# Risk Register – Antivirus System (FYP)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | Risk Description | Likelihood | Impact | Severity | Owner | Mitigation Strategy |
| 1 | Scanner fails on hidden/system files | High | Medium | High | Dev Team | Use safe system calls, add error handling for inaccessible files |
| 2 | Malware not detected due to outdated signature DB | High | High | Critical | Dev Team | Regularly update local DB, allow manual DB refresh |
| 3 | False positive classification (non-malware flagged) | Medium | High | High | Dev Team | Implement confidence thresholds, log suspected cases separately |
| 4 | Antivirus falsely quarantine critical system/user files | Medium | High | High | Dev Team | Require user confirmation for critical paths, simulate during testing |
| 5 | Signature DB file gets corrupted or unreadable | Medium | Medium | High | Dev Team | Add DB integrity check on load; keep backup DB copy in project |
| 6 | Scan fails on large directories with deep nesting | Medium | Medium | Medium | Dev Team | Set recursion limits, notify user if exceeded |
| 8 | Quarantine folder access denied or blocked | Medium | Medium | Medium | Dev Team | Create quarantine folder at install; request admin rights on use |
| 9 | Log files not created or missing entries | Medium | Medium | Medium | Dev Team | Implement consistent structured logging (e.g. JSON); verify write success |
| 10 | Multiple scans may cause file system lag | Low | Medium | Medium | Dev Team | Restrict concurrent scans; optimize scan timing or threading |
| 11 | Lack of real-time feedback may frustrates user | Medium | Low | Medium | Dev Team | Show simple progress bar or scanned file count in terminal |
| 12 | Classifier behaves unpredictably due to unseen file types | Medium | Medium | Medium | Dev Team | Add fallback handling for unknown extensions or missing metadata |