# A blue and white logo AI-generated content may be incorrect. UNIVERSITY OF HERTFORDSHIRE School of Physics, Engineering and Computer Science

MSc in Cyber Security  
7COM1070: Cyber Security Master Project  
27 March 2025

Rule Base Insider Threat Detection System Using SIEM-IDS Correlation

Name: Nirali Ketanbhai Jobanputra  
Student ID: 23034938  
Supervisor: Joseph Spring

# Declaration

This report is submitted in partial fulfilment of the requirement for the degree of:  
Master of Science in Cyber Security, at the University of Hertfordshire (UH).

I hereby declare that the work presented in this project and report is entirely my own, except where explicitly stated otherwise. All sources of information and ideas, whether quoted directly or paraphrased, have been properly referenced in accordance with academic standards. I understand that any failure to properly acknowledge the work of others could constitute plagiarism and may result in academic penalties.

**I did not use human participants in my MSc Project.**

I hereby give permission for the report to be made available on the university website provided the source is acknowledged.

# Abstract

# Table of Contents

**1. Abstract**

1.1 Introduction – The Problem of Insider Threat

1.2 Introduction to the Project – Optimized SIEM-IDS Correlation

1.3 Goals and Objectives

1.4 Research Questions

1.5 Background Research

**2. Introduction**

2.1 Overview of Progress

2.2 Completed Tasks and Deliverables

2.3 Challenges Encountered and Solutions

2.4 Project Management and Timeline

2.5 Evidence of Progress

2.6 Next Steps

**3. Literature Review**

3.1 Ethical Considerations

3.2 Legal Considerations

3.3 Professional Considerations

3.4 Social Considerations

3.5 Summary

**4. Methodology**

4.1 Project Management Approach

4.2 Key Remaining Tasks and Deliverables

4.3 Project Timeline and Tracking

4.4 Quality Evaluation Strategy

**5. Quality and Results**

5.1 Understanding the Challenge and Motivation

5.2 What This Project is Building (Artefact)

* 1. Depth of Research and Complexity

5.4 Testing, Validation, and Experimentation

**6. Evaluation and Conclusion**

**7. References**

**8. Appendix**

Appendix A: System Architecture Diagram

Appendix B: Sample SIEM Correlation Rules

Appendix C: Gantt Chart