1. INTRODUCTION

The increasing dynamics and complexity of network traffic have made cybersecurity a critical concern, prompting the use of intelligent solutions such as Artificial Intelligence (AI)-based anomaly detection. Among these, Artificial Neural Networks (ANN) have proven highly effective in identifying intricate patterns within network intrusion data [1, 2]. However, despite their high predictive performance, ANN models often operate as "black boxes," making it challenging for end-users and security analysts to understand the reasoning behind their decisions. In cybersecurity environments, where trust, accountability, and transparency are vital, this opacity can hamper effective threat detection, investigation, and response.

To address this issue, Explainable AI (XAI) methods have emerged as a pivotal solution. Among these, SHapley Additive Explanations (SHAP) have gained prominence for providing both global and local attribution of feature contributions [3, 4]. However, traditional SHAP visualizations — such as summary or style plots — often struggle to effectively capture the complexity and interplay of features in high-dimensional network anomaly detection scenarios [5]. Although prior studies have evaluated the efficiency and interpretability of various SHAP visualizations [6, 7], a systematic comparison focusing on their interpretability, computational efficiency, and visual complexity within the cybersecurity context has yet to be conducted.

This paper aims to fill this gap by systematically assessing five SHAP-based visualizations Bar, Beeswarm, Waterfall, Decision, and Cohort plots. In the context of ANN-based network anomaly detection. We evaluate these methods using five metrics: Time to Insight, Rendering Complexity, Entropy, Edge Density, and File Size. By doing so, this study provides actionable guidelines for cybersecurity researchers and practitioners, facilitating the selection of XAI visualizations best suited for real-time threat detection, forensic analysis, and model transparency. Ultimately, this work aims to bridge the gap between complex ANN-based anomaly detection and the interpretability required for trust, accountability, and effective cybersecurity decision-making.