УДК 004.056.53

Securing Kubernetes: Developing an Advanced Monitoring Agent for Enhanced Threat 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 rapid proliferation of Kubernetes in contemporary IT landscapes, the imperative for robust security measures cannot be overstated. This research responds to this need by presenting an advanced monitoring agent designed explicitly to elevate the security posture within Kubernetes environments. By delving into the intricacies of monitoring nodes and applications, the research endeavors to establish a foundation for proactive threat detection[1].

Основная часть. The core of this research lies in the development of an intelligent monitoring agent equipped with sophisticated capabilities. This agent operates as a vigilant sentinel, continuously collecting and analyzing a comprehensive array of metrics from both nodes and applications within the Kubernetes clusters. The goal is to provide real-time insights into system health, enabling the early identification of anomalies indicative of potential security threats.

The gathered dataset becomes a pivotal asset for training a machine learning model tailored to Kubernetes security. By encompassing metrics related to resource utilization, network activities, and application behaviors, the model gains a nuanced understanding of the normal operational patterns. This knowledge forms the bedrock for the model's ability to discern aberrations that may signify security risks, including unauthorized access, unusual traffic patterns, and resource misuse.

The integration of machine learning into the security framework empowers the model to serve as an intelligent and proactive defense mechanism. By identifying patterns associated with known and emerging security threats, the model augments traditional rule-based approaches, providing an additional layer of protection against potential risks. The combination of the monitoring agent and machine learning capabilities promises a heightened level of security in Kubernetes environments[2].

Выводы. In conclusion, the development and integration of an advanced monitoring agent herald a new era in Kubernetes security. The agent's capacity to comprehensively monitor and collect data, coupled with the machine learning model's ability to identify and respond to security threats, positions Kubernetes environments for heightened resilience against evolving cyber threats. This research contributes a tangible and innovative solution to fortify the security posture of Kubernetes deployments, ensuring they are well-equipped to face the challenges of the dynamic modern 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.