Artificial Intelligence (AI) - Security Architecture services from 2T Security

2T Security provides an Artificial Intelligence (AI) Security Architecture service to assist our clients with the design and delivery of AI within their projects, whilst managing the complex security needs of architecture, technology, integration and operations against a backdrop of ever-increasing hostile cyber threat.

AI introduces new risks, ethical, legal, and governance challenges, and to survive organisations must deal with the AI challenge and opportunity proactively. Embedding AI into corporate strategy and governance does not need to be overwhelming. We can help you to evaluate the risks, identify the controls, and deploy the proper strategy and governance for AI.
We provide a suite of AI Advisory Services to help organisations with the development and deployment of their AI strategy, products, and services.

We work predominately on the client side in the public sector, and have worked on some of the most sensitive, most complex, most critical, highest-profile projects within Government. We are certified by NCSC to provide competent Security Architecture services to our clients, and have strong relations with many parts of the NCSC, enabling us to leverage their skills and expertise efficiently.

If you require support implementing AI in your organisation, then we can help. We can support with small or large projects, across a wide variety of security disciplines.

Capabilities

- Assess AI integration security, preventing data exchange risks
- Evaluate data privacy and protection compliance
- Checking algorithms for biases and fairness in decision making
- Assessing that models are interpretable, accountable, and trustworthy
- Review adherence to relevant data protection laws
- Secure by Design principles are at the heart of everything we deliver, and we have significant experience contributing to the design process, from a security perspective, across central government & civil service bodies
- We have real-world experience contributing to the security design process
- Our team of Security Architects include AWS and Azure certified consultants, with cloud, and cloud security experience across numerous implementations and security initiatives
- We have a broad mix of skills which include deep AWS, Azure & M365 capabilities, DevOps, and Identity Governance, alongside the more traditional physical infrastructure
- Service assured by National Cyber Security Centre (NCSC)
- Service led by ACSC (CCP) Lead Security Architect

© 2T Security Ltd 2024

Key benefits

- Extensive data analytics experience in high threat environments
- Secure by Design principles are embedded at earliest opportunity
- Experience in creating architectural blueprints and standards
- Experience navigating Technical Review Boards and other appropriate change boards
- Technology agnostic approach that reflects business needs
- Confidence working with internal and external stakeholders across your organisation
- Confidence your technical security problems will be managed by an NCSC assured organisation
- Confidence that your security architecture is being delivered to a consistent standard
- Backed up by extensive real-world experience covering most central Government departments and organisation
- Modular approach to functionality — we can support and rapidly deliver a minimal set of requirements for a client's immediate needs, which can then be augmented in stages to support enhanced requirements.
- Services led by ACSC (CCP) Lead Security Architect
- Extensive experience in security design in public and private sectors
- Trusted by NCSC for high value and complex projects
- Skills transfer to internal staff including training.

Engagement Process

Our AI security architecture service engages widely to deliver high levels of value to your business, including:

- Identifying business, technical, and supplier stakeholders
- Full support for any AI discovery, user research, design, develop, delivery, build, and on-going support for live activities undertaken
- Access to datasets and data owners will be required, including understanding how your data is being used
- Understanding existing security controls for effectiveness and response capabilities
- Risk assessments to identify your most critical business assets
- Developing response plans to protect your controls to protect business assets in the most efficient way
- Regular checkpoints to review performance and deliver continuous improvement
- All of our security delivery is managed by a Technical Account Manager, meaning our delivery is focussed and communication is clear

© 2T Security Ltd 2024