Literature Review Outline

Topic: Implementing Cyber Security tools and techniques in crime prediction

Related subtopic: Criminal profiling (a part of criminology)

Introduction (200 words)

This literature review discusses crime prediction using cybersecurity tools and techniques, focusing specifically on cybercrime. Cyber Threat Intelligence (CTI) is introduced as a key cybersecurity strategy that comprises of a range of tools and techniques in predicting cybercrime. Criminal profiling takes human factors into consideration and is relevant in analysing the characteristics of threat actors who partake in cybercrime.

Cybercrime trend analysis (300 words)

Overview of the most common types of cybercrime in the last five to ten years. Key topics:

- Social engineering
- Malware and ransomware
- Artificial Intelligence (AI) and Internet of Things (IoT)

Cybercrime detection and prediction (500 words)

This section describes real-world cybersecurity techniques in cybercrime detection and prediction. Key topics:

- Criminology
- Deviation detection / outlier analysis

- Predictive modelling using data mining, machine learning, CTI and criminal profiling

Cyber Threat Intelligence (CTI) (500 words)

Key topics:

- Strategic, operational, tactical intelligence
    - Tactics, techniques and procedures (TTPs)
    - Indicators of Attack (IOA)
    - Indicators of Compromise (IoC)
- Cyber Kill Chain

Criminal Profiling (200 words)

Key topics:

- Types of threat actors: insider vs external
- Characteristics of threat actor
- Matching threat actor profile to cybercrime

Evaluation of cybersecurity techniques in cybercrime prediction (300 words)

How has the implementation of cybersecurity techniques such as CTI and criminal profiling contributed towards cybercrime prediction and what are key gaps in the future of cybercrime mitigation?

References