e2e assure

Threat Modelling Assessment

Service Definition Document

Threat Modelling Assessment

Service Definition Document – G-Cloud 15

CONTENTS

SERVICE INTRODUCTION

e2e-assure provides structured threat modelling services designed to help organisations identify, understand, and prioritise security risks early in the system lifecycle. Our approach aligns technical architecture with business risk, enabling informed decisions and practical remediation planning.

SERVICE OVERVIEW

The Threat Modelling Engagement is delivered as a collaborative, evidence-driven process. It combines architectural discovery, structured threat analysis, and risk-based prioritisation to produce actionable security outcomes that integrate into agile delivery and operational processes.

SCOPE OF ACTIVITIES

The assignment will include the following actions and areas of assessment:

Stage	Tasks
Engagement Initiation & Scope Definition	• Define scope, objectives, and success criteria aligned to business risk and critical assets • Confirm in-scope systems, environments, integrations, and "what good looks like" • Identify key stakeholders and decision makers (engineering, product, security, ops) • Establish engagement governance: cadence, working sessions, risk scoring approach, artefact storage, and signoff process
Architecture Discovery & Evidence Collection	• Collect architecture artefacts (diagrams, ADRs, OpenAPI/GraphQL schema, cloud patterns, CI/CD overview) • Build an interface and dependency inventory (APIs, events, queues, third parties, admin paths) • Identify data assets and classify data flows (PII/PCI/secrets, retention, residency) • Map identity model (users/roles, service identities, authN/authZ patterns, privileged access) • Review existing controls (WAAP/WAF, rate limits, logging/monitoring, secrets/KMS, IAM guardrails)
System Decomposition & DFD Modelling	• Define system boundaries, trust boundaries, and key security assumptions • Create logical DFD (conceptual view) and physical DFD (deployment/runtime view) • Annotate flows with protocol, authentication method, encryption, data classification, and trust transitions • Validate DFDs with architects/engineers and confirm "as built" reality
Threat Identification (STRIDE + Modern Abuse Lens)	• Perform STRIDE analysis across DFD elements (processes, data stores, data flows, external entities) • Identify abuse cases / misuse cases (business logic abuse, fraud patterns, scraping/bot flows) • Identify misconfiguration and identity threats (overpermissive IAM, weak boundaries, exposed storage) • Build top attack paths (how threats chain end-to-end) for highest-risk scenarios
Findings Analysis & Risk Prioritisation	• Score threats using agreed impact/likelihood and exposure context (internet-facing, privilege required, detectability) • Identify control gaps, blind spots, and weak trust boundaries • Categorise risks by theme (auth, data exposure, DoS, supply chain, observability) • Conduct risk triage with stakeholders: mitigate / accept / transfer / defer with rationale and review dates
Mitigation Design & Remediation Backlog Creation	• Define mitigations: secure design patterns, control improvements, and compensating controls where needed • Produce sprint-ready backlog items with acceptance criteria and owners • Define security requirements (NFRs): logging/audit, rate limiting, encryption, session/token handling, least privilege

	• Provide quick wins vs structural improvements plan (what to do first, and why
Verification & Traceability	• Create Threat → Control → Evidence mapping (what mitigates what, and how we prove it) • Define security test cases (negative tests, abuse tests, auth tests) derived from top threats • Define monitoring and alerting requirements for critical flows and sensitive actions • Validate closure approach: what "fixed" means, and what evidence is required
Closeout, Playback & Operationalisation	• Deliver technical playback and executive playback sessions • Provide an operational model to keep threat modelling "alive" (triggers, cadence, lightweight feature-level process) • Embed into agile ways of working (Definition of Done, design review gates, release readiness checks) • Final sign-off: residual risk statement, decision log, and next-step roadmap

SCOPE OF DELIVERABLES

The following tangible outputs will be provided as part of the engagement sign-off:

Output	Description
Executive Summary & Risk Narrative	• Concise summary of key risks, business impact, and recommended priorities • Top attack paths and what must be fixed first • Residual risk and decision highlights
DFD Pack (Logical + Physical)	• Approved DFDs with trust boundaries and data classification annotations • Versioned artefacts suitable for ongoing updates • "Facts & assumptions" sheet to prevent future drift
Threat Register (STRIDE + Abuse Cases)	• Prioritised list of threats mapped to DFD nodes/flows • Includes abuse cases, misconfiguration risks, identity threats • Clear descriptions + recommended mitigations
Risk Scoring & Decision Log	• Scoring approach applied consistently • Record of decisions: mitigate / accept / transfer / defer • Risk acceptance rationale with review dates
Remediation Backlog (Sprint-Ready)	• Tickets/epics with acceptance criteria, owners, and prioritisation • Quick wins vs structural improvements • Dependencies and sequencing guidance
Security Requirements / NFR Pack	• System security requirements (logging/audit, rate limits, encryption, auth standards, least privilege) • Secure design patterns aligned to the architecture • Guardrails for future changes
Threat → Control → Evidence Matrix	• Traceability showing how each critical threat is mitigated • Evidence expectations (tests, configs, logs, dashboards) • Supports audit readiness and measurable closure
Verification & Monitoring Recommendations	• Security test cases derived from threats • Monitoring/alerting requirements for critical flows • Detection gaps and observability improvements
Post-Engagement Consultation & Next Steps	• Debrief session with key stakeholders • Prioritised action plan for the next 30/60/90 days • Recommended cadence and operating model for ongoing threat modelling

SERVICE OUTCOMES

- Identifies architectural and design risks before they become expensive defects or incidents
- Creates a shared understanding of trust boundaries, data flows, and security ownership across teams
- Produces a practical remediation backlog that engineering teams can deliver in sprints
- Improves security posture across identity, APIs, data protection, resilience, and monitoring
- Establishes a repeatable threat modelling capability integrated into agile delivery