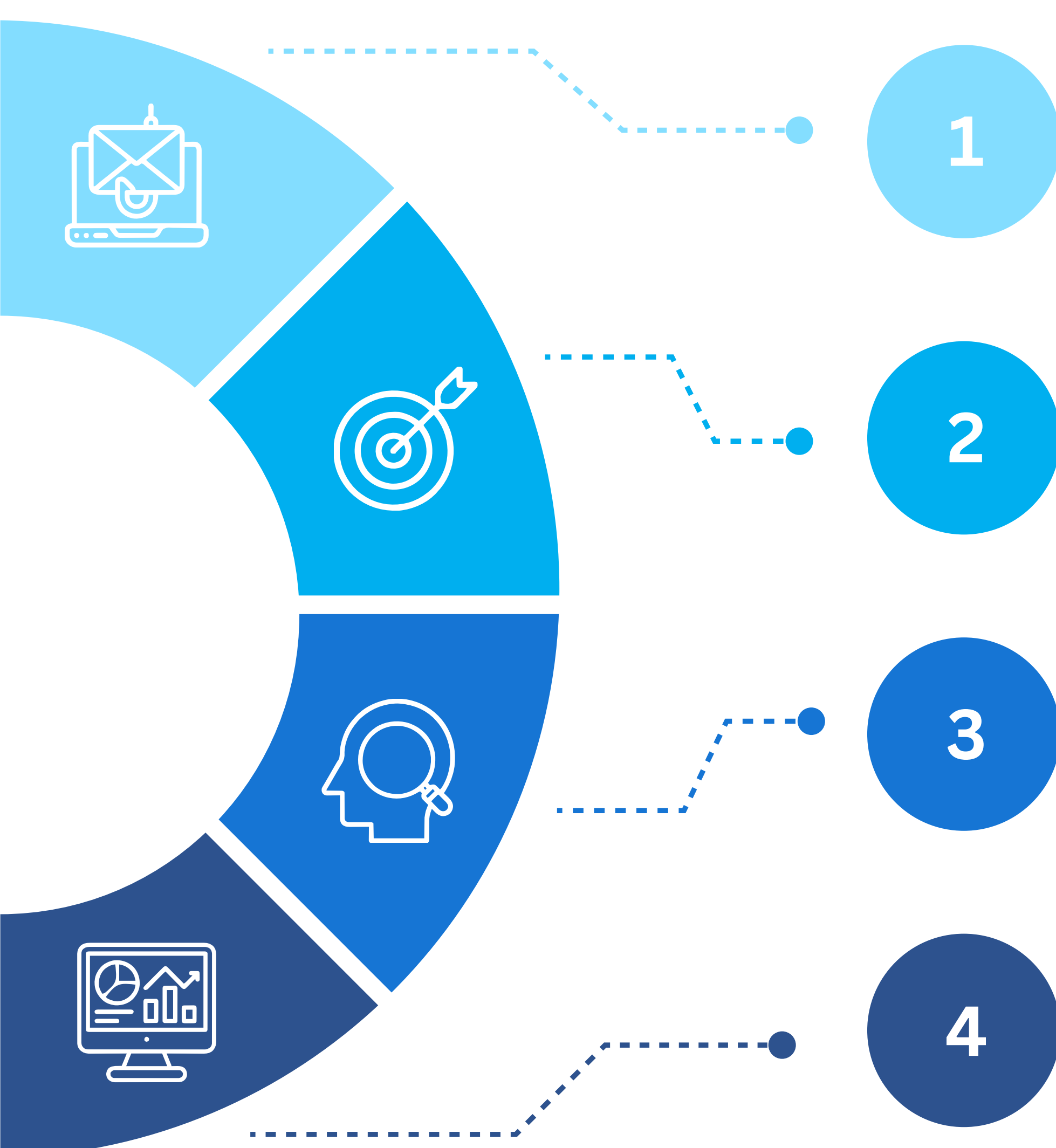
03

IMPROVE

Trigger instant, targeted micro-learning the moment someone fails, turning every mistake into a behavior change that sticks.

PLATFORM CAPABILITIES

Everything You Need to Manage Human Risk



1

Advanced Simulation Engine

Realistic campaigns covering spear-phishing, credential harvesting, brand impersonation, and attachment-based attacks - built around the techniques your adversaries actually use today.

2

Instant Adaptive Training

When someone fails a simulation, Phishlens automatically delivers a targeted micro-learning module - role-specific, threat-specific, and timed exactly when attention is highest.

3

Human Risk Intelligence

Move beyond click rates. Phishlens scores behavioral risk at the individual and department level - revealing your real exposure, not just your average awareness score.

4

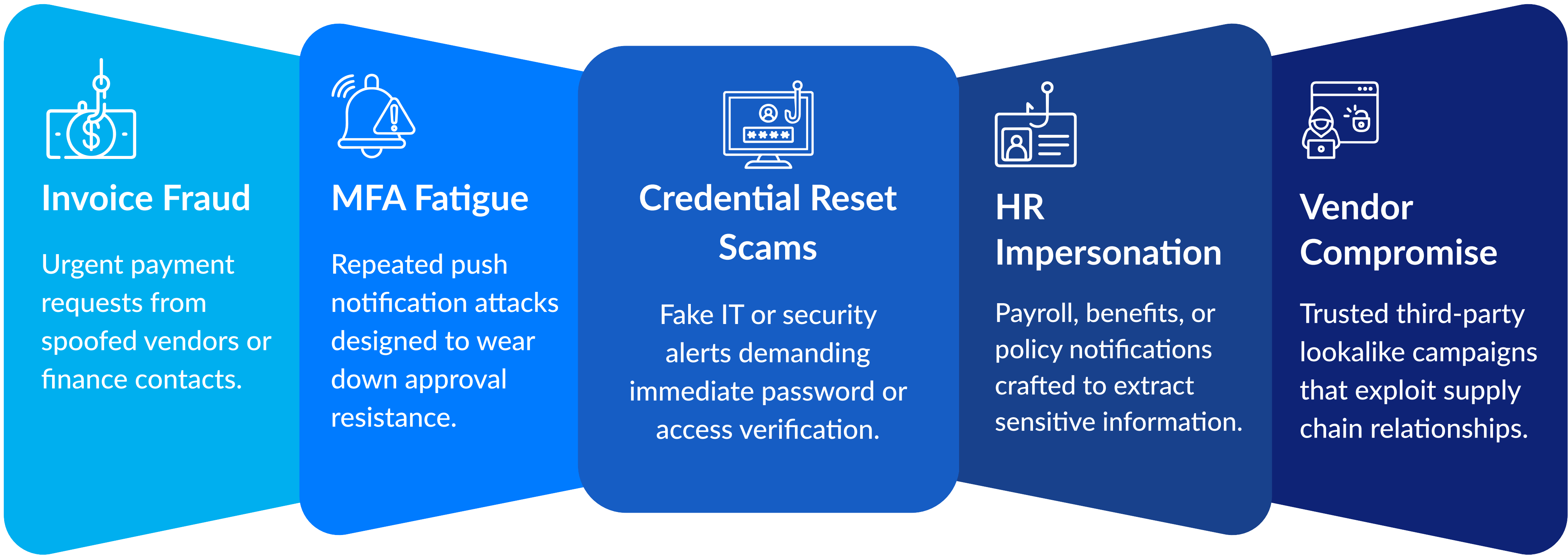
Executive Risk Dashboard

Board-ready reporting that tracks risk reduction over time, campaign performance, and awareness maturity giving leadership clear evidence that the program is working.

SIMULATION REALISM

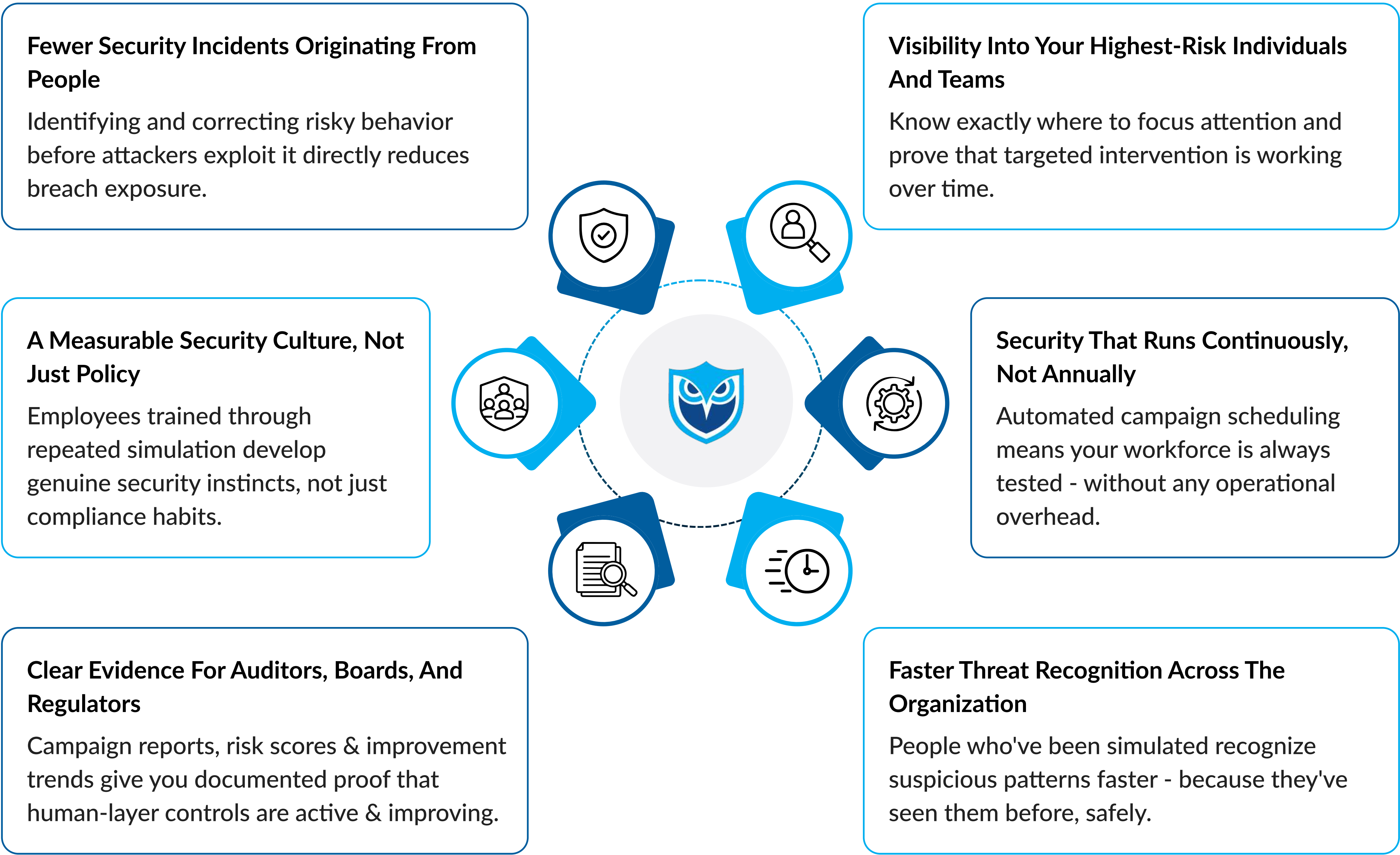
Built Around How Attackers Actually Operate

Generic phishing tests don't prepare your team for the real thing. Phishlens simulations are built around current attacker playbooks - so your employees face the same tactics, pressure, and deception they'd encounter in an actual attack.



BUSINESS OUTCOMES

What Changes When Human Risk Is Managed



PRECISION TARGETING

The Right Campaign, for the Right Person, at the Right Time

Not every team carries the same risk. Finance is targeted differently than IT. A new hire faces different threats than a senior executive. Phishlens lets you design campaigns that reflect these realities - so your simulation program is as precise as the attacks it prepares people for.

**By Department**

Finance, HR, IT, Legal - each team gets scenarios relevant to their role and risk exposure.

**By Designation**

Executives, managers, and frontline staff face appropriately calibrated simulation difficulty.

**By Geography**

Regional or country-specific campaigns that reflect local threat context and language.

**By Risk Profile**

High-risk individuals and repeat clickers receive increased simulation frequency and intensity.

GOVERNANCE & COMPLIANCE

Proof That Your Human Layer Is Under Control

Regulators and auditors are no longer satisfied with awareness training policies. They want evidence - that employees are tested, that risk is tracked, and that your program demonstrably improves over time. Phishlens generates exactly that evidence.

Compliance Support

- ✓ Employee Security Awareness Validation
- ✓ Social Engineering Resilience Evidence
- ✓ Security Control Effectiveness Testing
- ✓ Incident Preparedness Maturity Documentation
- ✓ Risk Reduction Tracking And Reporting
- ✓ Awareness Program Accountability Records

Governance Value

- ✓ Demonstrates Active, Continuous Human-Layer Testing
- ✓ Provides Documented Evidence Of Risk Reduction
- ✓ Satisfies Regulators That Awareness Is Measurable
- ✓ Supports BFSI, Healthcare & Regulated Sector Audits
- ✓ Moves Security Culture From Policy To Proof
- ✓ Shows Boards That Human Risk Is Actively Managed

Documented policy alone is no longer considered sufficient. Regulators increasingly expect measurable evidence of effectiveness.

WHY PHISH SHIELD

Beyond Generic Awareness - What Makes the Difference

Most organizations run some form of security awareness program. Very few can measure whether it actually changes behavior under real attack conditions. That's the gap Phishlens closes.

NO.	CAPABILITY	TRADITIONAL AWARENESS	TECHOWL PHISH SHIELD
1	Annual awareness training only	✗	✓
2	Generic phishing test emails	✓	✓
3	Spear-phishing & targeted simulation	✗	✓
4	Behavioral risk scoring per user	✗	✓
5	Departmental exposure heatmaps	✗	✓
6	Immediate micro-learning on failure	✗	✓
7	Threat-aligned simulation templates	✗	✓
8	Risk trend tracking over time	✗	✓
9	Board-ready compliance reporting	Limited	✓
10	Campaign scheduling automation	✗	✓

Part of the TechOwl Security Platform



Attack Surface Monitoring



Email Trust Assurance



Third-Party Risk Intelligence



Cloud Security Visibility



Employee Risk Readiness



Threat Signal Intelligence



Advanced Threat Detonation



Continuous Breach & Attack Simulation

Validate Trust Before Attackers Exploit It.

TechOwl Phishlens transforms awareness into measurable defense - so you know your people are ready when it matters most.