IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 1, November 2025
Impact Factor: 7.67

INTRUDEX: Intelligent Honeypot-Based Threat Monitoring System

Ingle Ram Vilas, Jadhav Vaishnav Pravin, Wagh Yashraj Kakasaheb, Prof. Bhor. P. G.
Department of Computer Engineering
Samarth College of Engineering and Management, Belhe, Pune

Abstract: *In today's digital era, cyberattacks have become more frequent, sophisticated, and dam-aging. Organizations face continuous threats from malicious actors targeting sensitive data,critical infrastructures, and online services. Traditional defense mechanisms such as fire-walls and intrusion detection systems often fail to provide deep insights into attacker be-havior.To address this challenge, a Cybersecurity Honeypot Simulation System is proposed, whichacts as a decoy environment to attract, detect, and analyze malicious activities in realtime.The system deploys multi-interaction honeypots that emulate real network services such as SSH, HTTP, and database systems. These traps deceive attackers into interacting with decoy systems, allowing detailed monitoring and data capture of their activities. Us-ing advanced log analysis and machine learning techniques, IntrudeX identifies malicious patterns, classifies attack types, and extracts valuable threat intelligence. The enriched data is visualized through dashboards for better understanding and faster response. The system deploys honeypot environments like SSH and Telnet traps (using tools suchas Cowrie) to lure attackers by mimicking real services. All interactions are logged and securely forwarded to a centralized data pipeline, where Logstash performs parsing and enrichment, including GeoIP tagging of attacker IP addresses. This project demonstrates how honeypots not only function as an early-warning system but also as an intelligence-gathering tool, helping security teams understand evolving attack patterns. By simulating realistic targets while ensuring isolation from production networks, the proposed system offers a cost-effective, scalable, and practical approach for improving cyber defense strategies. Enhancing early threat detection and providing actionable insights into attacker tactics, techniques, and procedures (TTPs). By integrating deception technology with analytics, IntrudeX strengthens cybersecurity resilience and contributes toward developing proactive defense strategies for both enterprise and academic environments.*

Keywords: Cybersecurity Honeypot Simulation System

DOI: 10.48175/IJARSCT-29687