FUJITSU

Threat Model

Intelligence-driven defence

Discover your attack surface and the threat actors most relevant to your organisation.

Modern organisations face increasingly complex systems, integrations, and dependencies - all of which introduce hidden security weaknesses. Fujitsu's Threat Modelling Service provides a structured, intelligence led view of how adversaries could compromise your environment, giving you clear, prioritised actions to improve resilience before attackers can exploit gaps. We work collaboratively to map critical assets and attack paths, then apply intelligence-led scenarios to test how those threats could realistically unfold. This ensures outputs are grounded in your environment, aligned to current attacker behaviour, and directly actionable by your teams.

Understand how attackers could realistically move through your environment to reach critical assets

Focus remediation efforts on the controls and fixes that address the highest-risk attack paths, embed security into design and transformation initiatives, and continuously strengthen your security posture using intelligence aligned to current attacker behaviours.

- Clear visibility of attack paths
- Prioritised remediation roadmap
- Improved security-by-design
- Continuously uplift security posture

Know where attackers are most likely to succeed and prioritise action to reduce risk.

Our approach combines threat intelligence, architectural analysis, and risk assessment to build a comprehensive understanding of your threat landscape.

Adversary-based modelling

Map realistic attacker behaviours using threat intelligence, MITRE ATT&CK, and industry patterns.

Architecture and system analysis

Review workflows, integrations, data flows, and trust boundaries to uncover structural risks.

Use-case and scenario development

Build threat scenarios tailored to your business, technologies, and regulatory landscape.

Control assessment and gap identification

Evaluate existing security controls and highlight weaknesses or bypass opportunities.

Remediation guidance and design uplift

Provide practical, achievable recommendations aligned to your architecture and teams.

Executive-ready reporting

Deliver clear summaries suitable for both technical and non-technical stakeholders.

Why work with us?

Holistic visibility across your environment: Applications, cloud, integrations, identities, and data all assessed cohesively.

Accelerated delivery with expert facilitation: Workshops, modelling sessions, and design reviews run by senior security architects.

Strengthens governance, compliance, and resilience: Aligned to Australian and New Zealand frameworks.

Contact us today

Visit our website