ITFORUM 2026
UGRA ЮГРА 尤格拉

LUNTRY
SOLAR Group

# Безопасная разработка программного обеспечения как основа построения системных ИТ-решений

Luntry защита контейнеров и Kubernetes

# О нас

LUNTRY
SOLAR Group

**Станислав Проснеков**
Глава DevOps департамента
Luntry, ГК “Солар»

В основе продукта LUNTRY заложены собственные исследования, а также опыт проведения аудитов и пентестов Kubernetes

## ДМИТРИЙ ЕВДОКИМОВ

Founder & CTO Luntry

## СПЕЦИАЛИЗАЦИЯ — БЕЗОПАСНОСТЬ КОНТЕЙНЕРОВ И KUBERNETES

Специалисты с опытом ИБ более 15 лет

## КОМАНДА БАЗИРУЕТСЯ В САНКТ-ПЕТЕРБУРГЕ

- Ведем тренинги по организации безопасности в Kubernetes
- Организуем уникальную конференцию по безопасности контейнеров — «БеКон»
- Занимаемся кураторством учащихся по тематике безопасности контейнеров
- Делимся с сообществом знаниями о безопасности Kubernetes в telegram-канале «k8s (in)security»

## ВЫСТУПЛЕНИЯ НА КОНФЕРЕНЦИЯХ

VK Kubernetes | DevOpsConf | Kazhackstan | Confidence | HackInParis
HighLoad++ | ZeroNights | KuberConf | OFFZONE | БеКон
BlackHat | DevOops | HITB | PHDays | SAS

LUNTRY
SOLAR Group

# Контейнеры это современный IT стандарт

От разработки до запуска

## 01

### СТАНДАРТ РАЗРАБОТКИ

- CI pipelines

## 02

### СТАНДАРТ ДОСТАВКИ

- Образы контейнеров
- Helm charts

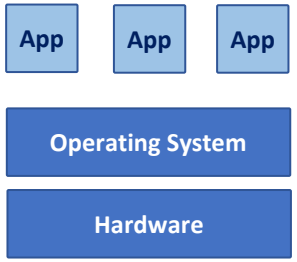
## 03

### СТАНДАРТ ЗАПУСКА

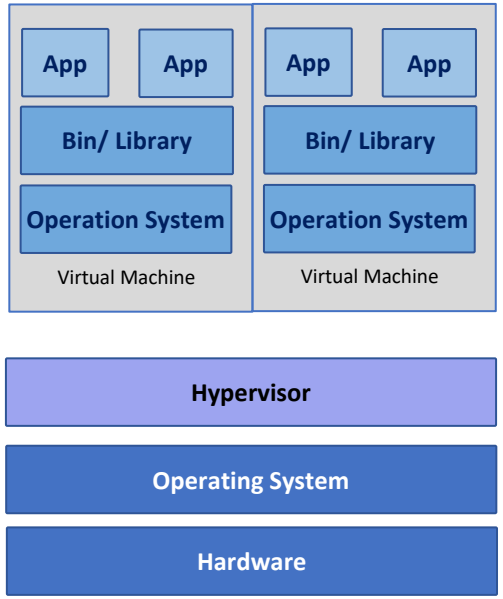
- Docker
- Kubernetes

# Эволюция от контейнеров к оркестраторам контейнеров

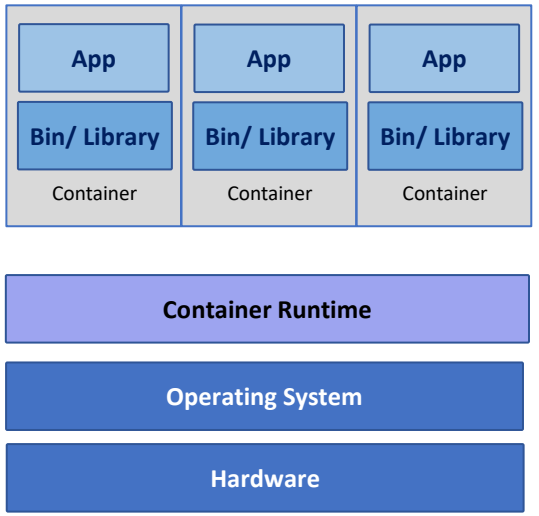
LUNTRY
SOLAR Group



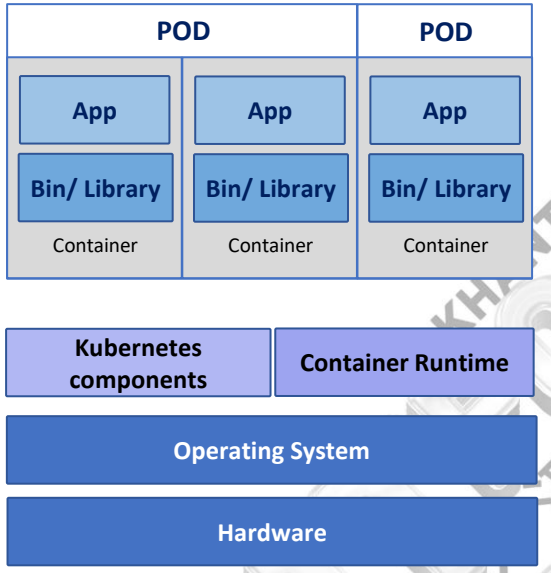

Традиционное развертывание




Виртуализированное развертывание




Контейнеризированное развертывание




Kubernetes развертывание

# Kubernetes (K8s)

МОЗГ СОВРЕМЕННЫХ ИНФРАСТРУКТУР

| | |
|---|---|
| Оркестратор | Стандарт де-факто для управления контейнеризированной нагрузкой |
| Обеспечивает надежную и масштабируемую среду для обработки больших данных | • Big Data-ворклоады (например, с использованием Hadoop, Spark или AI/ML-пайплайнов) в Kubernetes увеличивают сложность системы<br>  • Volume (Объем)<br>  • Velocity (Скорость)<br>  • Variety (Многообразие) |


# Регуляторика

LUNTRY
SOLAR Group

Защита ГИС и гос. ИС:
- Приказ ФСТЭК № 117 и методический документ от 12.04.26

Защита КИИ:
- 187-ФЗ
- Приказ ФСТЭК № 239 (Приложение)

Защита ИСПДн:
- 152-ФЗ
- Приказ ФСТЭК № 21 (п.8.11, Приложение)

Обязательность
- ГИС: К1, К2, К3
- ИСПДн: У31, У32
- ЗоКИИ: да

### 118 приказ ФСТЭК

Это требование к средам контейнеризации

### 117 приказ ФСТЭК и его методический документ

Устанавливает требования к ЗИ в ГИС в т.ч. для контейниризации

### Информационное сообщение ФСТЭК России 240/24/38

О повышении безопасности средств защиты информации, в состав которых разработчики включают средства контейнеризации или образы контейнеров

### Банк данных угроз безопасности информации от ФСТЭК

Содержит УБИ посвященные контейнерам

# Проблема #1

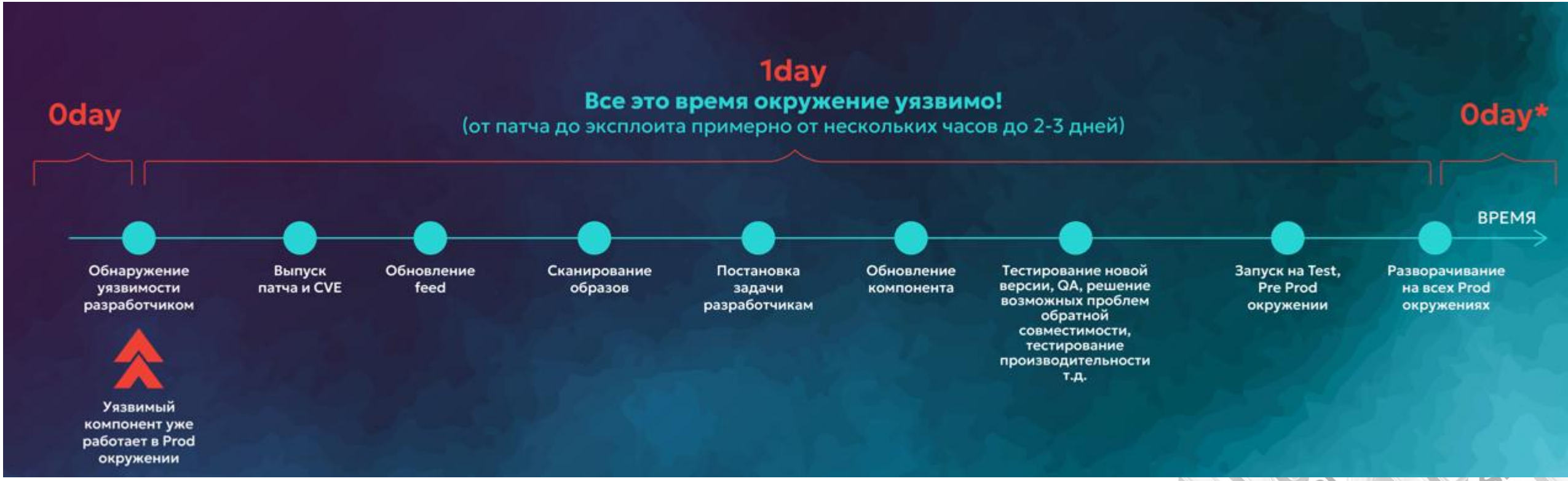
РОСТ КОЛИЧЕСТВА УЯЗВИМОСТЕЙ


Обновление политики NIST по NVD

# Проблема #2

LUNTRY
SOLAR Group

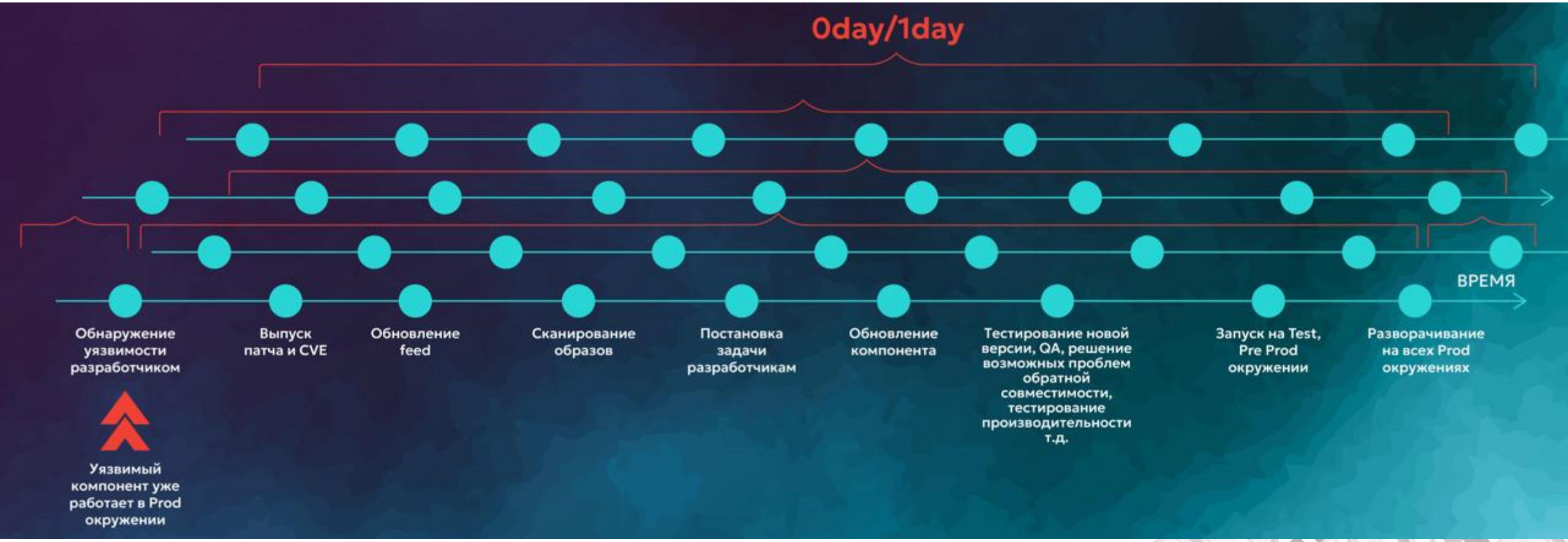
## СКОРОСТЬ ИСПРАВЛЕНИЯ УЯЗВИМОСТЕЙ НИЗКАЯ



# Проблема #2

LUNTRY
SOLAR Group

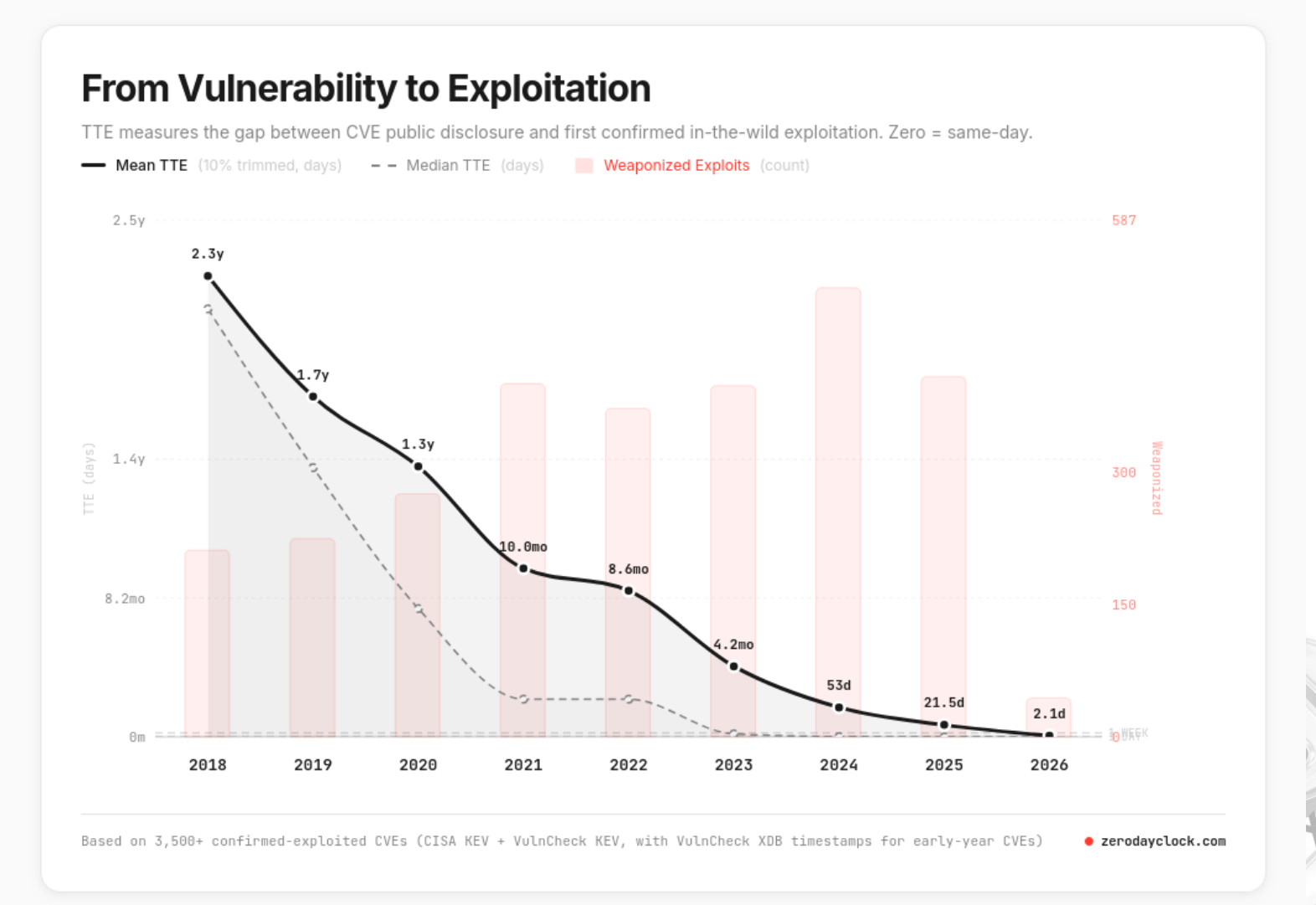
## СКОРОСТЬ ИСПРАВЛЕНИЯ УЯЗВИМОСТЕЙ НИЗКАЯ



# Проблема #3

LUNTRY
SOLAR Group

## СКОРОСТЬ СОЗДАНИЕ ЭКСПЛОИТА ТОЛЬКО РАСТЕТ



# Проблема #3

LUNTRY
SOLAR Group

## ВКЛАД AI

### XBOW

For the first time in bug bounty history, an autonomous penetration tester has reached the top spot on the US leaderboard.


### Claude Mythos

## IDENTIFYING VULNERABILITIES AND EXPLOITS WITH CLAUDE MYTHOS PREVIEW

Over the past few weeks, we have used Claude Mythos Preview to identify thousands of zero-day vulnerabilities (that is, flaws that were previously unknown to the software's developers), many of them critical, in every major operating system and every major web browser, along with a range of other important pieces of software.

In a post on our Frontier Red Team blog, we provide technical details for a subset of these vulnerabilities that have already been patched and, in some cases, the ways that Mythos Preview found to exploit them. It was able to identify nearly all of these vulnerabilities—and develop many related exploits—entirely autonomously, without any human steering. The following are three examples:

- Mythos Preview found a 27-year-old vulnerability in OpenBSD—which has a reputation as one of the most security-hardened operating systems in the world and is used to run firewalls and other critical infrastructure. The vulnerability allowed an attacker to remotely crash any machine running the operating system just by connecting to it;
- It also discovered a 16-year-old vulnerability in FFmpeg—which is used by innumerable pieces of software to encode and decode video—in a line of code that automated testing tools had hit five million times without ever catching the problem;
- The model autonomously found and chained together several vulnerabilities in the Linux kernel—the software that runs most of the world's servers—to allow an attacker to escalate from ordinary user access to complete control of the machine.

# Проблема #4

LUNTRY
SOLAR Group

## AI СГЕНЕРИРОВАННЫЙ КОД

01

AI ОПТИМИЗИРУЕТ КОД НА «РАБОТОСПОСОБНОСТЬ», А НЕ НА БЕЗОПАСНОСТЬ

02

ОТСУТСТВИЕ ПОЛНОГО КОНТЕКСТА СИСТЕМЫ

03

ОБУЧЕНИЕ НА НЕОДНОРОДНЫХ ИСТОЧНИКАХ

04

ГЕНЕРАЦИЯ ШАБЛОННОГО КОДА

05

ОТСУТСТВИЕ ВСТРОЕННОЙ ПРОВЕРКИ БЕЗОПАСНОСТИ

# Проблема #5

LUNTRY
SOLAR Group

## 01

### НА УРОВНЕ ОБРАЗОВ

- уязвимость в компонентах образа
- небезопасная конфигурация
- наличие чувствительных данных
- вредоносное ПО
- отсутствие подлинности образов

## 02

### НА УРОВНЕ КОНТЕЙНЕРОВ

- недекларированные возможности
- небезопасная конфигурация
- избыточные привилегии

## 03

### НА УРОВНЕ ОРКЕСТРАТОРА

- неподдерживаемые системные компоненты
- уязвимость в системных компонентах
- отсутствие изоляции
- отсутствие сетевой сегментации
- небезопасная конфигурация
- отсутствие контроля доступа
- избыточные привилегии сущностей

# Итоги

LUNTRY
SOLAR Group

- Количество известных уязвимостей растет как никогда быстро
- Скорость разработки эксплоитов тоже
- Современные стандарты упаковки, доставки и запуска усложняются
- Сложность ИТ-среды растет
- Усиливается необходимость наличия интегрированного решения или группы решений закрывающих требования безопасности приложений на всем жизненном цикле от кода до работающего приложения
- Такие решения должны полагаться не только на поиск известных сигнатур, т.к. сигнатуры устаревают слишком быстро
- ИБ это не только отсутствие известных сигнатур и ошибок в статических анализаторах, но и контроль работы уже запущенных приложений

LUNTRY
SOLAR Group

# IT FORUM 2026

UGRA ЮГРА 尤格拉

+7 (499) 755-07-70
info@rt-solar.ru

Центральный офис.
125009, Москва,
Никитский переулок, 7с1