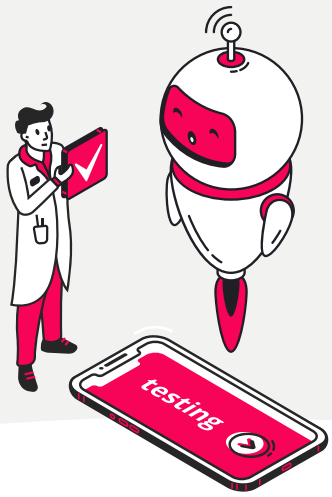
CONNECT®

In partnership with BLØCKPHISH

Protect your AI with Connect Adversarial AI Attack Simulation.



Strengthen your AI models against emerging threats.

AI is changing industries by making smarter decisions and automating important tasks. But, just like any powerful tool, it can be vulnerable to attacks. Small changes to input data can trick AI models into making wrong decisions, causing errors and disruptions.

Connect Adversarial AI Attack Simulation helps businesses identify weaknesses in their AI models and improve their security before these risks can be exploited. Whether you're using AI for tasks like customer support, detecting fraud, or improving everyday services, we provide solutions to keep your AI secure and reliable.

Why choose Connect's Adversarial AI Attack Simulation?

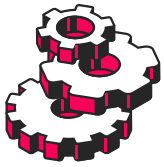
1. **Proactive risk management**
   AI is essential for decision making in many industries. As attacks become more advanced, it's crucial to secure your AI systems now to avoid costly problems later.

2. **Protect your reputation**
   A malfunctioning AI model can cause errors that damage your customers trust or lead to legal issues. Our service helps ensure your AI performs reliably, safeguarding your reputation.

3. **Compliance and security**
   As AI regulations grow, it's important to meet security and fairness standards. Connect help ensure your AI stays compliant with the latest rules, avoiding penalties and protecting your systems.

How we strengthen your AI.

Our approach is simple, yet effective. We test how your AI models perform under attack and provide clear solutions to improve their security and performance:



Comprehensive, tailored testing:
We simulate attack scenarios tailored to how you use AI and customise our solutions to fit your specific needs and risks.

Actionable recommendations:
We go beyond identifying issues and give you practical steps to improve your AI's security and reliability.

Regulatory alignment:
We ensure your AI meets industry standards and stays compliant with regulations, reducing the risk of penalties.

Deliverables.

- Simulation reports documenting:
  - Types of adversarial attacks conducted (e.g. data poisoning, model evasion, adversarial inputs).
  - AI model vulnerabilities exposed during testing.
  - Success rates of simulated attacks and corresponding impact analysis.
- Recommendations for improving model robustness.
- AI attack resilience scorecard.
- Technical playbook for mitigating identified weaknesses.
- Post-simulation debriefing session with key stakeholders.

The risk of inaction.

AI systems, while powerful, can be vulnerable to attacks. Not securing your AI now could lead to:

- **Reputation damage:** AI errors can harm your brand's credibility and push customers away.
- **Financial loss:** The cost of breaches or mistakes can add up, including fines, lost revenue, and legal fees.
- **Regulatory penalties:** AI regulations are tightening. Failing to comply can result in costly fines.

Stay secure. Stay resilient. Stay ahead.

Don’t wait for an attack to expose weaknesses in your AI. With Connect’s Adversarial AI Attack Simulation, you can ensure your AI is secure and performing at its best.

BLOCKPHISH - Trusted experts in security solutions

BLOCKPHISH, an NCSC Assured Service Provider, brings together a team of seasoned security professionals with expertise spanning commercial CISOs, ex-Special Forces, intelligence services, and senior advisors to central Government. They are passionate about keeping organisations secure, and provide insightful, proven solutions to tackle complex security challenges. BLOCKPHISH provide a tailored service based on their deep understanding and years of experience in building robust security postures that mitigate the most prevalent cyber and physical security threats. They have proudly supported organisations across diverse global industries, including Government, Defence, Healthcare, Legal, Energy, Critical National Infrastructure, Not-for-Profit, Financial Services, and Telecommunications sectors.

Connect with us.

Fortify your AI against vulnerabilities.

+44 2070 751450 (UK) +27 10 476 0300 (SA)

info@weconnect.tech

weconnect.tech