Editorial

We release the first issue of this volume of the **Information Security Education Journal** with the following papers.

In the opening paper, "**Interpretable Cyber Threat Detection Using SHAP-Based Explainable AI in Classroom Data Security Systems,"** the authors outlined an interpretable cyber threat detection framework using SHAP-based Explainable AI (XAI) for classroom data security systems. This work used a simulated dataset containing diverse threat categories, including insider threats, phishing, unauthorised access, data breaches, and malware, to develop a transparent, predictive intrusion detection model. The authors found that insider threats (n=218) and phishing attacks (n=204) dominate the threat landscape, underscoring human-centric vulnerabilities over purely technical exploits.

In the next paper, "**Structural and Semantic Analysis of a Cybersecurity Knowledge Graph: Network Topology, Community Detection, and Embedding Insights for Cybersecurity Education,"** the authors introduced AISecKG, a comprehensive cybersecurity knowledge graph dataset comprising 1,460+ entities and 726 semantic relations, designed to bridge the gap between theoretical ontology construction and practical application. They systematically analyzed the graph's structural and semantic properties through network topology metrics, community detection, and embedding techniques. This study validated AISecKG's utility for downstream machine learning tasks, including entity classification and similarity search, while demonstrating its potential to enhance adaptive cybersecurity education.

In the last paper, "**Information Security Education and Incident Analysis: A Holistic Approach in the Digital Era,"** the authors studied the vital role of information security education in mitigating cyber risks, emphasizing that awareness training is a critical investment rather than a cost center. Further, this study presented a detailed analysis of security incidents, categorising them into data breaches, unauthorised access, and information leakage. The study recommended a holistic approach that integrates technological controls, human-centric strategies, and organisational governance.

These papers underscore the need for a comprehensive security education system.

Editors