УДК 004.056

РАЗРАБОТКА МЕТОДИКИ МОНИТОРИНГА БЕЗОПАСНОСТИ В KUBERNETES

Юмадилова А.Г. (Университет ИТМО)

Научный руководитель — преподаватель факультета инфокоммуникационных технологий Филянин И.В. (Университет ИТМО)

Введение. Зарождение облачных вычислений и переход к распределенным системам ознаменовали собой существенную трансформацию в ИТ-ландшафте. Эволюция от монолитной к микросервисной архитектуре предоставила новую парадигму для разработки масштабируемых и отказоустойчивых систем. Из-за растущей популярности контейнеризации возникли платформы оркестровки, такие как Kubernetes, они играют важную роль в управлении контейнеризированных приложений [1] благодаря своей гибкости, масштабируемости и способности ускорять процессы развертывания. Несмотря на свои преимущества, технология Kubernetes также сталкивается с серьезными вызовами в области безопасности. Целью исследования является изучение особенностей мониторинга безопасности в Kubernetes и разработка методики для его реализации, которая позволит своевременно обнаруживать и устранять возможные риски безопасности.

Основная часть. В рамках работы был проведен тщательный анализ научной литературы, технической документации и изучены лучшие практики обеспечения безопасности в среде Kubernetes. В результате было определено, что традиционные инструменты мониторинга информационной безопасности не подходят для Kubernetes, так как в них не учитывается архитектура системы [2] и особенности контейнерных сред.

В рамках работы были изучены требования регулирующих документов таких как PCI DSS, NIST и CIS, в каждом из которых присутствуют требования о реализации мониторинга безопасности.

Особенное внимание было уделено модели угроз, которая является ключевым инструментом для построения мониторинга информационной безопасности, так как позволяет определить потенциальные угрозы и уязвимости, которые могут возникнуть в процессе использования системы. В качестве основной выбрана матрица угроз Microsoft для Kubernetes, являющаяся расширенной версией матрицы ATT&CK MITRE, и охватывающая большее количество тактик и техник злоумышленника [3].

Kubernetes создаёт уникальные проблемы для мониторинга и обеспечения безопасности из-за своей динамичной и эфемерной природы. Для мониторинга контейнерных сред были проанализированы инструменты на основе технологии eBPF [4], использующейся для мониторинга системных вызовов.

На основе данной информации была разработана методика для построения мониторинга безопасности в Kubernetes, учитывающая архитектуру и особенности системы. Так, проанализировав и сравнив существующие инструменты для мониторинга контейнерных сред, был выбран инструмент Falco, open-source решение для мониторинга безопасности, поддерживаемое CNCF [5]. Falco отслеживает системные вызовы, системные логи среды и генерирует предупреждения о подозрительной активности на основе правил. Для обеспечивания большего покрытия используемой матрицы угроз, исходный набор правил был расширен путем разработки новых правил для актуальных угроз. Для удобства и интеграции с центром мониторинга безопасности предложена интеграция используемых инструментов с SIEM-системой.

Вывод. Разработанная методика демонстрирует улучшение в области обнаружения и реагирования на угрозы информационной безопасности, предлагая использование мониторинга Kubernetes с учетом особенностей архитектуры, а также отвечает требованиям регуляторов в области безопасности. Внедрение данной методики позволит достичь более

высокого уровня безопасности и видимости в кластерах Kubernetes, эффективно снижая риски информационной безопасности для развёрнутой системы.

Список использованных источников:

1. Kampa S. Navigating the Landscape of Kubernetes Security Threats and Challenges //Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online). – 2024. – Т. 3. – №. 4. – С. 274-281.
2. Kubernetes Documentation [Электронный ресурс]. – URL: https://kubernetes.io/docs/
3. Спиридонов Д.П., Федорченко Е.В. Сравнительный анализ и применение матриц атак Microsoft Kubernetes ThreatMatrix и MITRE ATT&CK Matrix // Вестник науки. - 2024. - №12
4. Fournier G., Afchain S., Baubeau S. Runtime security monitoring with ebpf //17th SSTIC Symposium sur la Sécurité des Technologies de l'Information et de la Communication. – 2021.
5. The Falco Project [Электронный ресурс] - URL: https://falco.org/docs/