Threat Model Ranking:

What it mean  
  
During software design, threat modeling helps **find the most important parts** of your system or app. It checks for **possible dangers** to those parts.  It then **ranks those threats** based on how much damage they could cause to your business.

i) DREAD method:

|  |  |  |
| --- | --- | --- |
| **Letter** | **Meaning** | **What It Checks** |
| D | **Damage** | How bad would the attack be if it happened? |
| R | **Reproducibility** | Can the attack be repeated easily? |
| E | **Exploitability** | How easy is it to carry out the attack? |
| A | **Affected Users** | How many people would be impacted? |
| D | **Discoverability** | How easy is it to find the weakness or vulnerability? |

ii) CVSS method:

**How easy is it to exploit the threat?**

* **Does it require user interaction?**
* **How does it affect the system—confidentiality, integrity, availability?**
* **Is the threat local or can it be done remotely?**

**iii) CWSS Method**

CWSS stands for Common Weakness Scoring System. It is used to measure the severity of software weaknesses.

CWSS considers factors like:

* **Business Impact:** How does the weakness affect the organization?
* **Likelihood of Exploit:** How likely is it that the weakness will be exploited?
* **Technical Impact:** What damage can the weakness cause to the system?

CWSS scores help organizations focus

**Threat Model Execution Phases**

**What is threat modeling diagram?**

A threat modeling diagram is a visual tool used to map out how a system works and where potential security threats might arise. It helps teams understand the flow of data, identify weak points, and plan defenses before attackers can exploit them

**How do you create a threat model diagram?**

**🛠️ Steps to Create a Threat Model Diagram:  
 Define the Scope**

* + **Decide what system, app, or feature you're modeling.**
  + **Identify assets you want to protect (e.g., user data, credentials).**

1. **Choose a Diagram Type**
   * **Most commonly used: Data Flow Diagram (DFD)**
   * **Others include Process Flow Diagrams or Attack Trees**
2. **List System Components**
   * **External entities (users, third-party services)**
   * **Processes (functions, APIs, services)**
   * **Data stores (databases, file systems)**
   * **Data flows (how data moves between components)**
3. **Draw the Diagram**
   * **Use symbols: circles for processes, rectangles for entities, open-ended rectangles for data stores, arrows for data flow.**
   * **Mark trust boundaries—lines where the level of trust changes (e.g., between user and server).**
4. **Identify Threats**
   * **Apply models like STRIDE, DREAD, or CVSS to each component and data flow.**
   * **Ask: What could go wrong here? Who might exploit it?**
5. **Review and Iterate**

* **Validate with your team.**
* **Update the diagram as the system evolves.**

**🛠️ 1. Define Security Requirements**

* **Understand what you're protecting and why**
* **Set goals like confidentiality, integrity, and availability**
* **Example: “User data must be encrypted at store and in move”**

**🧭 2. Create an Application Diagram**

* **Map out your system visually**
* **Include external entities, processes, data stores, and data flows**
* **Helps you see how everything connects and where threats might sneak in**

**⚠️ 3. Identify Threats**

* **Use models like STRIDE or DREAD to spot potential risks**
* **Ask questions like: “Can someone spoof a user?” or “What if this API is misused?”**
* **Think like an attacker to uncover weak spots**

**🛡️ 4. Mitigate Threats**

* **Plan defenses for each threat you found**
* **Examples: input validation, encryption, access controls, rate limiting**
* **Prioritize based on risk scores (like DREAD, CVSS, CWSS—just like you’ve got on your page!)**

**✅ 5. Validate and Review**

* **Test your mitigations—did they actually fix the problem?**
* **Update your threat model as the system evolves**
* **Make this a regular part of your development cycle**

**A diagram of a threat modeling process

AI-generated content may be incorrect.**

**There are a number of symbols that are used in DFDs for threat modelling**

**A close-up of a chart

AI-generated content may be incorrect.**

**Diagram of a diagram of a library

AI-generated content may be incorrect.**