Risk & Threat Modelling Platform

---

1. Purpose of the Software

The **Risk & Threat Modelling Platform** (RTMP) is a specialized application designed to assist cybersecurity professionals, developers, and architects in systematically identifying, analyzing, and mitigating potential security risks and threats within software systems and IT infrastructure. The platform provides a structured framework for creating threat models, visualizing data flows, and documenting vulnerabilities. Its primary purpose is to integrate security into the early stages of the software development lifecycle (SDLC), enabling proactive risk management and reducing the cost of addressing vulnerabilities later in the process. The RTMP serves as a central repository for all security-related design decisions and risk assessments.

---

2. Users and Usage Scenarios

The RTMP will be used by a range of technical and non-technical stakeholders involved in the design, development, and security of software systems. The key user roles and their usage scenarios are as follows:

- **Security Architect/Analyst:** The security architect is a primary user who creates and manages threat models from scratch. They use the platform to diagram the system's architecture, identify trust boundaries, and apply established threat frameworks (e.g., STRIDE, OWASP Top 10) to pinpoint potential attack vectors. They also use it to generate security requirements for the development team.
- **Software Developer:** Developers will use the platform to consult existing threat models for the features they are building. They can review identified threats and the corresponding mitigation strategies to ensure their code is secure. They may also be required to update the threat model as new features are implemented or the system's architecture changes.

- **Project Manager:** Project managers will use the platform for a high-level overview of security risks associated with a project. They can track the status of identified threats, monitor the progress of mitigation efforts, and use the risk data to inform project timelines and resource allocation.
- **Auditor/Compliance Officer:** This user role will use the platform to review threat models and security documentation as part of an audit or compliance check. The platform's reporting features enable them to verify that security best practices have been followed and that risks are being appropriately managed.

---

3. Main Functionalities

The RTMP will include the following core functionalities:

- **Threat Modelling and Diagramming:** The platform will provide an intuitive, drag-and-drop interface for users to visually represent system components, data flows, and trust boundaries. Users can model the application's architecture and apply automated or manual threat analysis to generate a list of potential threats.
- **Threat Library and Frameworks:** A built-in, customizable library of known threats, vulnerabilities, and attack patterns will be available. The system will support standard threat classification frameworks such as **STRIDE** (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) to guide users in their analysis.
- **Risk Assessment and Prioritization:** The software will allow users to assess the likelihood and impact of each identified threat. It will use this data to calculate a risk score and help prioritize which threats need immediate attention. This feature enables teams to focus on the most critical security issues.
- **Mitigation Tracking:** For each threat identified, the platform will allow users to document and track the proposed mitigation strategies. This includes assigning a responsible party, setting a due date, and tracking the status of the mitigation (e.g., **"To Do," "In Progress," "Completed"**).

- **Reporting and Documentation:** The platform will generate comprehensive reports that summarize the threat model, list all identified threats, and outline the mitigation plan. These reports can be exported in various formats (e.g., PDF, CSV) to be shared with stakeholders and used for compliance purposes.
- **Version Control and History:** The system will automatically track changes to each threat model, allowing users to view a complete history of modifications. This ensures an auditable trail of all security decisions and changes to the system's threat landscape.
- **Collaboration Features:** The platform will enable multiple users to work on a single threat model simultaneously. Features like comments, notifications, and user roles will facilitate collaboration among different team members and departments.