|  |  |  |
| --- | --- | --- |
| **Sprint 1 Checklist (Place an ‘X’ for the Items you completed at Basic or higher)** | | |
| **Application Log Analysis** | | |
| **X** | Part A – Collect Application Logs | Basic: Write parsed output to a csv file, few OO concepts |
| **X** | Part B – Alert on an application log event | Basic: Use a hardcoded rule to find error, report to console |
| **System Log Analysis** | | |
| X | Part A – Collect System Logs | Basic: Write parsed output to a csv file, few OO concepts |
| **System Resource Analysis** | | |
| X | Part A – Collect system/resource utilization data | Basic: Output a .csv file with 10 minutes of system checks as timestamped tuples at 20 sec intervals |
| **Data Aggregation** | | |
| X | Part A – Filter Logs | Basic: param is a String used to filter the log |
| **File Replay and Simulation** | | |
| X | Part A – Replay Logs | Basic: Maintain a library of logs, replay captured logs by running it through the log parser and analyzer |
| **Statistical Detection** | | |
| X | Part A - Create a list of 100 numbers with different mean and standard deviations | Basic: generate a list of random numbers with mean= 10 and a sd = 1 and append another list with mean= 50 and a sd = 10 |
| X | Part B – Alert on a change in distribution | Basic: Implement baseline/sliding windows & generate an alert |
| **Rule Based Detection** | | |
| X | Part A - Generates alerts based on rules | Basic: Alerts using rules read from a separate policy config file |
| **Critical File Integrity Checks** | | |
| **X** | Part A – Initialize Hash Table | Basic: Write list to a csv file |

**IDS Project – CSCE 354**

**Sprint 1 Cover Page**

**March XX, 2021**

**Team Number:**

**Estimated hours for entire team:** *(this is not graded, just a data point for me)*

**Team Members with estimated % contribution to the team:** *(List in order of most to least)*

1)

2)

3)

4)

5)

**Team Achievements:** *(Describe what you did beyond the basic functionality)*

**Feedback:** *(Provide any feedback or notes you feel is necessary)*