LUNTRY Чек-лист интеграции защиты контейнеров и ASOC

☐	ШАГ 1	**НАСТРОЙКА ПОТОКОВ ДАННЫХ** →	· Настроить выгрузку результатов сканирования Container Security (образы, рантайм) в ASOC · Подключить в ASOC данные от SAST, SCA и других инструментов AppSec
☐	ШАГ 2	**ОПРЕДЕЛЕНИЕ КОНТЕКСТА ДЛЯ ПРИОРИТИЗАЦИИ** →	· В ASOC отметить бизнес-критичные приложения и микросервисы · Интегрировать ASOC с системой тикетов и SIEM
☐	ШАГ 3	**СОЗДАНИЕ ПРАВИЛ КОРРЕЛЯЦИИ** →	· Настроить правила, чтобы уязвимость из Container Security, найденная в запущенном контейнере, повышала приоритет в ASOC · Связать уязвимости зависимостей (SCA) с фактом их использования в сканированных образах
☐	ШАГ 4	**АВТОМАТИЗАЦИЯ РЕАГИРОВАНИЯ** →	· Настроить автоматическое создание тикета для разработчика, если Container Security нашел критичную уязвимость в образе, который идет в сборку · Добавить gate в CI/CD, который блокирует продвижение сборки при обнаружении критичных проблем
☐	ШАГ 5	**ВНЕДРЕНИЕ МЕТРИК И УЛУЧШЕНИЙ** →	· Отслеживать метрики "Time to Fix" для уязвимостей, найденных через связку Container Security + ASOC · Регулярно анализировать отчеты о наиболее рискованных компонентах

Luntry — это Комплексная Защита на всем жизненном цикле контейнерных приложений и средств оркестрации на базе Kubernetes

luntry_official luntrysolution luntrysolution info@luntry.ru