

Threatplane Consulting Service Definition

Threatplane Consulting Service Definition	1
Version	1
1. What the Service Is	2
2. Service Scope	3
3. Delivery	4
4. Service Constraints	5
5. Support	6
6. Data Handling	7
7. Security and Governance	8

Version

Document Version: 1.0

Last Updated: January 2026

1. What the Service Is

Threatplane provides expert threat modelling consulting services delivered by our in-house team of experienced security professionals. We deliver comprehensive threat models for your systems, applications and business processes. These give you simultaneous insight into risk, threats, and controls.

Our consulting service is outcome-based with fixed fees, giving you certainty of value. Each engagement produces a detailed threat model that serves as a master plan for cyber risk management.

Key deliverables:

- Complete threat model documentation
- Identified threats and attack vectors
- Risk assessment linking threats to business impact
- Controls assessment and gap analysis
- Prioritised remediation roadmap

2. Service Scope

Our pricing is based on system complexity, allowing us to take the risk for you. If the system turns out to be a little more complex than anticipated, as long as it remains within the same level of complexity, we will never charge more to deliver.

Pricing information is provided in the separate Pricing Document.

Getting Started

Threat modelling is very flexible. You do NOT need to fully know your system design or complexity to get started. We'll discuss this with you prior to booking to understand your requirements and agree the scope.

3. Delivery

Standard Delivery

We deliver all threat models within 4 weeks as standard.

Expedited Delivery

Need your threat model in a hurry? Speak to us about a 2-week delivery before booking.

4. Service Constraints

- Services are delivered remotely as standard
- Onsite delivery available at extra cost
- Customer participation required for discovery workshops and information gathering
- Final deliverables provided in PDF and Excel format

5. Support

During Engagement

Dedicated consultant assigned to your project with direct communication throughout.

Post-Delivery

Support available for questions about the delivered threat model. Extended support and ongoing maintenance available through our platform subscriptions.

6. Data Handling

Confidentiality

All customer information is treated as confidential. Our consultants operate under strict NDAs and information security policies.

Data Storage

- Customer data stored in United Kingdom
- Data encrypted in transit using TLS 1.2 or above
- Compliant with SSAE-18 / ISAE 3402 standards

Data Retention

Project documentation retained for 12 months following delivery unless otherwise agreed. Bulk data export available on request.

7. Security and Governance

Staff Security

- Staff screening performed
- Government security clearance available up to Developed Vetting (DV)

Quality Assurance

All threat models undergo internal quality review before delivery to ensure consistency and completeness.

Information Security Policies

We operate the following policies:

- Acceptable Use Policy (including AI governance)
- Network Security Policy
- Access Control Policy
- Data Management Policy
- Remote Access Policy
- Vendor Management Policy

For more information, visit the [Threatplane website](https://threatplane.com).

Threatplane is the trading name of Threatplane Limited, and is registered under company number 10549779 in England and Wales. Our registered offices are at Desklodge Beacon Tower, Colston St, Bristol BS1 4XE.