

Securing AI

Seismic advancements in AI and Machine Learning (ML) have changed our digital world, permeating every sector, fundamentally impacting business operations and conventional decision-making processes.

As with any major leap forwards in innovation, new challenges arise. Many have already surfaced, while much is still to be discovered as AI establishes its place in our daily lives. This challenges organisations and policy makers with the taxing task of harnessing the transformative potential of AI, while navigating the ever-evolving threat and regulatory landscape that it presents.

Securely integrate AI, drive innovation and safeguard against cyber risk.

We're here to help. Securing AI covers the breadth of our security consulting services, supporting our clients in getting to grips with what AI means for them, irrespective of size, industry or level of maturity with AI adoption and competency. We blend our rich heritage as a trusted advisor with a natural desire to stay at the forefront of new technology. We're ready to work with you to secure AI, drive innovation and safeguard against cyber risk.

Foundational, Technical and Strategic AI Consultancy Services



AI Strategic Consulting Build from the ground up. We'll help you assess your readiness for AI, develop your strategy and work with you to implement it into your business.



AI Technical Assurance Our AI/ML security assessments combine expertise with penetration testing, offering threat modeling, bias evaluations, and toxicity assessments to safeguard data and intelligence against evolving AI threats.



AI Governance, Risk & Compliance

Navigate incoming AI regulation such as the EU AI Act and ISO42001 with confidence. Identify risks and develop a roadmap towards compliance. Implement the right AI governance to execute your strategy.



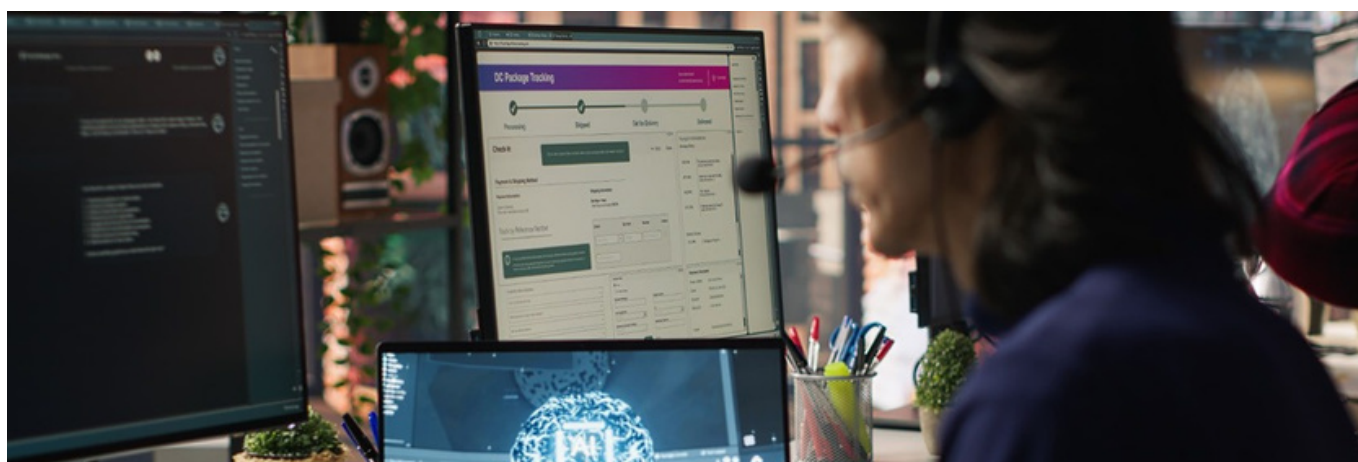
AI Research Services

Partner with our research team to leverage AI's potential, enhance cyber resilience, and develop risk-aware strategies that keep pace with emerging AI innovation and challenges.



AI Training & Awareness

AI impacts everyone, so take steps to ensure its advantages and inherent risks are understood. Our tailored Training & Awareness programs provide value at every level of your organization from the board to your in-house development teams.



Find end-to-end cyber security support at any stage in your AI adoption journey:

01

Examine your preparedness for AI adoption, identify gaps in compliance and assess your risk.

Assess

02

Develop your AI strategy based on your desired outcomes and level of investment.

Develop

03

Turn strategy into practice, close compliance gaps, reduce risk and embrace AI.

Implement

04

Continually monitor your resilience, maintain compliance and invest in staying ahead of AI threats.

Evolve



“Ensuring the safety and security of people, process and technology in an AI-augmented world demands vigilance and a commitment to forward-thinking strategies. This will require continuous adaptation to ensure we understand and secure the evolving use cases.”

Siân John MBE
Chief Technology Officer,
NCC Group

Why NCC Group



Track Record

Rich heritage of AI/ML technical security assurance, including testing AI-specific components within M&A engagements for over 10 Years.



Leading AI exploit discovery

We uncover new AI exploits and vulnerabilities first, and share our intelligence to protect our clients.



Fuelled by research

We partner with our clients to solve problems, build expertise and stay on the bleeding edge of technological innovation.



Breadth of capability

We align with the latest cloud ready frameworks, policies and controls to ensure you meet both current and evolving regulatory demands.



Enhanced decision-making

We present clear findings and actionable recommendations to help guide your investment decisions for securing AI products, models and solutions.



Industry influence

We actively engage and contribute towards the advancement of AI regulation and legislation across the globe to ensure security remains front and centre.

About NCC Group



NCC Group is a global expert in cyber security and risk mitigation, working with organisations to protect their brand, value and reputation against the ever-evolving threat landscape.

With our knowledge, experience and global footprint, we are well placed to help organisations identify, assess, mitigate and respond to the risks they face.

We are passionate about making the Internet safer and revolutionising the way in which organisations think about cyber security.





**For more information from NCC
Group on our G-Cloud 15 service,
please contact:**

+44 (0)161 209 5200

bidteam@nccgroup.com