LUNTRY

Карта мер безопасности для Kubernetes

С чего начать работу над безопасностью Kubernetes: основные шаги

	Шаг 1	Шаг 2	Шаг 3
Контроль состояния Kubernetes-кластеров	☐ Проверить актуальность версий	☐ Проверить наличие уязвимостей системных компонентов	☐ Обеспечить мультитенантность
Безопасность Runtime	☐ Контролировать нежелательные события	☐ Отслеживать процессные аномалии	☐ Отслеживать сетевые аномалии
Анализ прав доступа	☐ Проверить актуальность User, Group, SA, а также наличие полных доступов «*»	☐ Проверить доступ к критичным ресурсам	☐ Установить собственные правила
Контроль соответствия кластера стандартам	☐ Проверить на соответствие CIS Kubernetes Benchmark критичных пунктов	☐ Проверить на соответствие CIS Kubernetes Benchmark значимых пунктов	☐ Проверка оставшихся пунктов стандарта
Защита сети	☐ Проверить, какие приложения или сервисы доступны извне кластера и какие обращаются за пределы кластера	☐ Изолировать Namespaces друг от друга с помощью NetworkPolicy	☐ Ограничить взаимодействие между приложениями с помощью NetworkPolicy
Управление уязвимостями образов и best practices	☐ Устранить уязвимости с патчами с учетом приоритизации	☐ Проверить dockerfile на соответствие лучшим практикам	☐ Проверить образы на наличие вредоносного ПО и ПО двойного назначения
Проверка Kubernetes-ресурсов	☐ Проверить приложение на соответствие Pod Security Standard. Контролировать образы.	☐ Использовать библиотеки правил для других Kubernetes ресурсов	☐ Перейти от режима аудита к режиму блокировки

Далее

Luntry поможет на всех этапах

Видео о том, с чего начать безопасность контейнерных сред

luntry_official

luntrysolution

luntrysolution