

Security Engineering Services

Service Definition

Summary of Service

Telana provides a comprehensive suite of security engineering services designed to ensure the stability, security, and optimisation of our clients' platforms and solutions. Our approach integrates security into every stage of the engineering and development lifecycle, from initial strategy to ongoing assurance.

Service Features

- / Strategy, Governance & Risk
- / Identity & Access Management (IAM)
- / Infrastructure & Network Defence
- / Application, Product, and AI Security
- / Offensive Security & Assurance
- / Resilience & Continuity

Service Benefits

- / Proactively embeds security across the entire development lifecycle, reducing risk from the outset.
- / Ensures compliance with industry standards and regulatory requirements through robust governance and auditing.
- / Strengthens defences against cyber threats with a multi-layered approach covering identity, infrastructure, and applications.
- / Provides assurance and identifies weaknesses through expert-led offensive security testing.
- / Enhances organisational resilience by establishing clear strategies for business continuity and disaster recovery.

Service Description

Strategy, Governance & Risk

We establish a solid foundation for your security posture by developing robust governance frameworks and compliance strategies. Our experts conduct thorough

security audits and define clear remediation roadmaps to ensure your organisation meets regulatory requirements and effectively manages risk across all digital assets.

Identity & Access Management (IAM)

We design and implement comprehensive Identity and Access Management (IAM) solutions to ensure that only authorised users can access your systems and data. This includes designing and deploying Zero Trust architectures that enforce strict access controls, verifying every request regardless of its origin to minimise the risk of unauthorised access.

Infrastructure & Network Defence

Our services strengthen your organisation's defences at the infrastructure level. We implement robust perimeter security controls to protect your network from external threats and deploy advanced endpoint security solutions to secure servers, laptops, and other devices from malware and cyberattacks.

Application, Product, and AI Security

We integrate security directly into your development process through DevSecOps practices, ensuring your applications are secure by design. Our services include implementing strong data encryption and protection measures for data at rest and in transit, as well as specialised security protocols to protect the integrity and confidentiality of your AI and machine learning models.

Offensive Security & Assurance

To proactively identify and address vulnerabilities, we coordinate expert-led penetration testing for your networks and applications. We perform detailed vulnerability assessments to uncover potential weaknesses and provide actionable recommendations to strengthen your defences before they can be exploited.

Resilience & Continuity

We help you prepare for and recover from potential disruptions by developing comprehensive Business Continuity Plans (BCP) and Disaster Recovery (DR) strategies. Our service ensures that critical business functions can continue to operate during an incident and that your systems can be restored quickly and efficiently, minimising downtime and data loss.