ISEC 2077 Security Auditing
Assignment 7 – Anomaly Detection

Issued Date: November 25, 2025
Due date: December 9, 2025

Preamble

Logs are of no use if they are never monitored. However, most logs are so large and complex that they do not lend themselves to visual inspection. Instead, we must often develop programs that can search through logs looking for suspicious circumstances (anomalies). In this assignment you will be given a (fictious) log from a card-key access system covering a period of two weeks. The log is a TAB Delimited file where each line records the employee number (20 employees), the day, the month, the hour and minutes carded IN and the day, the month, and the hour and minutes carded OUT. All data is in integer format using a 24-hour clock. Employees are required to card IN and card OUT each day. Ignore the fact that they work seven days a week, this is not relevant. If a value for any time has not been recorded it will be shown as 0.

Requirements

You are required to write a program in the language of your choice which can process this log looking for any anomalies in the card IN and card OUT data.

There are 10 anomalies to detect, which can be found by visual inspection to check your results. HOWEVER, you must use your program to detect them. You must design the method of defining anomalies. For example, an employee carded OUT but never carded IN.

When the program discovers an anomaly, it must report to a file called ANOMALIES.TXT as follows for each anomaly:

First line: Employee Number, Month and Day of Anomaly.

Second line: Description of anomaly. For example, “Employee carded IN but didn’t card OUT”. There is no need to include the quotes.

Third Line: Equals signs to separate the anomalies “==========”

Submission

Load into the dropbox the text file containing the anomaly reports (ANOMALIES.TXT) and a text file containing the source code of your program, FULLY COMMENTED TO DESCRIBE THE FUNCTIONING OF EACH SECTION!

MAKE SURE YOU PLACE A COMMENT BLOCK AT THE TOP OF EACH FILE WHCH CONTAINS YOUR FIRST AND LAST NAME, COURSE CODE (ISEC2077), THE ASSIGNMENT NUMBER (6), CREATION DATE, LAST REVISED DATE.

Rubric

This assignment is worth 20% of your final mark and is marked out of 30 points based on the following Rubric:

Anomalies detect: 0 – 10

Descriptions are accurate: 0 – 10

Program is commented properly: 0 - 10