nccgroup

AI SECURITY TESTING SERVICES

Build cyber resilience in the age of Artificial Intelligence (AI)

Technological advancements within the realm of AI and Machine Learning (ML) have developed swiftly, permeating every sector, and systematically changing business operations and decision-making processes.

As with any rapid technological advancement, new challenges and threats arise – many of which have already surfaced within this domain - challenging organisations and policy makers with the taxing task of harnessing the transformative potential of AI, whilst combatting the ever-evolving threat landscape it presents.

The security of AI systems is an ever-evolving field, and ensuring the safety and security of people, processes and technology in an AI-augmented world demands vigilance, and a commitment to forward-thinking strategies that will require continuous adaptation.

Managing the ever-evolving landscape of AI cyber threats

By combining our AI and ML expertise with industry-leading penetration testing and threat modelling methodologies, NCC Group delivers comprehensive security threat assessments that enable organisations to make informed decisions on how best to safeguard valuable data and secure intelligence from the ever-evolving landscape of AI cyber threats. Our range of services focus upon evaluating:

- The unique threat model of AI-driven systems according to their integration content.
- Practical attack vectors within AI/ML threat models and their consequences for organisations' people, processes, and technology.
- The potential compromise of model-governed assets inclusive of training data, model weights, prompt secrets, API endpoints, plugin endpoints, and more.
- Insights into resilience, the likelihood and impact of vulnerabilities in line with policy compliance, with remediation recommendations for the model output.
- Resilience to attacks illuminated by Models-As-Threat-Actors (MATA) methodologies.
- Content-driven evaluation of an AI/ML system's alignment to its intended objective.
- Assessments in line with the MITRE ATLAS framework and OWASPs Top 10 AI/ML Vulnerabilities: Testing for known AI/ML Security vulnerabilities including, but not limited to*: Prompt Injection, Adversarial Attacks, Data Poisoning Attacks, Membership Inference, Model Inversion and Model Stealing.

**Test scope will be defined in line with your requirements, defined by our experts.*

Our Services

AI/ML Red Teaming

Our team of AI/ML experts will engage with your AI/ML solution to identify any security weaknesses and bring them to light before the attackers get the chance. We will draw on our years of research and experience delivering for clients and advising governments to produce a tailored approach that targets your environment and will take in to account your specific needs and concerns.

We will test against known best practices to exposes AI/ML specific vulnerabilities such as the OWASP AI/ML Top Ten and the OWASP LLM Top Ten. We will work with you to explore any potential threats introduced by the use of AI/ML systems and we will provide a full report including recommendations to help you bring your environment in-line with security best practice.

AI/ML Secure Development Lifecycle Testing

Secure solutions come from robust policies and procedures. NCC Group bring our collective years of experience working at the forefront of AI/ML research together with our involvement in shaping the AI/ML secure development practices at a national and global level. Our bespoke testing methodology aims to provide a tailored approach that will best fit the security assurances required by your AI/ML solution.

Our world leading experts will work with you to understand and analyse your current Secure Development Lifecycle (SDL) processes and policies relating to AI/ML as well as reviewing your AI/ML production pipeline. We will work with you to identify and address the security holes in your AI/ML and SDL.

AI and ML Threat Modelling

Within NCC Group's AI and ML threat modelling process, our consultants collaborate with your organisation's Subject Matter Experts (SMEs) to review design and architecture decisions, assess risk profiles, and evaluate the overall security posture of your AI/ML-integrated environment. By conducting thorough implementer interviews and carefully analysing relevant documentation, we can effectively identify potential security risks and vulnerabilities within your system.

During this process, our consultants meticulously evaluate various aspects of your platform, including assets, controls, data flows, trust boundaries, and threat actors. By understanding the intricacies of your organisation's unique security landscape, we can provide tailored recommendations to help you enhance your defences and minimise the potential impact of cyber threats on your business operations.

Why NCC Group

NCC Group is passionate about sharing our insights and intelligence from operating at the 'frontline' of cyber security with policy makers who are making important decisions about the future of AI. We have engaged with governments, regulators, and legislators across the world, helping to inform new laws and regulations and advocating for a more secure digital future. Recent highlights include inputting into the Australian Federal Government's discussion paper on AI regulation, providing evidence to a UK Parliament inquiry on LLMs and supporting the development of the UK's AI whitepaper.

Track Record
Rich heritage of AI/ML security testing, including AI specific components within M&A over the last 10 years.

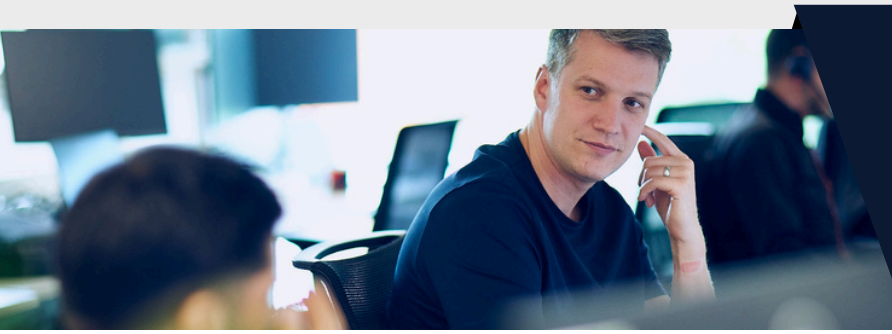
Experience
Achieve optimum enterprise cyber security resilience with NCC Group's highly skilled AI/ML security experts.

Research-led
World class AI/ML security research, fueling NCC Group's expert delivery methodology.

Technical Assurance
Collaborate with NCC Group's experts and assess AI/ML-driven product solutions and operations in the wider context of AI/ML business utilisation.

Actionable Intelligence
Guide decision-making with clear, actionable recommendations for secure intelligence with evolving technologies.

Manage Compliance
Aligned with regulation and compliance criteria for AI/ML technologies, and processes.



Our experts are here to help you.

Please get in touch to discuss your specific requirements and explore how you can benefit from our AI / ML services.

Get in touch