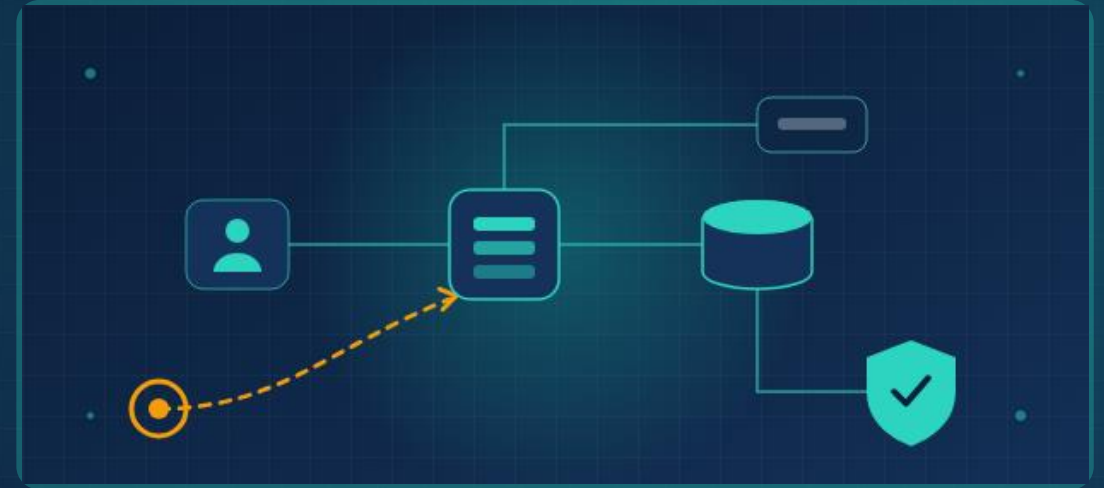


Threat Modelling

Spot attack paths before you build

A structured way to understand how your systems could be attacked, and to design in the right controls early. We work with your architects and developers to model threats, prioritise risks and build security into the design instead of bolting it on later.



THE CHALLENGE



Late discovery

Design flaws found in testing or production are costly and slow to fix.



Complex architectures

Cloud, APIs and third-party services widen the attack surface.



Speed of delivery

Teams need security insight that keeps pace with agile delivery.

How we deliver



ALIGNED TO

STRIDE

MITRE ATT&CK

OWASP

NIST SSDF (SP 800-218)

NCSC Secure Design Principles

ISO/IEC 27001 A.8.27

Our capability

- ✓ Workshops for new and existing systems
- ✓ Data flow and architecture security reviews
- ✓ Modelling for cloud, API and AI-enabled services
- ✓ Threat modelling embedded in DevSecOps pipelines
- ✓ Training and playbooks for your own teams

Benefits & value

Build security in from the start and cut the cost of fixing it later.

-  **Lower cost:** fix flaws at design, not in production
-  **Focused testing:** aim pen tests at the real risks
-  **Secure by design:** controls built into the architecture
-  **Team capability:** developers who think like attackers