LUNTRY

Интеграция Luntry и ASOC

Анатолий Карпенко

инженер автоматизации Luntry

Станислав Проснеков

Head of DevOps Luntry

Обо мне

> Ваша инфраструктура так же уязвима, как и самое слабое ее звено

Lead DevOps
Luntry

Более 15 лет опыта в ИТ

Специализация – построение процессов и автоматизация

Автор лучших сценариев

Эксперт в сфере безопасности контейнерных сред

- ИБ по образованию, в ИТ по призванию
- На 98% кандидат технических наук
- Org Team на ZeroNights и БЕКОН (БЕзопасностьКОНтейнеров)

Спикер

DevOpsConf

LUNTRY

Обо мне

> Мировоззрение:
> Все, что нажимается чаще 2 раз, лучше автоматизировать.

Инженер автоматизации Luntry

Более 15 лет опыта в ИБ

Специализация — безопасность контейнеров и Kubernetes

Автор ТГ-канала «Технологический болт Генона»

Любитель митапошных форматов

SPb Reliability Meetup	SafeCode	DevOops
DEFCON'ы	ТБ Форум	ITGM
TechTrain	БЕКОН	

Рисую несмешные мемы

:|

LUNTRY

О компании Luntry

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

Продукт в реестре Минцифры
https://reestr.digital.gov.ru/reestr/1057835/

LUNTRY.RU

Функциональность Luntry

Контроль Kubernetes-ресурсов

Контроль состояния Kubernetes-кластеров

Контроль соответствия кластера стандартам

Управление уязвимостями образов и best practice

Сетевая безопасность

Анализ прав доступа

Защита Runtime

Функциональность Luntry

Контроль Kubernetes-ресурсов

Контроль состояния Kubernetes-кластеров

Контроль соответствия кластера стандартам

Управление уязвимостями образов и best practice

Сетевая безопасность

Анализ прав доступа

Защита Runtime

План вебинара

LUNTRY

01	Знакомство с ASOC
02	Как Luntry помогает решить задачи, связанные с управлением уязвимостями
03	Выводы

Знакомство с ASOC

Что такое ASOC?

- Application Security Orchestration & Correlation (ASOC)
- Интеграция инструментов
- Координация процессов

LUNTRY

Какую проблему решает?

- **Автоматизация**
  - Процессов
  - Сценариев
  - Реагирования на инциденты
- **Получение комплексных отчётов**

LUNTRY

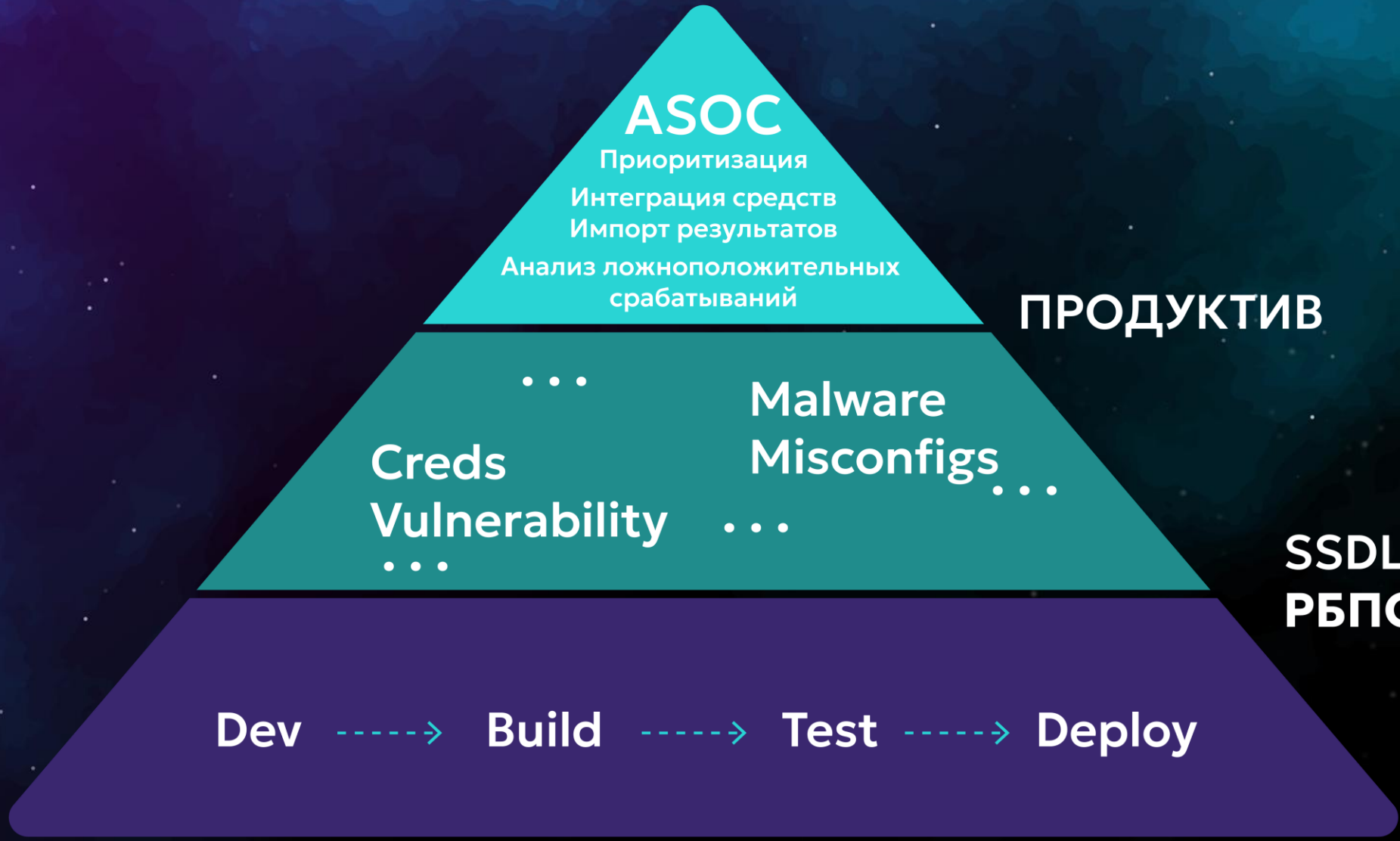
LUNTRY

Интеграция инструментов безопасности

Получение информации из разных источников

Построение корреляции определение закономерностей

«Пирамида потребностей ASOC»



LUNTRY

Пример: уязвимости в образах

LUNTRY

- **Проблема**: нашли много проблем, надо их ранжировать
- **Корреляция**:
  - Берём данные об уязвимостях из сканера
  - Определяем где, как и с какими параметрами запущены эти образы (например, через Kubernetes API)
  - Проверяем нет ли уже этой проблемы в таск-трекере *
- **Решения**:
  - Создать инцидент
  - Отправить уведомление команде Dev[Sec]Ops
  - Автоматически масштабировать в 0 уязвимый сервис **

* - Требует зрелых процессов
** - Требует силы духа

LUNTRY

КАК LUNTRY ПОМОГАЕТ РЕШИТЬ ЗАДАЧИ, СВЯЗАННЫЕ УПРАВЛЕНИЕМ УЯЗВИМОСТЯМИ

Возможности Luntry при работе с ASOC

- Виды сканирований:
  - Компонентный анализ (SBOM)
  - Уязвимости
  - Секреты
  - Мисконфигурации
  - Вредоносный код
- Вся информация доступна через API

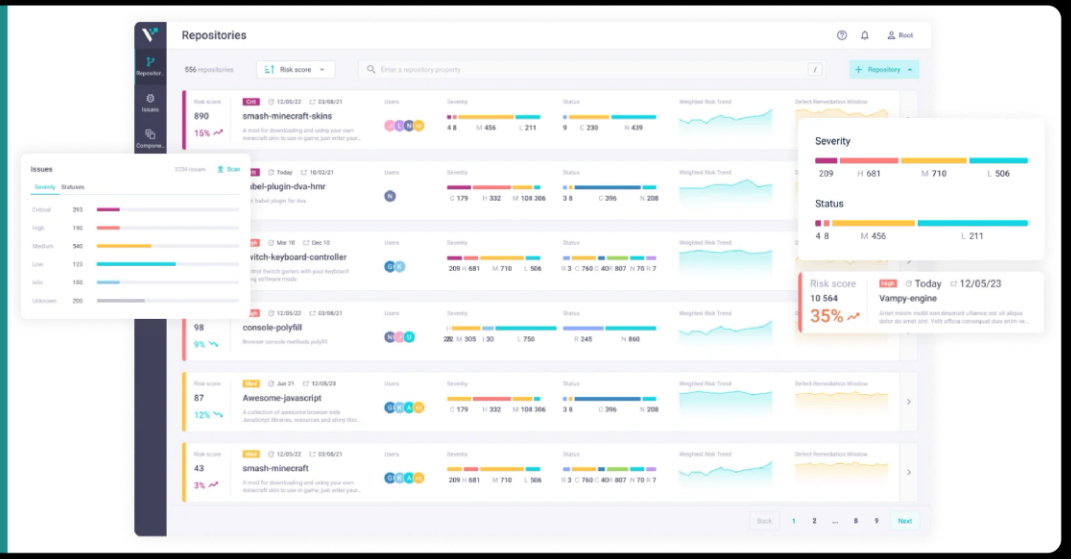
- Результаты в формате:
  - Json
  - Xml
  - CSV
  - PDF
  - HTML
  - CycloneDX-json v1.6
  - Gitlab-container-sast-report

LUNTRY

Live Demo Luntry

LUNTRY

Vampy



AppSecHub

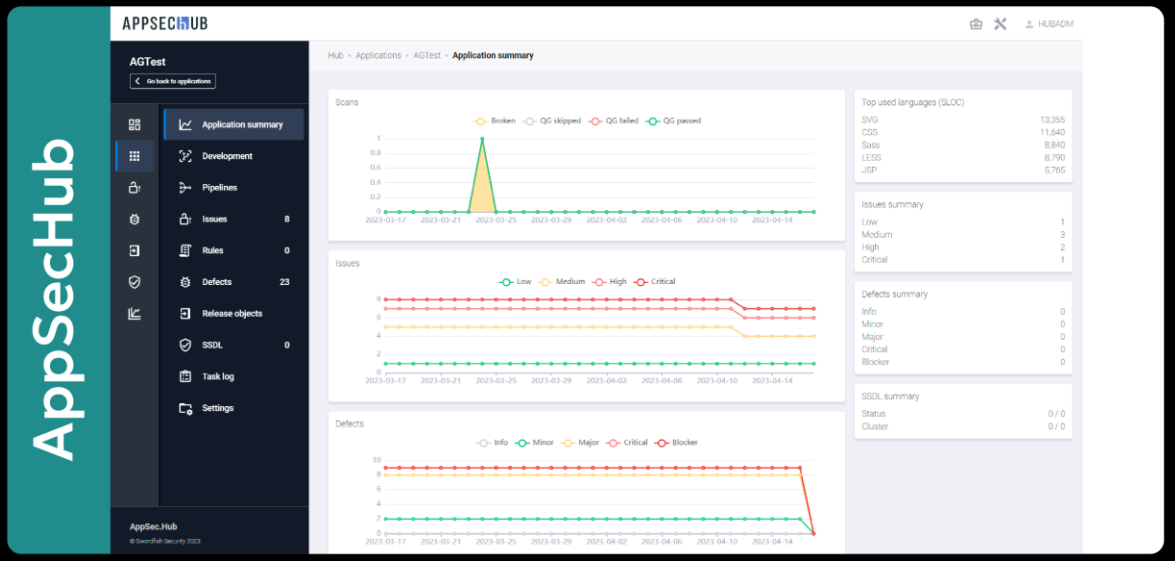


Схема стенда

LUNTRY

Какую ценность дает сканирование образов

LUNTRY

- **Вопрос**: у нас уже есть SAST и SCA в цепочке, какую ценность дает финальный Image Scan
- **Ответ** :
  - SAST и SCA не захватывают зависимости получаемые в процессе сборки* и подготовки образа:
    - Скомпилированные приложения
    - Системные пакеты и библиотеки
    - Состав базового образа
    - Без регулярного сканирования есть риск упустить новые CVE для уже работающих образов

* Зависит от окружения и языка программирования

Выводы

Выводы

LUNTRY

01 AppSec необходим

02 AppSec’у без ASOC’а тяжело контролировать состояние продукта

03 Luntry отлично интегрируется с ASOC и упрощает работу с контейнерными средами

Полезные ссылки

"Безопасность контейнеров и Kubernetes для DevSecOps специалистов",
Вебинар Luntry

LUNTRY

LUNTRY

luntry_official
luntrysolution
luntrysolution

luntry.ru
info@luntry.ru

СПАСИБО
ЗА ВНИМАНИЕ!