PASTA Threat Modeling

PASTA stands for **Process for Attack Simulation and Threat Analysis**. It is a **risk-based threat modeling framework** used to identify threats from both business and technical perspectives. It allows organizations to simulate real-world attacks and prioritize mitigation strategies based on business impact and likelihood.

Risk-centric threat modeling method, meaning that risk plays a central role and the focus is on the highest and most relevant risks that can affect your business.
most efficient because it operates strategically and uses security input from operations, governance, architecture, and development as crucial decision-making tools.

Qualities:

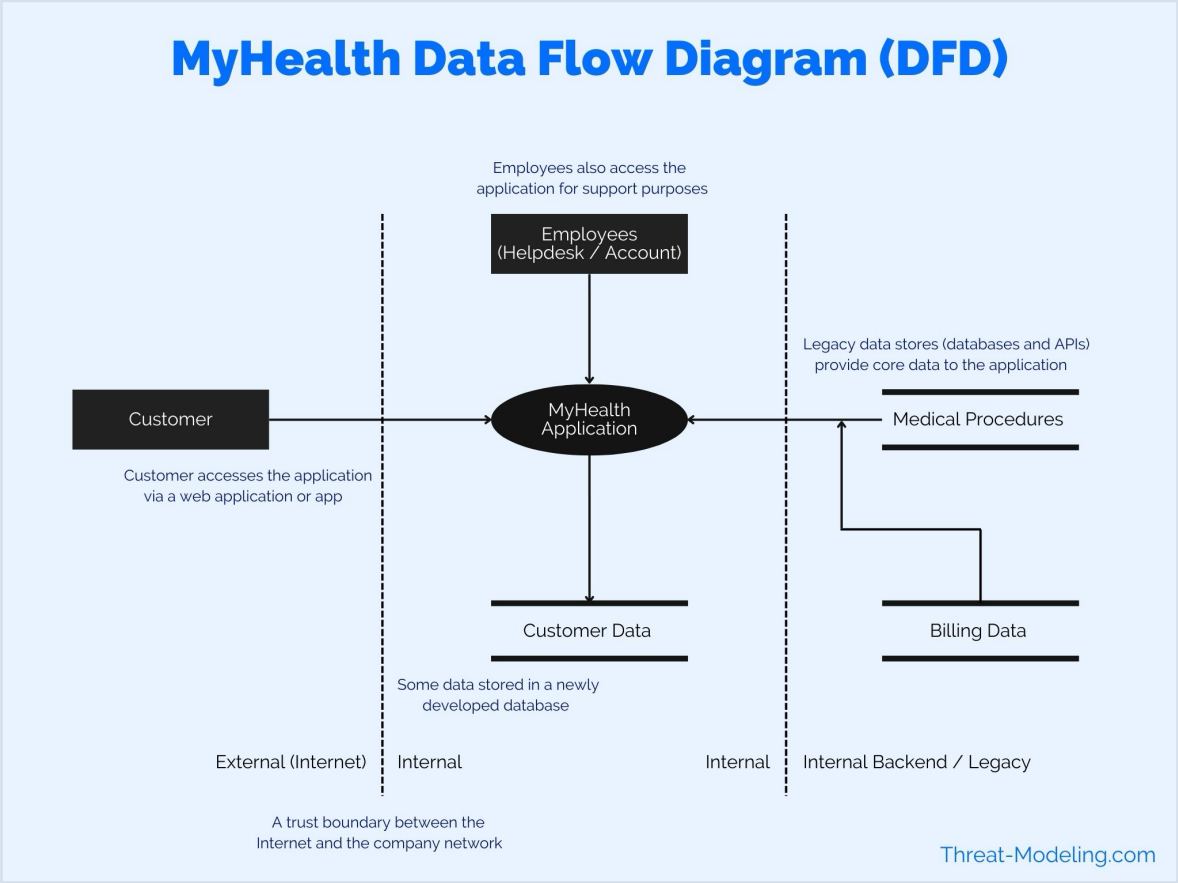
a) Risk centric
b) Collaboration across domains
c) Contextualized
d) Capable of simulations

7 stages of PASTA threat modeling:

1. Define the Objectives
2. Define the Technical Scope
3. Decompose the Application
4. Analyze the Threats
5. Vulnerability Analysis
6. Attack Analysis
7. Risk and Impact Analysis

Stage	Name	Purpose
1	**Define Objectives (Business Impact Analysis)**	Understand business objectives, compliance requirements, and risk tolerance.

2	**Define the Technical Scope**	Identify application components, technologies, boundaries, and interfaces.
3	**Application Decomposition and Analysis**	Break the application into parts (data flows, assets, roles, use cases). Similar to DFDs in STRIDE.
4	**Threat Analysis**	Identify potential threat agents and attack vectors. Use intelligence sources and attacker models.
5	**Vulnerability and Weakness Analysis**	Map threats to system weaknesses (e.g., known CVEs, design flaws, misconfigurations).
6	**Attack Modeling and Simulation**	Simulate attacks and assess impact and likelihood. This step often involves threat intelligence and kill chain mapping.
7	**Risk and Impact Analysis**	Evaluate risk based on business impact, likelihood, and exposure. Prioritize remediation.



EXTRA

1. PASTA vs STRIDE vs DREAD

   PASTA is risk-based and business-driven.
   STRIDE is a threat classification model.
   DREAD is a risk rating model.

2. In Stage 3 (Application Decomposition), what kind of diagrams or data do you use?

   DFDs (Data Flow Diagrams)
   Architecture diagrams
   Deployment diagrams
   Entity-Relationship models
   Use-case diagrams