|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Threat ID | Threat | Threat Type | Impact | Likeli-hood | Risk Treatment Strategy | Action Plan | Owner | Deadline |
| T01 | Astro data tampering through interception | Tampering | 5 | 2 | Mitigation | Data must be encrypted and verified with other ground stations. | Development team | Sprint 1 |
| T02 | Database manipulation | Tampering | 4 | 2 | Mitigation | Database should not be accessible by anyone other than admins. Logs will also be kept. | Development team/ IT team | Sprint 1 |
| T03 | Denial of service | Denial of service | 5 | 2 | Mitigation | Implementation of a Web Application Firewall and only approved of data from approves IPs | DevOps | Sprint 2 |
| T04 | Spacecraft Metrics Manipulation | Tampering / repudiation | 5 | 3 | Mitigation | Ensure that data cannot be altered other than admins, ensure that the system removes old data automatically. | IT Team/ Development Team | Sprint 2 |
| T05 | Staff research data alteration | Repudiation/ tampering | 3 | 2 | Mitigation | Logs of all transactions and access in the database will be kept | Security Engineer | Sprint 3 |
| T06 | Malicious User Gaining Access | Repudiation | 4 | 2 | Mitigation | Logs of all user activity will be kept | Security Engineer | Sprint 3 |
| T07 | Spoofed login pages | Spoofing | 3 | 2 | Mitigation /training | Only approved sites will be accepted and IPs will be tracked. The network will also remain closed. MFA is required for system use. | Security Engineer/ Development team | On-going |
| T08 | Data leak | Information disclosure | 3 | 2 | Mitigation | Minimum access privilege should be applied to reduce damage. | IT team | On-going |
| T09 | Wrong permissions | Elevation of privilege | 5 | 1 | Mitigation | Minimum access privilege should be applied. | Security engineer | On-going |