**ISEC 2077 Security Auditing**
**Assignment 5 (Third Medium Assignment) – Windows Events to NXLog in Json**

Issued Date: November 18, 2025
Due date: December 2, 2025

## Preamble

**Objective:** The purpose of this assignment is transfer Windows event logs to nxlog locally. Centralized log management is key to proper implementation of log management. In this exercise you will use the machine on which your nxlog is installed to import the windows event logs from the same machine and convert those events into json or syslog format (your choice).

## Requirements

To accomplish this task you must modify your nxlog.conf file to contain:

Part 1. the xm_json and syslog extensions

Part 2. an input Module that can retrieve Windows logs from the SECURITY log file (local file on your machine). You must identify the correct local windows log file.

Part 3. an output Module that can convert the Windows log events to json or syslog and direct the result to a new local log file in json or syslog format in a folder where you have write privileges.

Part 4. a Route from the input module to the output module. Display the contents of your Log file (Step 4 below).

Steps.

Step 1. Stop the nxlog service

Step 2. Modify the .conf file

Step 3. Restart the nxlog service

Step 4. Look in the file location specified for the new json or syslog log file and show the contents to your instructor.

## Rubric

This assignment is worth 20% of your final mark and will be evaluated based on in-class demonstration to your instructor and is assessed based on the following Rubric:

Part 1: 10 points

Part 2: 10 points

Part 3: 10 points

Part 4: 10 points