



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

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

DEFCON'ы

TechTrain

SafeCode

ТБ Форум

БЕКОН

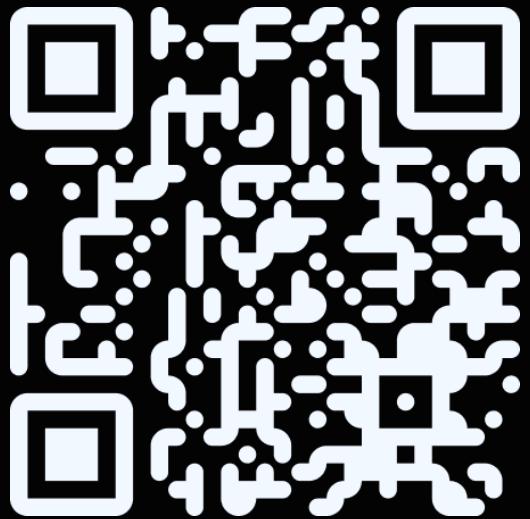
DevOops

ITGM

Рисую несмешные мемы
:|

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

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



Знакомство с ASOC

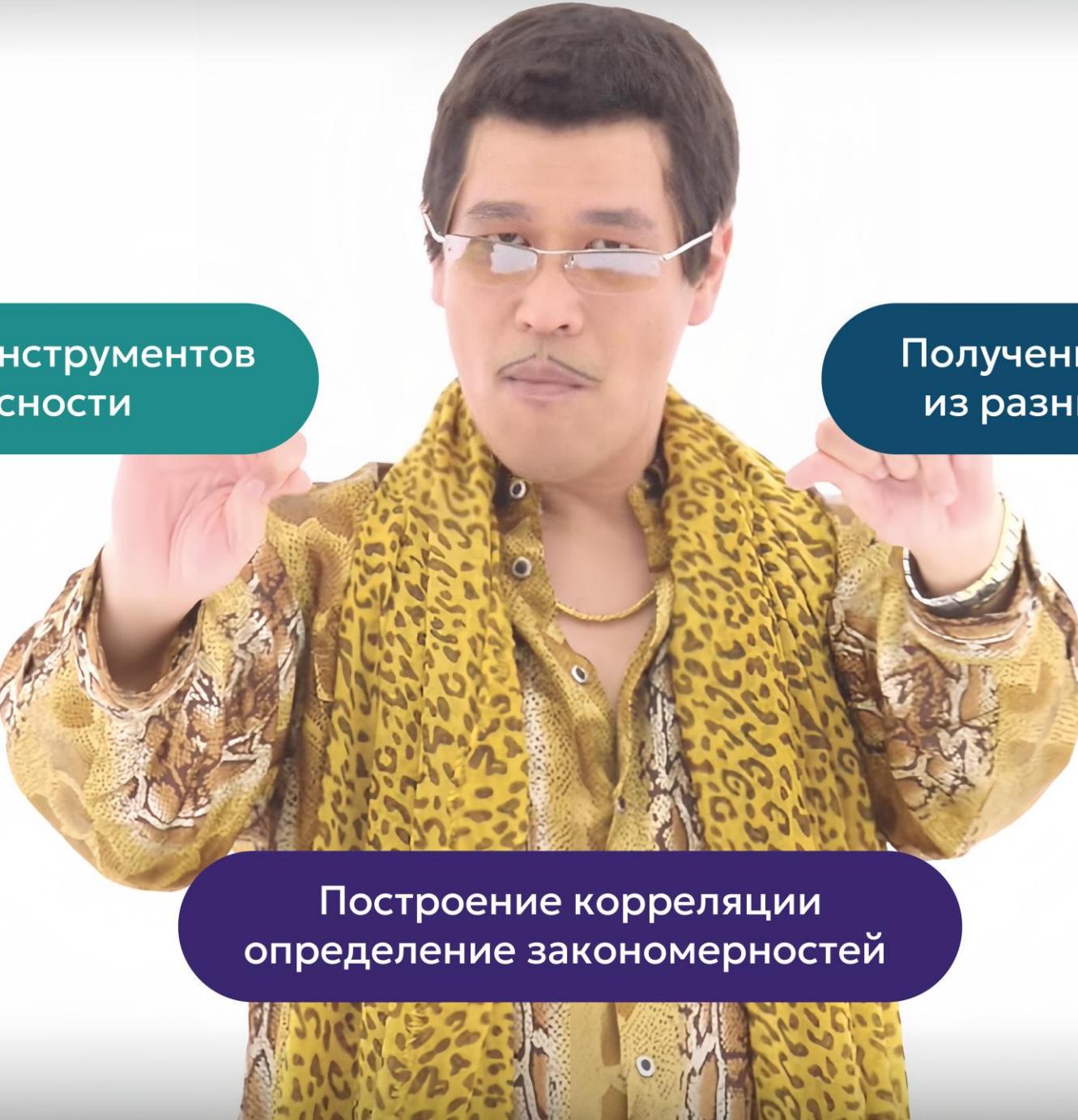
Что такое ASOC?

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



Какую проблему решает?

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

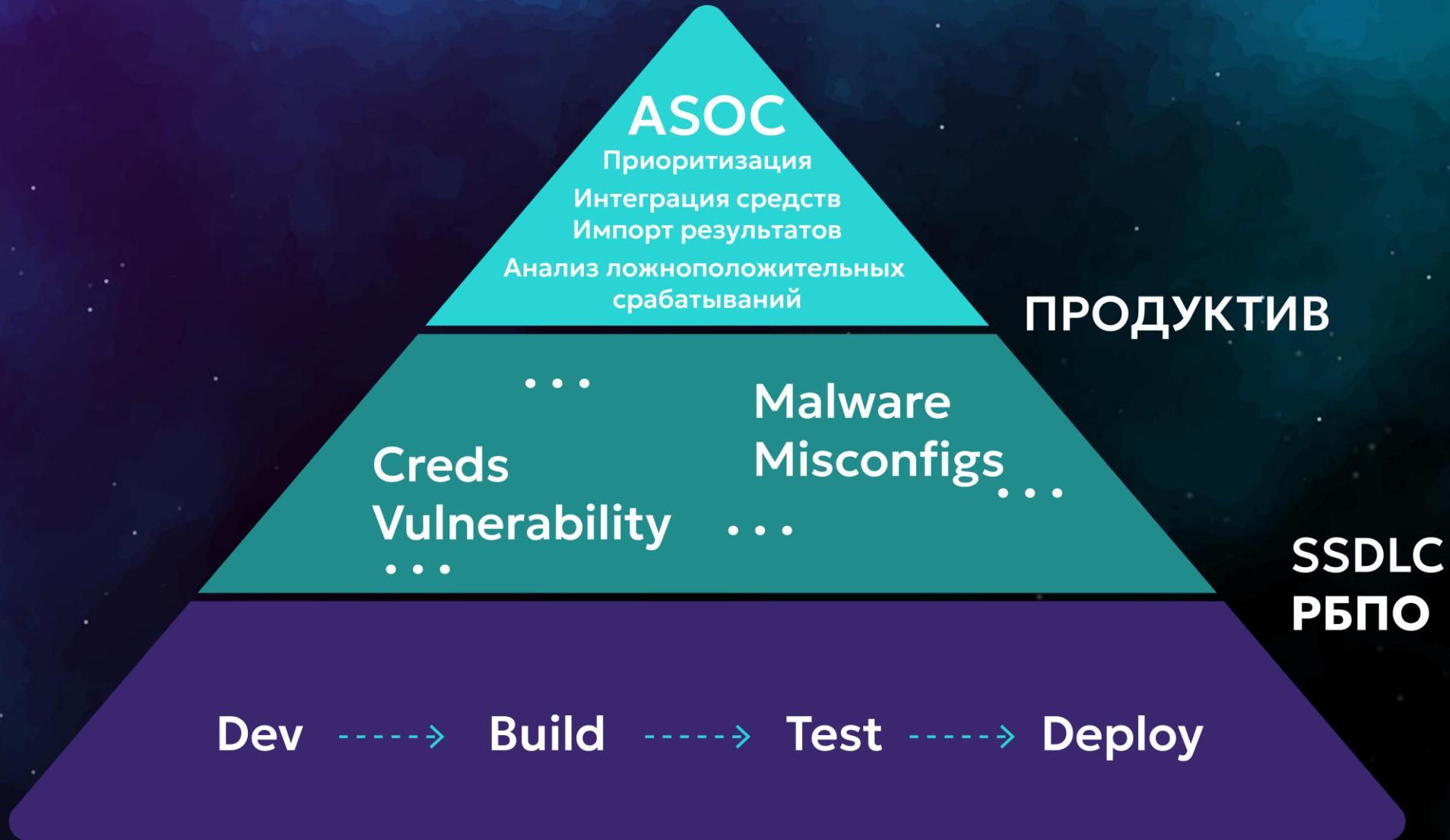


Интеграция инструментов
безопасности

Получение информации
из разных источников

Построение корреляции
определение закономерностей

«Пирамида потребностей ASOC»



Пример: уязвимости в образах

- **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



**КАК LUNTRY ПОМОГАЕТ
РЕШИТЬ ЗАДАЧИ, СВЯЗАННЫЕ
УПРАВЛЕНИЕМ УЯЗВИМОСТАМИ**

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

Live Demo Luntry

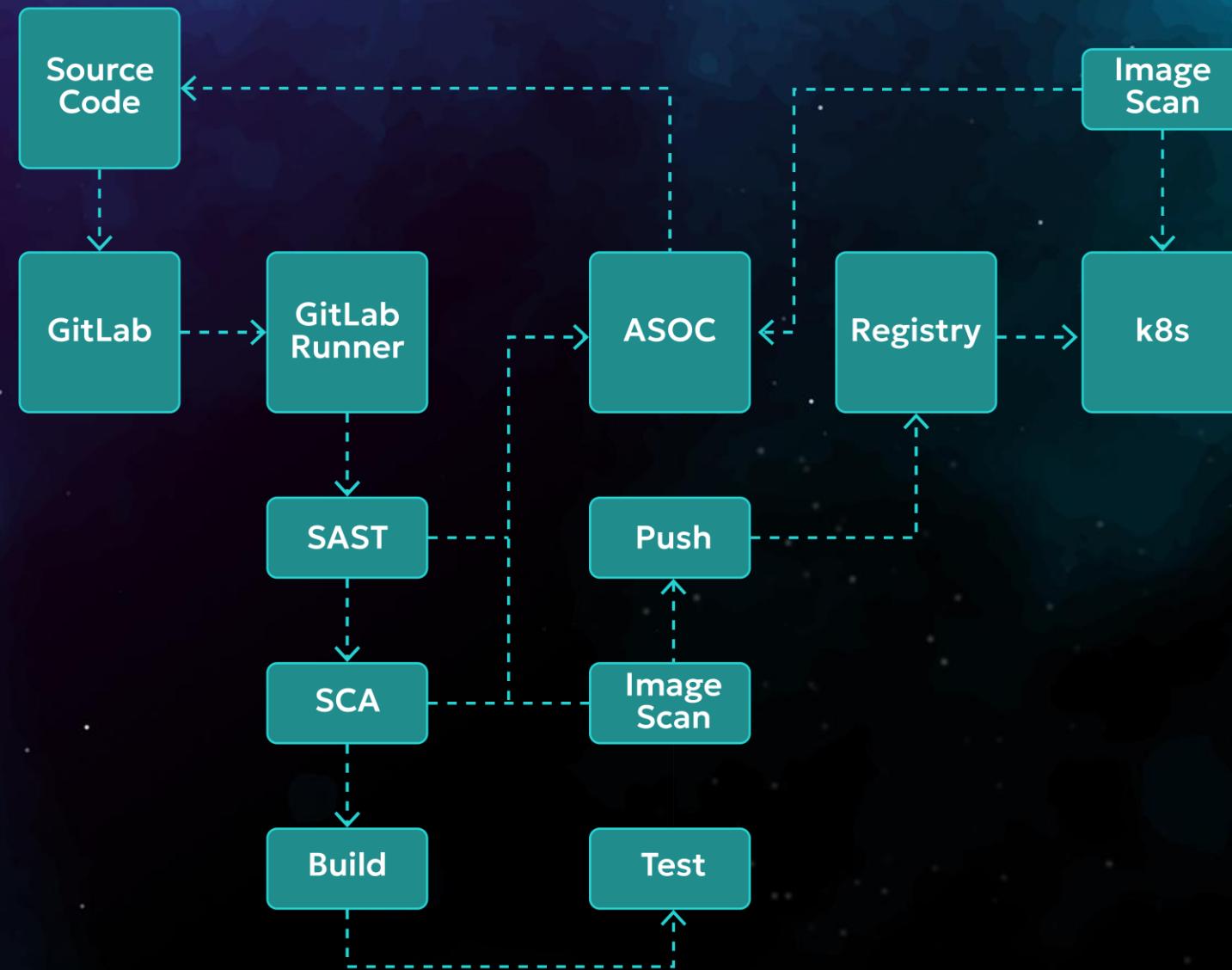
Vampy

The screenshot shows a dashboard for managing multiple GitHub repositories. At the top, there's a summary bar for a repository named 'smash-minecraft-skins' with a risk score of 890 and 15% remediation progress. Below this, a list of repositories is displayed, each with its name, last update date, risk score, severity distribution (Critical, High, Medium, Low, Info, Unknown), and status distribution (H, M, L, N). Each repository card also includes a 'Scan' button and a detailed risk trend chart.

AppSecHub

The screenshot displays the 'Application summary' page for the 'AGTest' application. It features three main charts: 'Scans' (a spike in 'Brokers' on March 25, 2023), 'Issues' (a count of Low, Medium, High, and Critical issues over time), and 'Defects' (a count of Info, Minor, Major, Critical, and Blocker defects over time). To the right, there are sections for 'Top used languages (SLOC)', 'Issues summary', 'Defects summary', and 'SSL summary'. A sidebar on the left provides navigation links for Application summary, Development, Pipelines, Issues (8), Rules, Defects (23), Release objects, SSL, Task log, and Settings.

Схема стенда



Какую ценность дает сканирование образов

- **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

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_official](#)

 [luntrysolution](#)

 [luntrysolution](#)

 [luntry.ru](#)

 info@luntry.ru

**СПАСИБО
ЗА ВНИМАНИЕ!**