Development of detection common attacks in Kubernetes environment using machine learning approaches

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 come up with a new security layer based on machine learning detection model to secure Kubernetes cloud environment against common attacks (e.g. DDos, Spoofing, etc.).

Введение.

Kubernetes has arisen as the most popular orchestration platform for automatic deployment, expansion, and management of the Docker container life cycle. Platform-as-a-service suppliers, such as AWS and Azure, also provide Kubernetes as the main container orchestration environment for users. However, containerized environments also get new difficulties terms of complete monitoring and security arrangement. Thus, hackers can take advantage of the security weaknesses of containers to gain remote control permissions and cause extensive damage to organization resources. and one of the ways to secure k8s is by using Machine Learning (ML). ML techniques have been used in various ways to prevent or detect attacks and security gaps on the k8s cloud system. In this work, we provide a new effective way to secure the k8s cloud system against common attacks using ML techniques.

Основная часть.

Our work aims to propose a new anomaly detection model that can detect attacks in k8s environment depending on the behavior of on-site containers in Kubernetes. Our goal is to build a monitoring module with own extractors and customized rules to collect data and logs from nodes and running pods in real environment.

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 analyse 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 aim to develop 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)