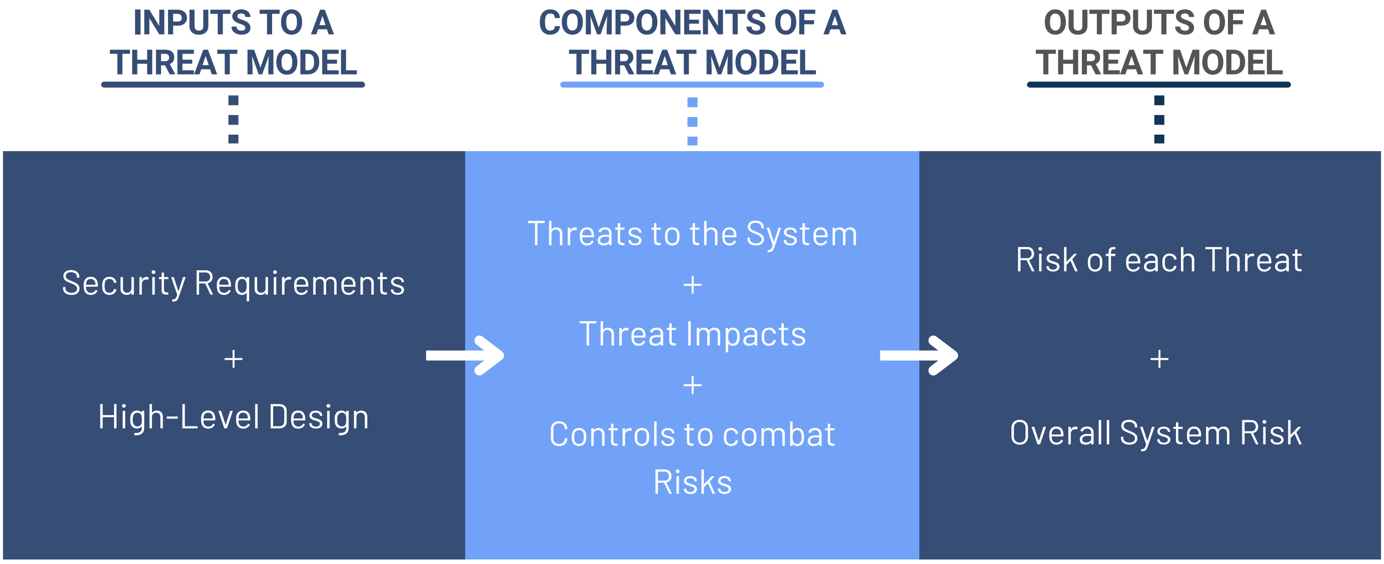
**JONNY TYERS**
**Cyber Security Consulting**

# WHAT IS A THREAT MODEL

The threat model acts as a centrepiece in shifting security left for the modern tech business, and it’s used across the leading tech firms right up to the major cloud providers.

Threat models capture security risks, threats, controls and impacts for a system. It is the “fact sheet” from which all other security decisions and insights can derive. They have great power in capturing this security knowledge in a single place and communicating it efficiently to different teams who are looking for different levels of detail.

Threat models also provide great strategic value in providing a view of security risks across a vast, complex technology estate, and aiding decision-making around investment in controls to reduce that risk where most needed.



INPUTS TO A THREAT MODEL

Security Requirements
+
High-Level Design

COMPONENTS OF A THREAT MODEL

Threats to the System
+
Threat Impacts
+
Controls to combat Risks

OUTPUTS OF A THREAT MODEL

Risk of each Threat
+
Overall System Risk

The threat model determines the level of risk and provides the explanation, or source, of that risk through the context of threats, impacts and controls. This risk-driven approach ensures controls and other security work is focused on reducing business risks that matter.

## THE COMPREHENSIVE SOLUTION TO SHIFTING LEFT

Developing a threat model allows you to integrate security implementation in the early stages of your software development lifecycle. By identifying risks in advance, issues are resolved before applications go live, reducing costs and speeding up delivery. Failing to identify risks in advance of go-live exposes the business to up to 15x the costs to fix each risk identified*

*IBM Systems Sciences Institute research*

# THE BENEFITS OF THREAT MODELLING

**RISK-DRIVEN SECURITY**

Our risk-first approach avoids limited security resources being spent mitigating low-risk threats, instead enhancing the value security provides to the business by focussing on reduction of business risks only.

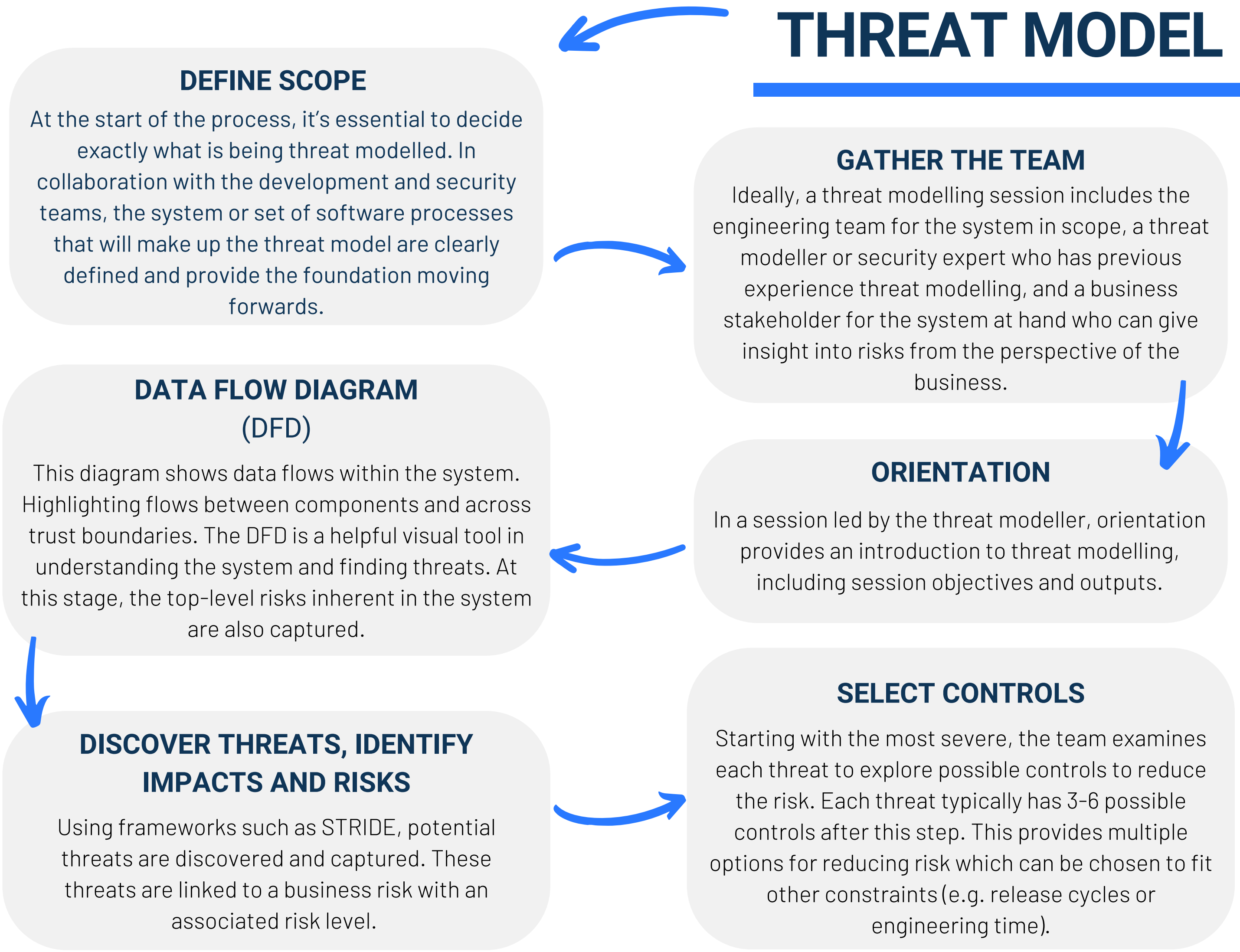
**CLEAR COMMUNICATION**

A comprehensive threat model enables different teams to communicate threats, risks and controls in both a detailed and straightforward manner, ensuring that everyone can work together, regardless of technical ability and know-how.

**RISK MANAGEMENT**

Our approach to threat modelling puts risk first and presents it in a form that's easy to understand regardless of the reader's technical know-how. For readers that require it, the threat model sets out the detail behind each risk, making it both a tactical and strategic asset. It is also possible to use threat models to measure and manage risk across groups of systems, for example to capture risk across a whole line of business.

# BUILDING A THREAT MODEL



### DEFINE SCOPE

At the start of the process, it's essential to decide exactly what is being threat modelled. In collaboration with the development and security teams, the system or set of software processes that will make up the threat model are clearly defined and provide the foundation moving forwards.

### GATHER THE TEAM

Ideally, a threat modelling session includes the engineering team for the system in scope, a threat modeller or security expert who has previous experience threat modelling, and a business stakeholder for the system at hand who can give insight into risks from the perspective of the business.

### ORIENTATION

In a session led by the threat modeller, orientation provides an introduction to threat modelling, including session objectives and outputs.

### DATA FLOW DIAGRAM (DFD)

This diagram shows data flows within the system. Highlighting flows between components and across trust boundaries. The DFD is a helpful visual tool in understanding the system and finding threats. At this stage, the top-level risks inherent in the system are also captured.

### DISCOVER THREATS, IDENTIFY IMPACTS AND RISKS

Using frameworks such as STRIDE, potential threats are discovered and captured. These threats are linked to a business risk with an associated risk level.

### SELECT CONTROLS

Starting with the most severe, the team examines each threat to explore possible controls to reduce the risk. Each threat typically has 3-6 possible controls after this step. This provides multiple options for reducing risk which can be chosen to fit other constraints (e.g. release cycles or engineering time).

jonnytyers.co.uk