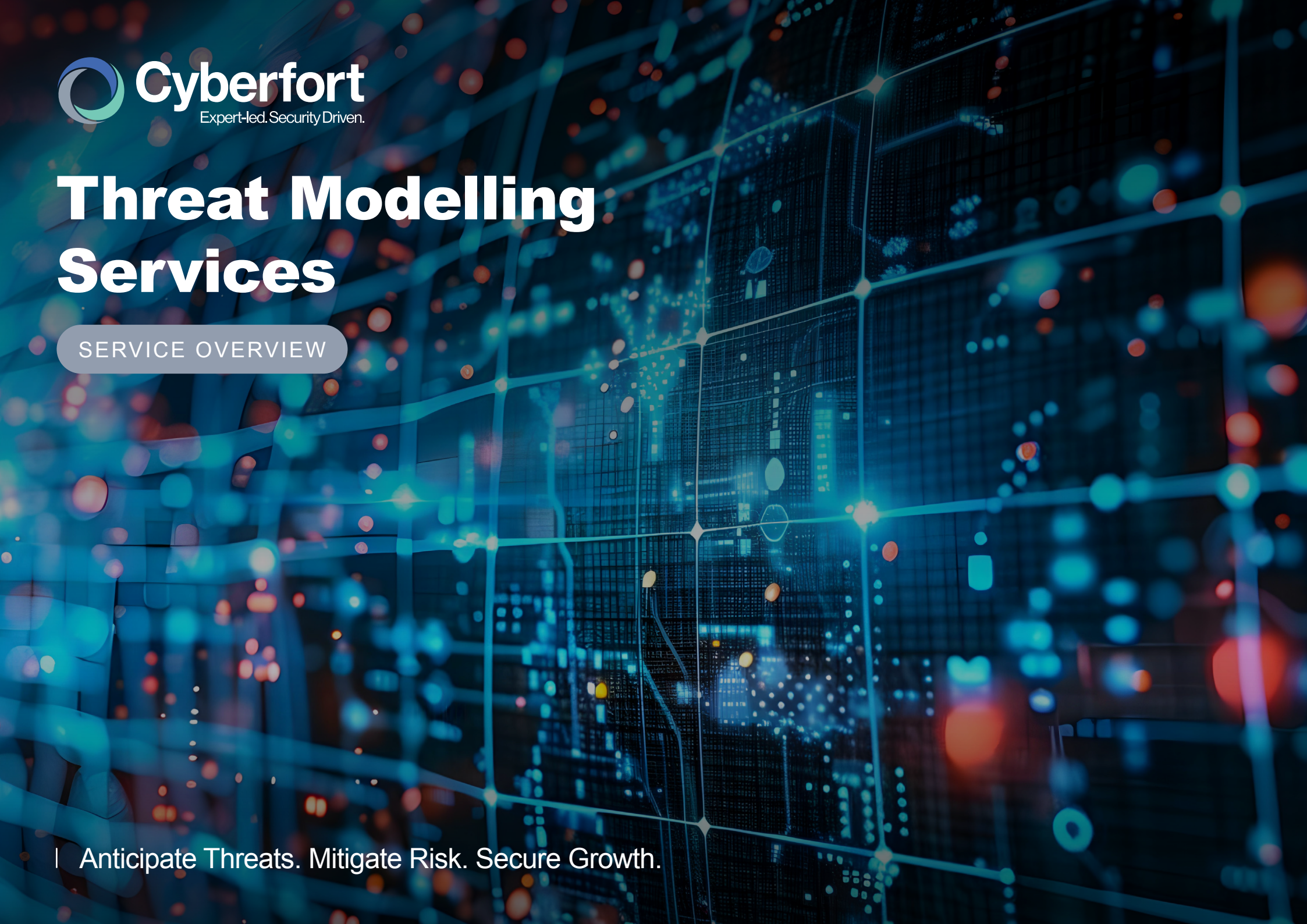

Cyberfort
Expert-led. Security Driven.
Threat Modelling Services
SERVICE OVERVIEW
Anticipate Threats. Mitigate Risk. Secure Growth.

The Reality Every Organisation Is Facing

It usually starts with progress.

A new platform is launched.
A cloud migration accelerates delivery.
An AI capability is introduced to drive efficiency or insight.

On the surface, everything is working as intended. The business is moving faster, becoming more competitive, more connected, more capable.

But beneath that progress, something else is happening.

Every new integration, every system dependency, every dataset, and every AI interaction is quietly expanding the organisation's attack surface.

And unlike the past, threats are no longer random.

They are deliberate. Targeted. Patient.

Attackers are no longer simply trying to "get in." They are trying to disrupt operations, exploit trust, and create measurable business impact.

The uncomfortable truth is this

Most organisations don't fully understand how they could be attacked - until it happens.

From Blind Spots to Visibility

One Cyberfort client came to us after a period of rapid transformation. They had embraced cloud technologies, integrated third-party platforms, and were beginning to explore AI-driven automation. From a business perspective, the transformation was a success.

But when we asked a simple question:

"If you were an attacker, where would you start?"

There was no clear answer.

Not because the organisation lacked security controls. But because they lacked a joined-up view of risk.

This is the gap that threat modelling fills.

It doesn't just identify vulnerabilities. It tells the story of how your organisation could realistically be attacked - step by step, across systems, processes, and people.

And once you can see that story, you can change it.

Why Traditional Security Falls Short

Most organisations have invested heavily in cyber security.

They have tools. Controls. Policies. Frameworks.

But these are often deployed in isolation, designed to solve specific problems rather than provide a holistic understanding of risk.

The result?

- **Security controls that exist but aren't aligned to real threats**
- **Investments that don't deliver proportional risk reduction**
- **Gaps that sit between systems, teams, or responsibilities**
- **A reliance on reacting to incidents rather than preventing them**

In this model, security becomes reactive.
And reactive security is always one step behind.

Cyberfort's Threat Modelling service shifts that position.

It gives organisations the ability to step into the attacker's perspective, understand the paths they would take, and break those paths before they can be exploited.

Seeing Your Organisation Through an Attacker's Eyes

Imagine an attacker targeting your organisation.

They don't see departments or organisational charts. They see opportunity.

They see:

- **A supplier with weaker controls that provides a backdoor into your environment**
- **An employee account with excessive access that can be exploited**
- **An AI system connected to sensitive data without sufficient guardrails**
- **A monitoring gap that allows them to move undetected**

Individually, these may seem manageable. But attackers don't think in silos - they think in sequences.

Threat modelling connects these dots.

It maps how small weaknesses combine into credible, high-impact attack paths, the kind that lead to operational disruption, data compromise, or financial loss. And crucially, it allows you to stop those paths early.

Cyberfort
Expert-led. Security Driven.

The Risks That Matter Most

Across organisations, certain patterns emerge, not theoretical risks, but real-world issues that consistently lead to impact. We see:

Businesses brought to a standstill by ransomware, not because controls didn't exist, but because the attack path was never fully understood.

Supply chain dependencies introducing unseen exposure - where trust is extended without full visibility of risk.

Identity as the weakest link - where a single compromised credential can unlock critical systems.

Monitoring capabilities that generate alerts, but not insight - allowing attackers to operate undetected.

And increasingly, we see AI introducing a new category of risk entirely.

The AI Shift - Innovation Meets Exposure

AI is transforming how organisations operate.

It is accelerating decision-making, automating processes, and unlocking new capabilities. But it is also introducing risks that don't behave like traditional security challenges.

In many organisations, AI adoption is outpacing governance.

Employees experiment with tools.
Teams integrate AI into workflows.
Systems connect to data in new and sometimes uncontrolled ways.

This creates exposure that is often invisible.

- Sensitive information can be leaked through prompts.
- Outputs can be manipulated through prompt injection.
- AI systems can be granted access far beyond what is necessary.

And because these risks are new, they are often not captured by existing controls.

Cyberfort helps organisations bring AI back under control, not by slowing adoption, but by ensuring it is secure by design.

Building a Capability, Not Just Delivering a Report

One of the most common frustrations organisations face is receiving a security assessment that quickly becomes outdated.

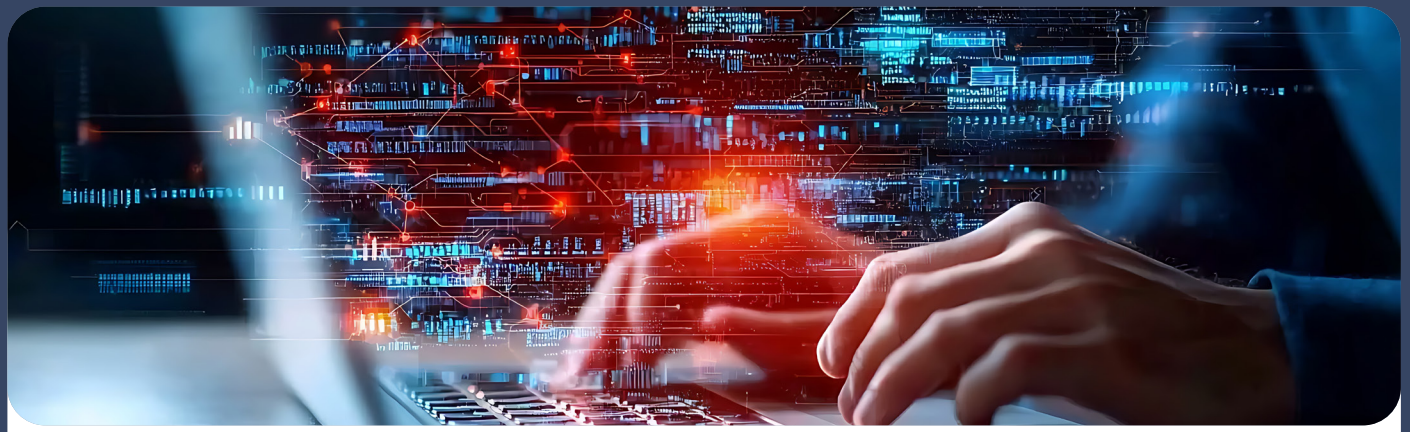
Threat modelling should not be a one-off exercise.

It should be a capability, something that evolves with your organisation as systems change, new technologies are adopted, and new risks emerge.

Cyberfort works with your teams to embed this capability into your operating model.

We make threat modelling repeatable. Scalable. Aligned to development, architecture, and AI governance processes.

So that security is not revisited after decisions are made, but informs them from the start.



What Changes When You Get This Right

When organisations adopt a threat modelling approach, something shifts.

Decisions become clearer.

Instead of asking, “Are we secure?” - they ask,“Where are we most exposed, and what matters most to fix?”

Security investment becomes more efficient, because it is based on real risk, not assumptions.

Innovation accelerates, because risks are identified early, not late, when they are more costly to address.

Incidents become less disruptive, because the organisation understands where they are most likely to occur and how to respond.

And perhaps most importantly, security becomes part of the business conversation - not separate from it.

The Measurable Impact

Organisations that work with Cyberfort consistently achieve:

- Reduced exposure to high-impact threats
- Faster, more confident decision-making
- Lower cost of remediation through early intervention
- Improved operational resilience
- Stronger alignment between business, technology, and security teams
- The ability to adopt AI and new technologies without increasing unmanaged risk

This is not just improved security
It is improved business performance.

Cyberfort
Expert-led. Security Driven.

Why Cyberfort

Cyberfort combines deep technical expertise with a clear understanding of commercial priorities.

We know that security cannot exist in isolation. It must support delivery, enable innovation, and align to business outcomes.

That is why our approach is always:

- Tailored to your organisation
- Focused on real-world risk
- Designed to deliver practical, actionable outcomes

Built to support long-term capability, not short-term fixes

We don't just help you understand risk.
We help you take control of it.

Cyberfort
Expert-led. Security Driven.

A Different Starting Point

The organisations that succeed in today's environment are not those that avoid risk entirely.

They are the ones that understand it clearly, realistically, and in the context of their business.

Threat modelling gives you that understanding.
It allows you to see your organisation as an attacker would.

To identify the paths they would take.
And to close them before they are ever used.

Get Started

The pace of change is not slowing.
Neither are the threats.

But with the right approach,
risk does not have to be a barrier.

It can be managed.
Reduced.
Controlled.

And in doing so, it can enable you to move faster, with confidence.

Adopt AI without compromise.
Turn uncertainty into control.
Build growth securely.

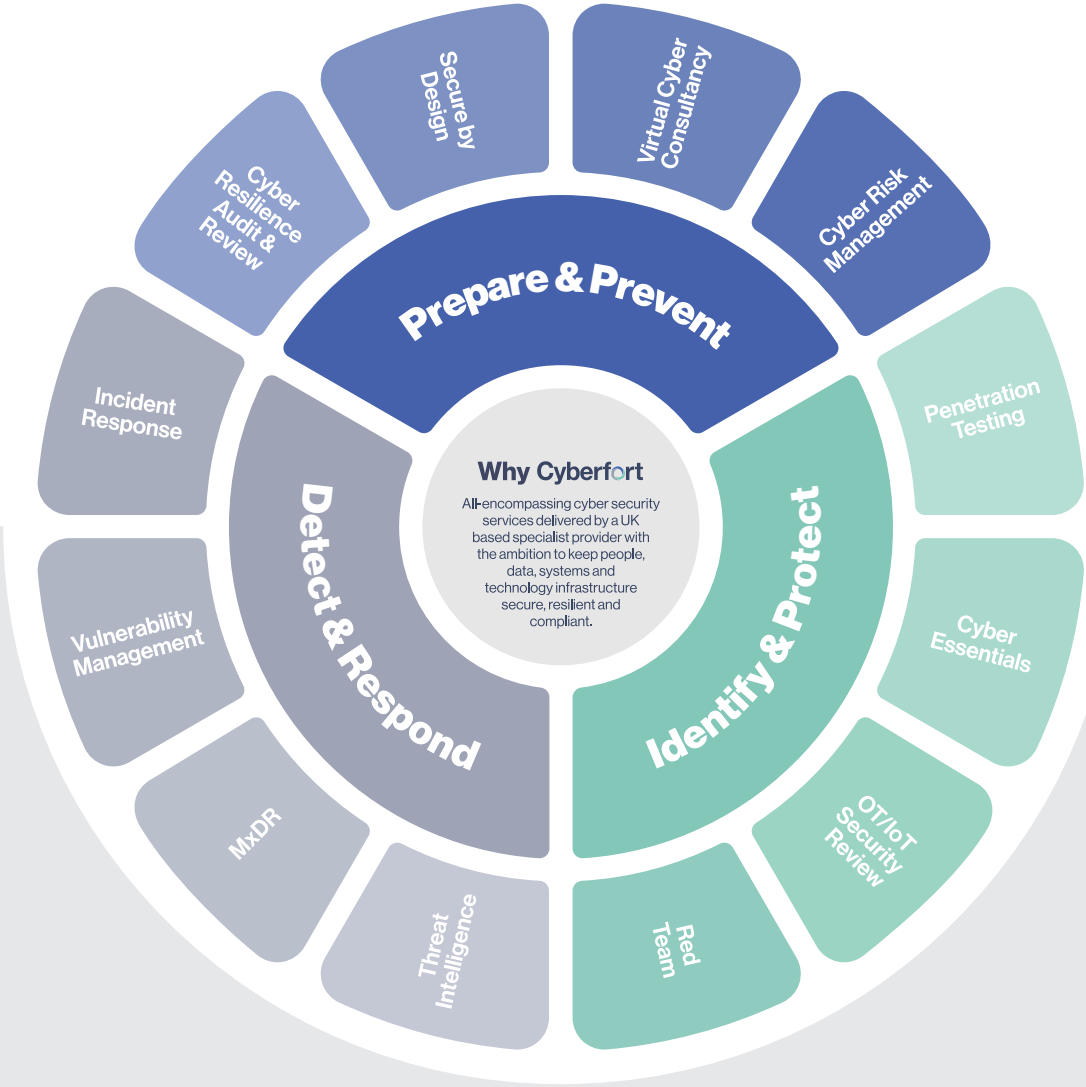
With Cyberfort Threat Modelling Services.

Discover more about Cyberfort's 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 cyberattacks, and proactive Detection and Response to security incidents through our 24/7 security operations centre.

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.



For more information on our Threat Modelling services please contact us at the details below:

+44 (0)1304 814800 | info@cyberfortgroup.com | https://cyberfortgroup.com

We look forward to working with you

Cyberfort
Expert-led. Security Driven.