A new monitoring agent in the Kubernetes environment for security purposes

Дарвиш Г. (National Research University ITMO)

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

The goal of this work is to propose a new monitoring agent in the Kubernetes system, that can collect security and performance metrics from nodes and export them to our dataset. The collected dataset will be used in the future to come up with a new machine learning module for anomaly detection.

Введение.

Kubernetes is one of the most common open-source container orchestration systems which is used to automate, scale, and manage the software development processes. Despite its widespread support by Google and Cloud Native Computing Foundation, it still faces many security problems. Since Kubernetes is often used in production, an issue such as detecting attacks is a significant hindrance due to the latency. In our quest to build an efficient attack detection system, we present in this work a new Kubernetes monitoring agent with its extractors and customized rules that collect important metrics from cluster nodes. These metrics can be used later to train machine learning models to detect unusual activities on nodes. Our experiments which were conducted on a real production Kubernetes environment in Azure and collected 24 metrics in a reasonable time show that the proposed agent can stream a real-time dataset that can feed a machine learning model working in parallel with the Kubernetes cluster.

Основная часть.

In this work, we developed a new agent service that collects metrics from the Kubernetes nodes and forwards them to a central database. The exported data include the most important metrics to define the nodes' behavior and the attack's baselines.

In the process of building the monitoring module, now we have an agent service which is running on every Kubernetes node so that we can detect anomaly behavior in the containers. The agent sends metrics to a central api where the analyzer processes the data to produce new datasets that can be used to develop a machine learning algorithm for anomaly detection.

The developed system in a real Kubernetes environment can be used in production, generating a labeled time-series dataset with anomalies produced by a microservice, as well as it aims to analyze the ways an anomaly detection plug-in could be implemented to detect those anomalies. Hence, it could be used to predict anomalies in the system deployed or the approach could be extrapolated to be used in another different system.

Выводы.

In our work we propose a new system that provides security monitoring capabilities for anomaly detection on the Kubernetes orchestration platform. We developed a container monitoring module for Kubernetes and implement neural network approaches to create classification models that strengthen its ability to find abnormal behaviors such as web service attacks and common vulnerabilities and exposures attacks.

Дарвиш Г. (автор)

Воробьева Алиса Андреевна (научный руководитель)