Лещенко Б. С., аспірант,
Єфіменко А. А., к.т.н., доцент,
Державний університет «Житомирська політехніка»

SECURING CONTAINERIZED ENVIRONMENTS: INTEGRATING CLAMAV WITH KUBERNETES FOR INTRUSION DETECTION AND PREVENTION

Application deployment and orchestration are undergoing a paradigm shift, as evidenced by the development and growing uptake of containerised environments in the dynamic field of modern IT infrastructure. Security and a lack of training are the two main concerns expressed by respondents regarding the use and deployment of containers. In actuality, the biggest thing impeding adoption is a lack of training. For 44% of those who have not yet implemented containers in production and 41% of those who use them occasionally, this is the biggest obstacle. Security emerges as the primary challenge when almost all apps are deployed in containers[1]. However, these environments' intrinsic dynamic and intricate architecture pose difficult security issues, necessitating the development of efficient intrusion detection and prevention techniques. Small-to-midsized businesses (SMBs) are the target of more than half of all cyberattacks, and 60% of them shut down within six months after becoming the victim of a hack or data breach [2].

Although it poses special problems, the deployment of Intrusion Detection Systems (IDS) like ClamAV systems is essential. The open-source antivirus engine ClamAV is well-known for identifying trojans, viruses, malware, and other harmful threats. However, it needs to adjust to the complexities of microservice architectures and container orchestration without sacrificing scalability or performance [3]. The transient nature of containers, the simple layout of container images, and the complex network traffic patterns common to microservice-driven architectures provide challenges for traditional intrusion detection systems (IDS), which are frequently designed for static and centralised architectures [4].

In addition to highlighting a paradigm shift in security practices, the adaptation, and integration of IDS solutions like ClamAV also emphasize the urgent need for a nuanced security approach that can handle the challenges of visibility, network segmentation, and persistent monitoring of ephemeral workloads, while also taking into account the specifics of containerized environments [5]. Cloud-native technologies are becoming more and more popular among businesses, so it is imperative to improve security in these types of environments. To achieve this, we need to fully comprehend and strategically use robust security solutions, like file scanners and other IDS systems.

To sum up, intrusion detection systems (IDS) are essential for improving security posture in containerised environments because they can identify and stop threats, adjust to the intricacies of microservice architectures, offer visibility and monitoring features, and guarantee adherence to legal requirements. With the growing adoption of cloud-native and containerised technologies by enterprises, it is imperative to strategically install intrusion detection systems (IDS) to prevent cyberattacks and safeguard vital resources.

Список використаних джерел

1. CNCF Annual Survey 2022. *CNCF*. URL: https://www.cncf.io/reports/cncf-annual-survey-2022/
2. Cybercrime To Cost The World $10.5 Trillion Annually By 2025. *Cybercrime Magazine*. URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
3. Introduction – Clam AV Documentation. URL: https://docs.clamav.net/Introduction.html
4. Combe T., Martin A., Di Pietro R. To Docker or Notto Docker: A Security Perspective. *IEEE Cloud Computing*. 2016. Vol. 3, no. 5. P. 54–62. URL: https://doi.org/10.1109/mcc.2016.100.
5. Borg, Omega, and Kubernetes / B. Burnsetal. *Communications of the ACM*. 2016. Vol. 59, no. 5. P. 50–57. URL: https://doi.org/10.1145/2890784 (dateofaccess: 16.03.2024).