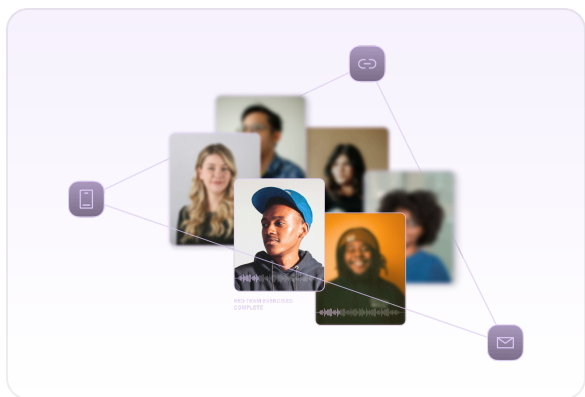


Red Teaming and Insider Risk Management

Pressure-testing that scales with the adversary

Emulate real attacker tactics across email, voice, SMS, social, and messaging with AI-powered or human-led conversations, while Doppel runs the infrastructure and measures every employee response.



Adversaries are resource-rich

Modern social engineering campaigns combine phishing, vishing, smishing, impersonation, and targeted pretexts across multiple channels simultaneously. Attackers follow up on existing threads, respond in near real time, and change tack when they hit a wall.

Why traditional red teaming falls short

Red teams and pen testers that rely on manual exercises, expensive consultants, or single-channel testing struggle to keep pace. The result is an uphill battle to validate employee readiness and eliminate risk, whether it is malicious, negligent, or ignorant.

Quantifying human and insider risk

>60%

of breaches include the human element

Source: [Verizon DBIR](#)

>41%

of social engineering attacks are multi-channel

Source: [TechMagic](#)

<15 sec

of audio required to produce a convincing AI voice clone

Source: [OpenAI](#)

\$4.91M

average cost of a malicious insider

Source: [IBM](#)

PROOF POINT

Fortune 50 healthcare company: external helpdesk

A Doppel red team engagement against the helpdesk exposed how real conversations leak process details and bend protocol.

8.8 min

average conversation with a human agent

15%

of calls leaked info about internal processes

92%

of calls perceived as human

12%

violated internal protocols

7

organizational technology leaks

How Doppel scales red teaming

01 Sophisticated conversational threading

Dynamic, multi-step threads let red teams emulate real attackers by engaging in back-and-forth exchanges with target users, moving seamlessly across channels.

02 Insider risk management at scale

Doppel handles the infrastructure so red teams can create multi-step, dynamic interactions with users on any platform, directly within Doppel.

03 AI-powered or human-led

AI-powered responses boost efficiency, while human-led interactions let red teams respond directly to users. Include synthetic voice clones and AI-generated pretexts.

04 Behavioral measurement and interventions

Every interaction, escalation, and exception granted is tracked and correlated with actual signals ingested from across the security stack, for a defensible view of where risk lies.

Outcomes

✓ Red teaming at scale

Interactions keep the pressure on, so employees face real attacker tactics, not static campaigns.

✓ Increased operational efficiency

Combine channels, dynamic conversations, and Doppel-hosted infrastructure in one platform.

✓ Clear visibility into risk

See employee performance in every scenario, closing awareness gaps and identifying ill intent quickly.

✓ Higher protocol compliance

Measurably higher adherence to security processes through a continuous cycle of training, validating, and reinforcing.

Safe, scoped, and measurable

All simulations are controlled and scoped to improve resilience and response behavior. Outcomes focus on systems and workflows, not blame. Success looks like stronger verification, faster escalation, higher reporting rates, and fewer risky behaviors, delivered in executive-ready reports tied to users, teams, and channels.

Cadence

Run awareness-focused red teaming continuously or quarterly. Insider-risk exercises can be narrower in scale but more frequent.

Book your demo at doppel.com/request-a-demo