UDC 004.056.53

Analyzing Resource Usage to Detect Attacks in Kubernetes Environments

Бархоом М (ИТМО)

Научный руководитель – к.т.н., доцент Воробьева А.А. (ИТМО)

Введение

The widespread deployment of the Kubernetes platform as a container management tool has created new security challenges, particularly in detecting the abnormal behaviour of the Decade. Traditional methods often fail to detect attacks targeting resource consumption such as "DoS", requiring more sophisticated solutions. This work aims to collect and analyze host data to develop an intelligent anomaly detection and security pattern analysis system.

Основная часть

The proposed work is based on the deployment of a monitoring agent within Kubernetes nodes to collect critical data using Prometheus and Node Exporter [1], and then sending this data to a central database for analysis and detection of abnormal patterns that may indicate cyberattacks or suspicious activities. Host data will be collected including CPU usage, memory consumption, disk activity, and network movement to ensure accurate performance monitoring and identification of any abnormal resource consumption that may indicate potential threats. This approach allows a careful analysis of contract behavior, which helps improve performance monitoring and enhance infrastructure security.

In addition, advanced machine learning technologies such as Random Forest and AdaBoost will be applied to process data and develop attack detection models [2]. These models are based on analysis of resource consumption deviations, enabling them to distinguish between natural processes and harmful activities. To ensure efficient performance, the proposed model will be evaluated and compared to conventional systems in terms of detection accuracy, false alarm rate, and immediate response to attacks, enhancing the reliability and security of Kubernetes.

Выводы

This work contributes to improving cybersecurity within Kubernetes environments by analyzing host data to detect suspicious activities and attacks. The proposed approach allows continuous monitoring and accurate analysis of resource consumption, providing a strong basis for the development of more efficient and proactive threat detection systems.

Список использованных источников

[1] G. Darwesh, J. Hammoud, and A. A. Vorobeva, “A novel approach to feature collection for anomaly detection in Kubernetes environment and agent for metrics collection from Kubernetes nodes,” *Naučno-teh. vestn. inf. tehnol. meh. opt.*, vol. 23, no. 3, pp. 538–546, Jun. 2023, doi: 10.17586/2226-1494-2023-23-3-538-546.

[2] G. Darwesh, J. Hammoud, and A. A. Vorobeva, “Enhancing Kubernetes security with machine learning: a proactive approach to anomaly detection,” vol. 24, no. 6, 2024.

Автор _____ Бархоом Моттее

Научный руководитель _____ Воробьева Алиса Андреевна