The STRIDE Threat Modeling of all the DFD elements are as follows:

**DFD Element: Processes**

|  |  |  |
| --- | --- | --- |
| **Threat** | **Description of Threat Events/Scenarios and Impact** | **Mitigation Techniques** |
| ***Spoofing*** | Attackers spoof the identity of legitimate users to gain unauthorized access. | Use strong authentication (e.g., MFA), enforce strong password policies, use SSL certificates. |
| ***Tampering*** | Attackers modify the code or analysis results during the static code analysis process. | Implement proper input validation, use checksums/hashes, employ code signing. |
| ***Repudiation*** | Users deny performing certain actions within the static code analysis process. | Implement logging and auditing mechanisms. |
| ***Information Disclosure*** | Sensitive information is exposed during the static code analysis process. | Encrypt data in transit and at rest, enforce access controls. |
| ***Denial of Service*** | Attackers overload the system with requests, causing the process to become unavailable. | Implement rate limiting, use robust infrastructure, employ load balancing. |
| ***Elevation of Privilege*** | Attackers gain higher privileges, allowing them to control the process. | Apply the principle of least privilege, use role-based access control, review and update access permissions regularly. |

**DFD Element: Interactors**

|  |  |  |
| --- | --- | --- |
| **Threat** | **Description of Threat Events/Scenarios and Impact** | **Mitigation Techniques** |
| ***Spoofing*** | Attackers spoof the identities of legitimate users to gain unauthorized access. | Use strong authentication (e.g., MFA), enforce strong password policies, implement CAPTCHA. |
| ***Repudiation*** | Users deny performing certain actions within the system. | Implement logging and auditing mechanisms, secure logs from tampering. |

**DFD Element: Data Flows**

|  |  |  |
| --- | --- | --- |
| **Threat** | **Description of Threat Events/Scenarios and Impact** | **Mitigation Techniques** |
| ***Tampering*** | Attackers modify data in transit between components of the system. | Use secure communication protocols (HTTPS, SSL/TLS), implement data integrity checks, validate data at client and server sides. |
| ***Information Disclosure*** | Sensitive information is exposed during data transmission. | Encrypt data in transit (HTTPS, SSL/TLS), enforce access controls, use VPNs. |
| ***Denial of Service*** | Attackers flood the system with excessive requests, disrupting normal data flows. | Implement rate limiting, use load balancing, deploy WAFs. |

**DFD Element: Data Stores**

|  |  |  |
| --- | --- | --- |
| **Threat** | **Description of Threat Events/Scenarios and Impact** | **Mitigation Techniques** |
| ***Tampering*** | Attackers modify or corrupt data stored in the system's databases. | Implement strong access controls, use database encryption, perform regular integrity checks, maintain backups. |
| ***Information Disclosure*** | Sensitive data stored in the system's databases is accessed by unauthorized users. | Encrypt data at rest, enforce strict access controls, use database activity monitoring. |
| ***Denial of Service*** | Attackers overload the database with excessive requests, making it unavailable. | Implement database load balancing, use query optimization, deploy database firewalls. |