УДК 004.056.5:004.75

Марчук В. О.

Салієва О. В.

УДОСКОНАЛЕННЯ МОДЕЛІ ПРОАКТИВНОГО РЕАГУВАННЯ НА ІНЦИДЕНТИ В KUBERNETES-КЛАСТЕРАХ ШЛЯХОМ КОРЕЛЯЦІЇ ПОДІЙ ТА АВТОМАТИЗОВАНОЇ ІЗОЛЯЦІЇ

Вінницький національний технічний університет

Анотація

У роботі розглядається проблема затримки реагування на інциденти безпеки у високодинамічних середовищах оркестрації контейнерів Kubernetes. Встановлено, що традиційні системи моніторингу (SIEM, IDS) часто нездатні забезпечити своєчасну локалізацію загроз через надмірну кількість подій та швидку динаміку їх розвитку. Запропоновано удосконалену модель проактивного реагування, що базується на кореляції різнорідних подій (Kubernetes Audit Logs, системні журнали, мережеві потоки) для розрахунку інтегрального показника ризику для кожного контейнера. На основі цього показника, модель активує алгоритм автоматизованої ізоляції, який миттєво обмежує мережевий доступ (через NetworkPolicy) та ресурси скомпрометованого елемента, запобігаючи горизонтальному поширенню атаки.

Ключові слова: Kubernetes, кібербезпека, аналіз подій, кореляція подій, автоматизована ізоляція, реагування на інциденти, SecOps.

Abstract

This paper addresses the problem of delayed incident response in highly dynamic Kubernetes container orchestration environments. It is established that traditional monitoring systems (SIEM, IDS) are often unable to provide timely threat localization due to the high volume of events and their rapid development. An improved proactive response model is proposed, based on the correlation of heterogeneous events (Kubernetes Audit Logs, system logs, network flows) to calculate an integral risk score for each container. Based on this score, the model activates an automated isolation algorithm that instantly restricts network access (via NetworkPolicy) and resources of the compromised element, preventing the lateral spread of the attack.

Keywords: Kubernetes, cybersecurity, event analysis, event correlation, automated isolation, incident response, SecOps.

Вступ

Технології контейнеризації, зокрема платформа Kubernetes, стали де-факто стандартом для розгортання та управління мікросервісними архітектурами [1]. Однак, ця гнучкість та динамічність створюють унікальні виклики для кібербезпеки. Динамічний життєвий цикл контейнерів, складна мережева взаємодія та висока щільність робочих навантажень ускладнюють традиційні підходи до захисту [2]. Проникнення в один контейнер може швидко призвести до компрометації всього кластера через горизонтальне переміщення.

Існуючі системи моніторингу та безпеки, такі як SIEM або IDS, часто є реактивними. Вони фіксують інцидент вже після того, як він відбувся, а ручне втручання адміністратора для локалізації загрози потребує значного часу, протягом якого зловмисник може поширити атаку. Проблема полягає у відсутності механізму, що поєднує глибокий аналіз подій у реальному часі з негайною автоматизованою реакцією.

Метою даної роботи є удосконалення моделі, що вирішує цю проблему шляхом тісної інтеграції кореляційного аналізу подій та алгоритмів автоматизованої ізоляції для проактивного реагування на інциденти в Kubernetes.

Результати дослідження

Для вирішення поставленої задачі було розроблено багаторівневу модель проактивного реагування, що складається з трьох ключових фаз:

1. Збір та кореляція подій.

Модель агрегує дані з різноманітних джерел у кластері: журнали аудиту API-сервера Kubernetes, системні журнали контейнерів та вузлів, а також дані мережевих потоків. На відміну від простого збору логів, система використовує математичну модель кореляції $R(e_i, e_j)$, яка встановлює зв'язки між, на перший погляд, не пов'язаними подіями (наприклад, "exec у Pod" → "зміна ServiceAccount" → "нетипове зовнішнє з'єднання") [3].

2. Динамічне оцінювання ризику.

Для кожного контейнера (c) розраховується інтегральний показник ризику (D_c). Цей показник є зваженою сумою, що враховує критичність подій (w_i), пов'язаних з контейнером, та їхній контекст (k_i) (наприклад, чи виконується подія у привілейованому контейнері або в чутливому namespace) [4].

$$D_c = \sum_{i=1}^{n} w_i \cdot P(e_i|k_i)$$

Такий підхід дозволяє відрізнити легітимну активність (наприклад, під час CI/CD) від реальної загрози.

3. Автоматизована ізоляція.

Якщо розрахований показник ризику (D_c) перевищує встановлений поріг (D_{th}), модель автоматично запускає модуль реагування ("Isolation Controller"). Цей модуль не вимагає втручання людини і негайно виконує дії з локалізації загрози [5]. Найпоширенішою дією є динамічне застосування тимчасової політики NetworkPolicy, яка блокує весь вхідний та вихідний трафік для скомпрометованого Pod, розриваючи ланцюг атаки. В більш критичних випадках модуль може ініціювати зупинку або перезапуск Pod.

Перевага такого підходу полягає у переході від реактивної (реагування на наслідки) до проактивної (запобігання наслідкам) парадигми безпеки. Система мінімізує час між виявленням і реагуванням (Mean Time to Respond, MTTR) до кількох секунд, що є неможливим при ручному управлінні інцидентами.

Висновок

Запропонована модель інтеграції кореляційного аналізу подій та автоматизованої ізоляції дозволяє створити принципово новий рівень захисту для Kubernetes-кластерів. Усуваючи залежність від ручного втручання, такий підхід нейтралізує загрозу горизонтального поширення атак, що є одним із головних ризиків у мікросервісних архітектурах.

Ключовим результатом є розробка замкненого циклу безпеки (виявлення → аналіз → оцінювання ризику → ізоляція), який функціонує автономно та в реальному часі. Хоча впровадження такої моделі вимагає ретельного початкового налаштування профілів поведінки та порогів ризику, виграш у швидкості реагування та зниженні наслідків інцидентів є виправданим для будь-яких критичних систем, що експлуатуються в Kubernetes.

Подальші дослідження можуть бути спрямовані на інтеграцію механізмів машинного навчання для автоматичного оновлення профілів ризику та поведінкових шаблонів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. The 2023 Kubernetes Security Report [Електронний ресурс] / Wiz Research // wiz.io - 2023 - Режим доступу до ресурсу: https://www.wiz.io/blog/key-takeaways-from-the-wiz-2023-kubernetes-security-report

2. Gartner. Market Guide for Cloud-Native Application Protection Platforms [Електронний ресурс] / Gartner - 2024 - Режим доступу до ресурсу: https://www.crowdstrike.com/en-us/resources/reports/2024-gartner-market-guide-for-cloud-native-application-protection-platforms/

3. Automated Incident Response in Kubernetes [Електронний ресурс] / A. Sharma, R. Gill // International Journal of Network Security & Its Applications (IJNSA) - 2022 - Vol. 14, No. 3 - Режим доступу до ресурсу: https://aircconline.com/ijnsa/V14N3/14322ijnsa01.pdf

4. Q. Li. A security event description of intelligent applications in edge-cloud environment. Journal of Cloud Computing. / Q. Li // journalofcloudcomputing.springeropen.com - 2020 - Режим доступу до ресурсу: https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-020-00171-0

5. H. Pitkar. Cloud Security Automation Through Symmetry: Threat Intelligence, Event Correlation and Automation. *In:* Symmetry *17(6)*, / H. Pitkar // mdpi.com - 2025 - Режим доступу до ресурсу: https://www.mdpi.com/2073-8994/17/6/859

Марчук Валерія Олегівна – студентка групи 2КІТС-24м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: valerymarchuk2103@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@vntu.edu.ua

Marchuk Valeriia O. – student of 2KITS-24m group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: valerymarchuk2103@gmail.com

Supervisor: ***Saliieva Olha V.*** – Doctor of Philosophy (PhD) in specialty 125 "Cybersecurity", Associate Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, email: salieva8257@vntu.edu.ua