Test Plan

PC- THREAT MONITORING

Prepared by: Anto

**Status: Final Version**

Version: 1.0

Last Updated: 03/03/2021

Audience:

The intended audience for this Test Plan document includes:

* Members of the Threat Monitoring software team

Change Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Editor** | **Change Description** |
| 03/03/2021 | 0.1 | Anto | Final Update |

Small

Packet

Table of Contents

[1 Introduction / Project Scope 4](#_Toc20922072)

[2 Functional System Test Plan 5](#_Toc20922073)

[2.1 Test Strategy 5](#_Toc20922074)

[2.2 Test Coverage and Requirements Traceability 5](#_Toc20922075)

[2.3 Testing Scope 5](#_Toc20922076)

[2.3.1 In Scope Items 5](#_Toc20922077)

[2.3.2 Out of Scope Items 6](#_Toc20922078)

[2.3.3 Systems Impacted 7](#_Toc20922079)

[2.4 UI Test Automation 7](#_Toc20922080)

[2.5 Data Validation by manual testing 7](#_Toc20922081)

[2.6 Testing Risks and Mitigations 8](#_Toc20922082)

[2.7 Testing Assumptions 8](#_Toc20922083)

[2.8 Test Environment 9](#_Toc20922084)

[2.9 Test Data 9](#_Toc20922085)

[2.10 Test Phases 9](#_Toc20922086)

[2.11 Test Browsers 9](#_Toc20922087)

[2.12 Test Tools 10](#_Toc20922088)

[2.13 Entry and Exit Criteria 10](#_Toc20922089)

[2.13.1 System Test Entry Criteria 10](#_Toc20922090)

[2.13.2 System Test Exit Criteria 10](#_Toc20922091)

[2.14 Testing Responsibility Matrix 11](#_Toc20922092)

[2.15 Testing Strategies for Testing Phases other than Functional System Test 11](#_Toc20922093)

[2.15.1 Unit Testing 11](#_Toc20922094)

[2.15.2 Integration Testing 12](#_Toc20922095)

[2.15.3 User Acceptance Testing 12](#_Toc20922096)

[2.15.4 Performance Testing 12](#_Toc20922097)

[2.15.5 Test Data Management 13](#_Toc20922098)

[2.16 Test Deliverables 13](#_Toc20922099)

[2.17 Testing Timeline / Milestones 13](#_Toc20922100)

[3 Appendix 14](#_Toc20922101)

[3.1 Preventing Production Incidents 14](#_Toc20922102)

[3.2 Defect Management Process 14](#_Toc20922103)

[3.2.1 Use of Quality Center 14](#_Toc20922104)

[3.2.2 Defect Tracking and Resolution 14](#_Toc20922105)

[3.2.3 Defect Priority Levels 14](#_Toc20922106)

[3.2.4 Defect Severity Levels 15](#_Toc20922107)

[3.3 References 15](#_Toc20922108)

[3.4 System Test Deliverables 15](#_Toc20922109)

[3.5 Approvals 16](#_Toc20922110)

1. Introduction / Project Scope

**Problem Statement:**

Threat monitoring reduces insider threat risks and maximizes data protection capabilities. Organizations are in a better position to defend against insider and outsider threats when they have full visibility into data access and usage and can enforce data protection policies to prevent sensitive data loss. As a threat monitoring tool, it will secure the PC processes, transaction and manage the data with proper data integrity.

1. Test Data Driven Test Plan
   1. Test Strategy

Test Strategy identifies the Test Driven methodology, where the whole threat monitor software running based on the test Scripts developed basis on the outlined requirement

* 1. Test Coverage and Requirements Traceability

The project team will capture requirements traceability to ensure that the business requirements are implemented correctly. Capturing requirements traceability to test scripts will be a priority. Each test case will be linked to a requirement.

Details of Test coverage and Requirements Traceability can be found from HP ALM (QC) Project folder.

* 1. Testing Scope
     1. In Scope Items

| **Scope Area** | **Testing Scope** |
| --- | --- |
| **Verify Threat monitoring Data Accuracy** | * Provide the ability to monitor the software processing via threat monitor tool * The software must allow the user to maintain the data in the database for the accuracy * The software must provide the ability to identify if any unwanted process is running on the system * The system must allow the user to start and stop the monitoring software based on the needs * Provide the ability to alert the users via mail communication for any data hacking, attacking. |

* + 1. Out of Scope Items

The following are not planned as part of testing,

* + - * Verification of process is virus attacked or not
      * Database validations
      * Validating the real system data of executable or processing files
  1. API Test Automation
* QA Team will come up the Data Driven framework to automate the threat monitoring data accuracy
  1. Data Validation by manual testing

Team will validate the Data requirements Via Manual Testing – NOT all test cases are executable as some of them written based on the Assumption.

* Validate the processing data storing on cache system for every 60 seconds
* Every after 60 seconds the data should be restored in the cache system
* Emulate the dummy process and verify the data accuracy
* Validate the data recycled in cache system for every 60 seconds

| **S No** | **Risk** | | | **Mitigation Strategy** |
| --- | --- | --- | --- | --- |
| **1** | Delay in Code delivery | | | The QA team will work closely with Development, Business analysts and Business teams, to determine the priority of the code being delivered. |
| **3** | Vacation schedule for key personnel |  |  | Need to be discussed upfront during the project initiation phase. |
| **4** | Incomplete requirements |  |  | Ensure involvement of business users at each stage and signoff is achieved for the documentation created |
| **5** | Change in scope |  |  | Change Management practices will be in place to ensure any change in scope is adequately estimated and reviewed to validate the scope change can be completed within the project timelines. |
| **6** | Defects are not turned around in a timely manner |  |  | The QA team will work closely with all parties of the core team in discussing defects and solutions and prioritization of those defects. Defect triage meetings will be set up for these discussions. |
| **7** | Code is not properly unit tested prior to delivery to QA |  |  | Smoke testing will be executed in the test regions after each build. The results of this test will be used to make the decision of either accepting/rejecting the build for formal test execution. |
| **8** | Environmental issue force the delay of testing |  |  | Work closely with IT teams to ensure the proper set up and availability of the environments needed to support the project |

* 1. Testing Assumptions

|  |  |
| --- | --- |
| **S. No** | **Assumptions** |
| 1 | Assuming threat monitor software will provide the end point which generated the JSON file |
| 2 | Assuming the test driven |
| 3 | Assuming that simple external file will be maintained as the database system |
| 4 | Assuming the UI design, API design to create the test Cases |

* 1. Test Environment

Test Data

* QA team uses the static emulated data for processing the application
  1. Test Phases

**Dev Smoke Testing** – Once Dev Team completes each requirement and passed the unit testing in DEV environment, QA team will do a high-level smoke test in Dev environment to make sure that peace of code is working as expected.

**Integration Testing** – After testing completes of all the modules, QA team start testing End to End with all modules integrated and report defects if found any.

**Regression Testing** – Once all Critical and Major Defects are fixed and closed, QA Team performs the Regression Testing using automation on the latest build to make sure nothing has broken and meeting the expected results.

**User Acceptance Testing** – Once QA team completes the Regression Test and publish the results, UAT will be performed with Business users in coordination with QA & BA Team.

* 1. Test Tools

A combination of test tools may be used to test this project. The following table identifies the test tools and their uses for the purpose of this project:- Assumption

| **Tool** | **Description** |
| --- | --- |
| Quality Center | This tool will be used to document the requirements, Test Scripts and Test Execution Results |
| Java-Framework | java framework will be used to test the threat monitor file |

* 1. Entry and Exit Criteria
     1. System Test Entry Criteria

Prior to the beginning the System Test phase of the project, the following entry criteria must be met:

|  |  |
| --- | --- |
| ***Test Plan*** | Project Team have reviewed and approved the Test Plan. |
| ***Unit test reviews and code reviews*** | Unit test reviews and code reviews have been completed and approved by Development Lead. |
| ***System Access*** | QA team will have accesses to the Test & Dev environments of Threat monitoring software and Database |
| ***System Components*** | All components of the system test environment(s) must be functional and fully available for test execution. |
| ***Test Data*** | System should accept the emulated processing data |

* + 1. System Test Exit Criteria

Prior to exiting the System Test phase of the project, the following exit criteria must be met:

|  |  |
| --- | --- |
| ***Scripts Passing*** | In the final pass, 95% of overall test scripts must be passing and 100% of the critical and high scripts must be passing. |
| ***Critical System Functionality*** | All critical system functionality must operate as defined within the business requirements. |
| ***Defect Discovery Rate*** | The defect discovery rate has dropped to a manageable level, as determined by the project manager, QA team, project sponsor and other project team members. |
| ***Critical or High Severity Defects*** | * All defects with a Critical or High severity must have been resolved prior to UAT. * If any Critical or High severity defects remain open, they **must** have a planned future resolution noted within the Quality Center defect. |

* 1. Testing Strategies for Testing Phases other than Functional System Test
     1. Unit Testing
* The developer writes Unit Test script and share the results with all stakeholders
  + 1. Integration Testing
    2. User Acceptance Testing
    3. Performance Testing
    4. Test Data Management
  1. Test Deliverables

|  |  |
| --- | --- |
| **Deliverables** | **Dependencies** |
| Query Log | List of issues / questions for requirements and design |
| Test Plan | Approval of System Requirements |
| Test Cases | Approval of Design Requirements and Test Plan |
| Test Readiness Review | Approval of requirements, test cases and completion of test preparation. |
| Defect Report | Defect Report with list of defects. |
| Test Summary Report | Completion of Testing. |

* 1. Testing Timeline / Milestones

1. Appendix
   1. Approvals

|  |  |  |
| --- | --- | --- |
| **Role** | **Name** | **Date Approved** |
| Project Sponsor |  |  |
| Service Level Engineer (SLE) |  |  |
| Project Manager |  |  |
| Business Analyst Lead |  |  |
| Business Analyst |  |  |
| Technical Lead |  |  |
| Developer |  |  |
| Test Lead |  |  |
| Test Team |  |  |