G-Cloud 15

Service Definition

Threat Modelling Service

Table of Contents

1. Service Overview

Cyberfort's Threat Modelling Service delivers a Secure by Design approach to identifying, prioritising and mitigating cyber security risks across applications, infrastructure and business operations. We provide structured, evidence-led threat modelling that enables organisations to reduce risk earlier, make better security decisions, and strengthen resilience beyond software development alone.

Our threat modelling combines expert-led workshops with proven techniques to analyse how attackers could compromise systems, data, identities, business processes and critical services. We evaluate threats across technology and operational contexts, including cloud platforms, networks, users, suppliers and internal business workflows.

Cyberfort will deliver an innovative security service underpinned by cyber security best practice, delivered by skilled consultants using approved methodologies aligned to industry frameworks including NCSC Secure by Design principles and the Cyber Assessment Framework (CAF) where applicable. Threat modelling outputs are practical, actionable, and designed to integrate with delivery teams, risk owners and governance stakeholders.

We pride ourselves on delivering a holistic approach by considering an organisation in its entirety. This allows us to assess complex environments and provide clear security recommendations that help improve defensive posture, resilience, and decision-making across business and technical teams.

Cyberfort's Threat Modelling Service includes the following key elements:

- **Application threat modelling:** Identify risks across user journeys, APIs, data flows and trust boundaries
- **Infrastructure threat modelling:** Assess cloud design, network segmentation, identity controls and configuration risks
- **Business threat modelling:** Evaluate risks across business processes, insider threats, fraud/abuse cases and operational dependencies
- **Structured methodologies:** STRIDE, attack trees, misuse/abuse cases, kill chain thinking and scenario-led analysis
- **Actionable mitigations:** Prioritised remediation recommendations aligned to risk and delivery realities
- **Assurance-ready outputs:** Threat to mitigation traceability and evidence suitable for audit and governance
- **Secure by Design alignment:** Supports early risk reduction through design controls and secure defaults

1.1 Service Detail

Cyberfort's Threat Modelling Service includes the following capabilities and services:

1.1.1 Secure by Design threat modelling across the organisation

Our threat modelling approach is designed to reduce risk early by identifying realistic threat scenarios and focusing mitigation efforts where they deliver the highest value. We operate across:

- Applications and APIs

- Cloud infrastructure and network design
- Identity and access management
- Third-party services and supply chain dependencies
- Operational processes and business workflows.

This ensures security improvements are not limited to software development teams, but also reduce exposure introduced through infrastructure decisions, operational delivery and business change.

1.1.2 Alignment to your organisation's risks, threat landscape and risk appetite

Cyberfort threat modelling is risk-based and tailored to organisational priorities. We align threat analysis to:

- Business critical services and high-value assets
- Data classification and trust boundaries
- Known attacker behaviours and threat intelligence
- Your risk appetite and governance model

This enables threats to be prioritised consistently, and mitigations to be defined in proportion to risk and likely impact.

1.1.3 Threat workshops and collaborative working

Cyberfort facilitates structured threat modelling workshops that bring together the right stakeholders across engineering, infrastructure, operations and security. These sessions are designed to rapidly produce high-quality outcomes including:

- Defined architecture and trust boundaries
- Key threat scenarios and attack paths
- Control requirements and mitigation recommendations
- Ownership and delivery actions for tracking through to completion.

1.1.4 Infrastructure and cloud architecture modelling

We assess threats arising from infrastructure design and cloud configuration, including:

- Segmentation and exposure risks
- Privilege escalation paths
- Identity attack paths and authentication risks
- Logging, monitoring and alerting gaps
- Misconfiguration risks and insecure defaults
- High availability and recovery vulnerabilities.

This ensures infrastructure-related security risks are addressed alongside application risks.

1.1.5 Business and operational threat modelling

Where required, we model risks beyond technology controls, including:

- Insider threats and privilege misuse
- Fraud and abuse cases

- Process vulnerabilities and human error
- Supply chain compromise routes
- Threats affecting service delivery and operational continuity.

This approach improves overall resilience and supports CAF-style outcomes-based assurance.

1.1.6 Threat modelling outputs and evidence packs

Cyberfort provides outputs that are directly usable by delivery and assurance teams, including:

- System context and data flow diagrams (where required)
- Threat register with prioritised risks
- Mitigation plan and control mapping
- Recommendations aligned to secure design patterns
- Traceability evidence for governance and audit purposes.

Outputs can be aligned to customer templates and assurance requirements, including CAF-aligned reporting styles where applicable.

1.1.7 Continuous improvement and refresh on change

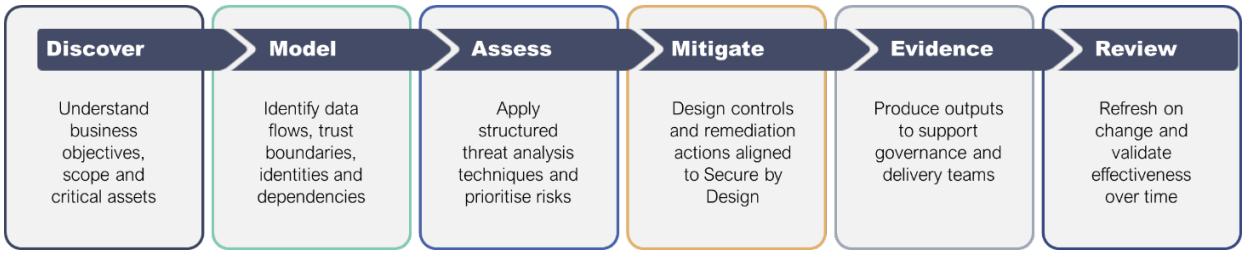
Threat models are living assets. Cyberfort can support ongoing refresh cycles triggered by:

- New services or major feature releases
- Architectural change (cloud, network, identity, supplier changes)
- New threat intelligence or emerging attacker techniques
- Lessons learned from incidents or exercises.

This ensures the threat model remains relevant and supports continuous security improvement.

1.1.8 Threat Modelling Approach (Example Workflow)

Cyberfort follows a structured approach to ensure consistent outcomes:



1.1.9 Evidence and Reporting

Cyberfort provides evidence-led outputs that support decision-making and assurance, such as:

- Threat register and prioritised risks
- Mitigation actions with ownership
- Recommendations mapped to architecture components and trust boundaries
- Option to map outcomes to CAF objectives and contributing outcomes

- Executive summary for governance stakeholders
- Technical annex for engineering and infrastructure delivery teams.

1.1.10 Security

Cyberfort's Threat Modelling Service is governed by strong security policies, procedures and controls which are aligned to recognised security standards and good practice.

Our approach supports key Secure by Design outcomes through:

- Reducing attack surface and eliminating threats through architecture choices
- Driving least privilege and secure identity design
- Designing secure defaults and hardened baseline configurations
- Ensuring visibility through logging and monitoring requirements
- Improving resilience and recoverability for critical services.

2. Onboarding and Offboarding Support

Cyberfort delivers threat modelling through a structured engagement approach:

- Rapid scoping and stakeholder identification
- Workshops scheduled to fit delivery plans and governance constraints
- Clear deliverables agreed at the start of the engagement
- Outputs designed to feed directly into backlog and risk registers
- Optional follow-up sessions to validate remediation and confirm closure.

3. Service Management Approach

3.1 Service Delivery Teams

Cyberfort provides a cross-discipline delivery team to ensure robust threat modelling outcomes across application, infrastructure and business risk:

- **Lead Security Consultant / Threat Modelling Lead:** owns delivery quality and outcomes
- **Security Architect:** validates design implications and mitigations
- **Cloud & Infrastructure Specialist:** addresses platform, IAM, and network threats
- **Governance & Assurance Support:** aligns outputs to CAF-style assurance needs (where required)

A named delivery lead provides a consistent point of escalation and reporting for the engagement.

4. Commercials & Pricing

4.1 Ordering & Invoicing Process

Please contact us for a quote via email at bidmanagement@cyberfortgroup.com

Orders are processed on receipt of a purchase order.

Prior to commencement of any work ordered via the G-Cloud framework, Cyberfort requires client acceptance of the order and also completion of a Call-Off Contract.

Clients are invoiced on a monthly basis or according to agreed milestones.

4.2 Service pricing model

Cyberfort's pricing for Threat Modelling links clearly to Resources Based Pricing detailed in our SFIA rate card framework.

Please refer to our Pricing document for more details.

4.3 Minimum contract period

Contract terms will be provided at the time of quotation, based on specification. These will not exceed the maximum contract constraints of the G-Cloud framework.

5. Governance Compliance

Cyberfort confirm that we will deliver our services to clients in line with all industry and Government recognised standards, best practice and legal regulations, including but not limited to the following:

5.1 GDPR

We adhere to the legal and statutory requirements outlined in the UK Data Protection Act 2018 and the General Data Protection Regulations (GDPR). Our organisation has a current registered Information Commissioners Office (ICO) certificate for Data Protection.

5.2 Government and industry standards

Throughout the life of any contract, our consultants will ensure that all service standard principles are adhered to so that clients can be assured that all delivered outcomes conform with Government and industry standards and expectations. Our teams are deeply experienced in operating services, to deliver outcomes and outputs that fully comply with:

- The principles defined in the Government's Service Standard and Technology Code of Practice (TCoP).
- The Government Functional Standard (GovS 007: Security), ensuring that the stated principles (for example security objectives are aligned to government policy and organisational objectives) are applied to all projects.
- Open standards supported include TOGAF, NIST-CSF, ISO/IEC27000, SANS and OWASP.
- Regulation frameworks including, Cyber Security and Resilience Bill, Digital Operational Resilience Act (DORA), and NIS2 Directive.
- Government Cyber Security Strategy, including National Cyber Security Centre (NCSC).
- As an NCSC assured Cyber Security Consultancy, we are members of the NCSC Assured Consultancy Scheme Community Network and leverage the CiSP (Cyber Information Sharing) platform.

5.3 Quality Management

Further, we have a fully implemented Quality Management System (QMS) and are certified to ISO 9001:2015 International Standard, which details our policy, objectives and processes, as well as demonstrating how our QMS framework enhances client satisfaction whilst ensuring consistent delivery of product and services is maintained to meet client, statutory and regulatory requirements.

Our delivery is underpinned by certifications and associated management systems including:

- ISO:27001
- ISO:14001
- ISO:9001
- ISO:45001
- Cyber Essentials Plus
- CREST Certified Body CE
- CREST Penetration testing
- NHS Digital Toolbox
- PCI DSS
- DSPT
- NCSC Cyber Security Consultancy
- NCSC CHECK ITHC

About Cyberfort

Cyberfort's all-encompassing Cyber Security Services

At Cyberfort we provide a range of customers with all-encompassing Cyber Security Services. We are passionate about the cyber security services we deliver for our customers which keeps their people, data, systems and technology infrastructure secure, resilient and compliant.

Our business offers National Cyber Security Centre assured Consultancy services, Identification and Protection against cyber-attacks, proactive Detection and Response to security incidents through our security operations centre and a Secure and Recover set of Cloud solutions which keeps data safely stored, managed and available 24/7/365.

Over the past 20 years we have combined our market leading accreditations, peerless cyber security expertise, strong technology partnerships, investment in our future cyber professionals and secure locations to deliver a cyber security experience for customers which enables them to achieve their business and technology goals in an ever-changing digital world.

Cyberfort

Care about the impacts we make on the Environment, Social and Governance.

We are passionate about empowering our employees, suppliers, customers, and the cyber security ecosystem to create a better world for our business and the communities we participate in, for example:

As a member of Neurodiversity in Business (NiB) and Disability Confident Employer

Cyberfort are supporting those with physical and neurodiverse disabilities, by disarming barriers for people with disabilities and ensuring equal opportunities for all.

Cyberfort are inspiring and attracting young people to the world of cybersecurity.

We support the development of their passion for technology through Apprenticeships, Graduate Schemes, CyberFirst and school education/awareness.

We are committed to achieving net zero carbon emissions by 2050.

Cyberfort have clear plans and activities that deliver environmental benefits by increasing the energy efficiency of our operations, reduce our waste, and protect our communities.

Our Values

Teamwork | Curiosity

Ownership | Agile | Innovative

Cyberfort

Accreditations

We are proud of the extensive list of industry and government accreditations we hold. We understand the need for independent validation when entrusting the security of valuable or sensitive data to a third party.

Our Vision

To be an integral part of the cyber security ecosystem, providing assured, highly skilled and reliable security services to businesses and government departments. Embodying the UK Cyber Security Strategy, through trusted partnerships we aim to empower businesses and government departments with confidence, making the world a safe and secure place to conduct business.

Our Mission

To provide our customers with an agile and innovative approach to help them overcome their cyber security challenges. Through a collaborative approach with our customers we design, build and operate their cyber security environments resulting in a secure and resilient infrastructure, providing a safe environment for employees, service users and stakeholders to conduct their business in the knowledge that their critical data remains safe in an ever-changing digital world.

www.cyberfortgroup.com

For more information, please contact us on:

01304 814800

info@cyberfortgroup.com