УДК 004.056.53

Securing Kubernetes: Dual-Agent System for Enhanced DoS Attack Detection

Дарвиш Г. (National Research University ITMO**)**

Воробьева Алиса Андреевна - кандидат технических наук, факультет безопасности информационных технологий, доцент
(National Research University ITMO**)**

Введение. With the growing adoption of Kubernetes in modern IT ecosystems, the need for enhanced security mechanisms has become increasingly critical. This work introduces a dual-agent system designed to improve the detection of Denial-of-Service (DoS) attacks in Kubernetes environments. By combining node-level and application-level monitoring, the research establishes a scalable, framework-agnostic solution for proactive threat detection and mitigation.[1].

Основная часть. The cornerstone of this research is the development of a dual-agent architecture comprising two specialized monitoring agents:

- Node-Level Agent: Gathers system metrics such as CPU usage, memory consumption, and network traffic from Kubernetes nodes.
- Application-Level Agent: Collects application-specific data, including logs, API request patterns, and response times, across various frameworks like Flask, Django, FastAPI, Node.js, and Golang.

The integration of these agents ensures comprehensive monitoring, bridging the gap between infrastructure-level and application-level security. Data collected by both agents feeds into a machine learning framework, which leverages advanced classifiers such as Random Forest, XGBoost, and LightGBM. This enables the detection of anomalies indicative of DoS attacks with high accuracy and minimal false positives.

The dual-agent system's framework-agnostic design and scalability make it suitable for diverse Kubernetes environments, ensuring robust performance even in large-scale deployments.[2].

Выводы. In conclusion, the proposed dual-agent system marks a significant advancement in Kubernetes security. Its ability to monitor and analyze both node-level and application-level metrics, combined with machine learning-driven anomaly detection, positions Kubernetes environments to effectively counter evolving cyber threats such as DoS attacks. This research contributes an innovative, scalable, and proactive approach to securing containerized infrastructures, ensuring their resilience in an increasingly dynamic threat landscape.

References:

[1] S. Sultan, I. Ahmad, and T. Dimitriou, "Container security: Issues, challenges, and the road ahead," *IEEE Access*, vol. 7, pp. 52976–52996, 2019, doi: 10.1109/ACCESS.2019.2911732.

[2] C. Tien, T. Huang, C. Tien, T. Huang, and S. Kuo, "KubAnomaly: Anomaly detection for the Docker orchestration platform with neural network approaches," *Eng. Reports*, vol. 1, no. 5, Dec. 2019, doi: 10.1002/eng2.12080.

Автор _____ Дарвиш Г.

Научный руководитель _____ Воробьева А. А.