MIDI 2024 Conference

FortGen IDS: The Fusion of SOAR and Hybrid IDS for Enterprise

Abstract

In this data era, enterprise are encountering rise of challenges in detecting and responding to cyberattacks. There is a need for a sophisticated cyber ap-proach that leverages cutting-edge technologies to fortify against the unex-pected attacks. This paper presents FortGen IDS, a novel cybersecurity solu-tion combining Security Orchestration, Automation, and Response (SOAR) with Hybrid Intrusion Detection Systems (IDS). The primary contribution of FortGen IDS is its innovative algorithm inspired by Genghis Khan's military tactics, enhancing threat detection and response, particularly against Dis-tributed Denial-of-Service (DDoS) attacks. The proposed model leverages ad-vanced automation and orchestration capabilities to provide a more holistic approach to enterprise cybersecurity. Empirical validation studies have been carried out to determine the best algorithm for anomaly detection, also ex-plicitly comparing the performance of FortGen and Hybrid IDS. It helps make businesses' digital defenses stronger against evolving cyber threats. This approach has greater scope in improving cyber-defense in the context of enterprise security, ensuring that firms are well-fortified against potential cyber threats.