Patch management не поможет, фиксики не спасут

Дмитрий Евдокимов

Founder&CTO Luntry

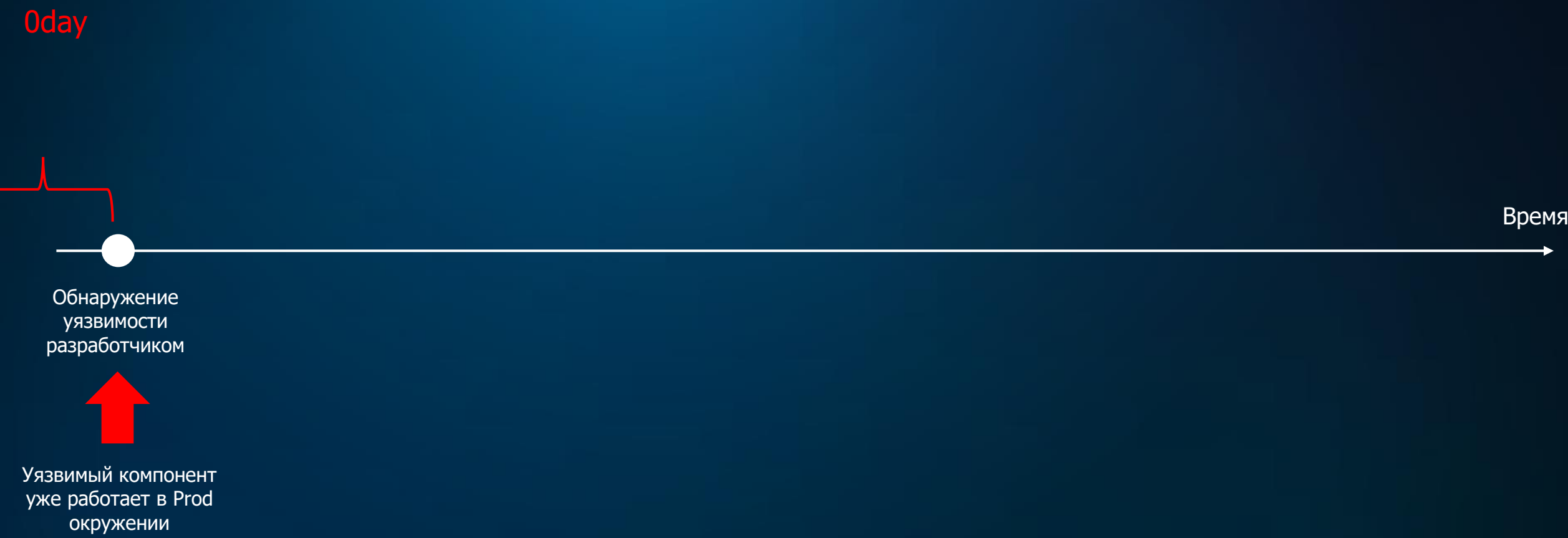
About me

- Основатель и технический директор Luntry
- Опыт в ИБ более 10 лет
- Специализация безопасность контейнеров и Kubernetes
- CFP DevOpsConf, HighLoad++
- Бывший автор статей и редактор рубрик в журнале “ХАКЕР”
- Создатель Telegram-канала “k8s (in)security”
- Автор курса “Cloud Native безопасность в Kubernetes”
- Не верит, что систему можно сделать надежной и безопасной, не понимая ее
- Докладчик: BlackHat, HITB, ZeroNights, HackInParis, Confidence, SAS, OFFZONE, PHDays, Kazhackstan, DevOpsConf, DevOops, KuberConf, VK Kubernetes Conference, HighLoad++, БЕКОН и др.

Проблематика

Работа с 1day уязвимостями

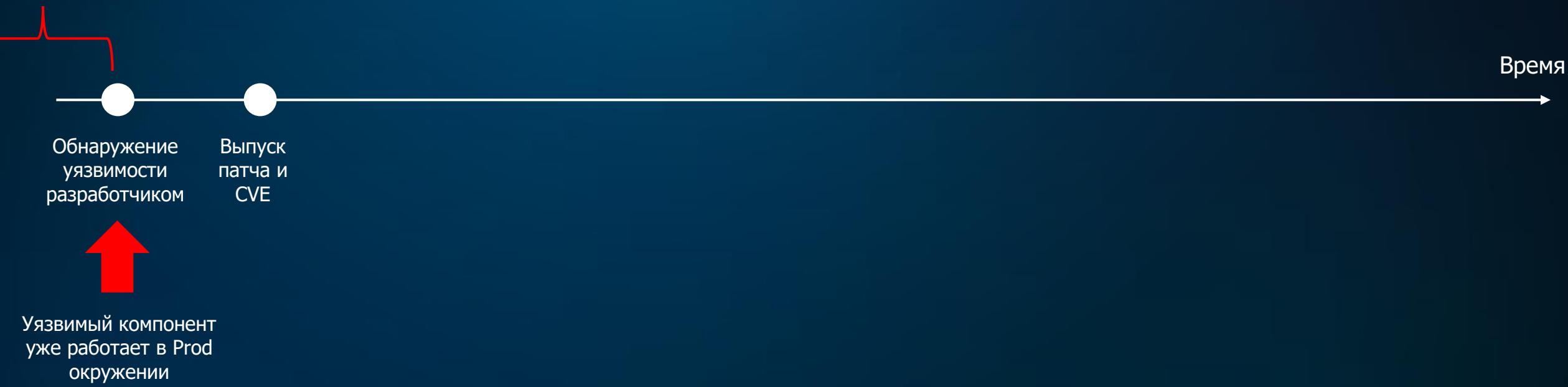
Работа с 1day уязвимостями



Работа с 1day уязвимостями

0day

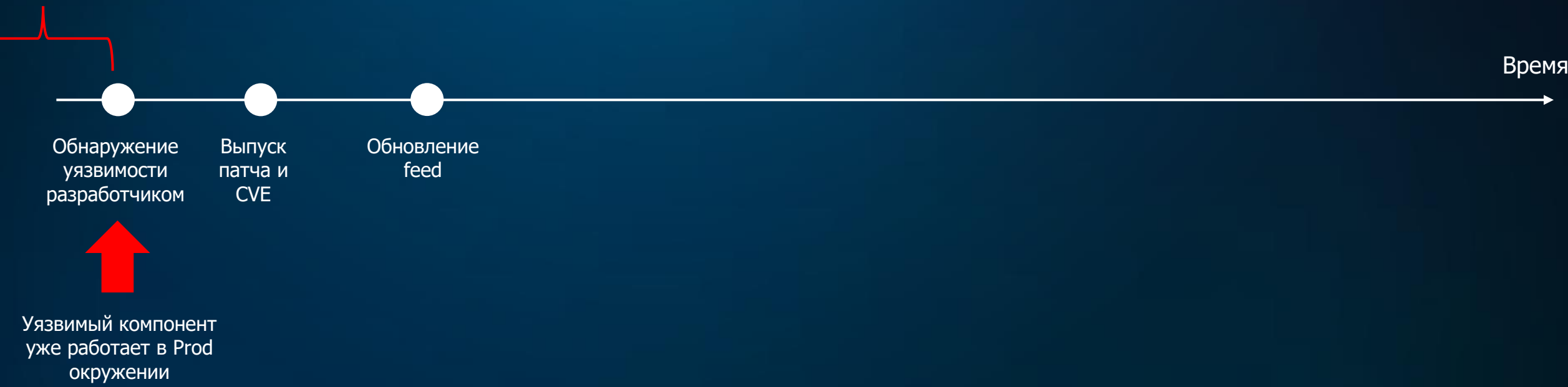
Разработка
Тестирование
Выпуск (?!)
Регистрация CVE (?!)
Корректность описания уязвимости



Работа с 1day уязвимостями

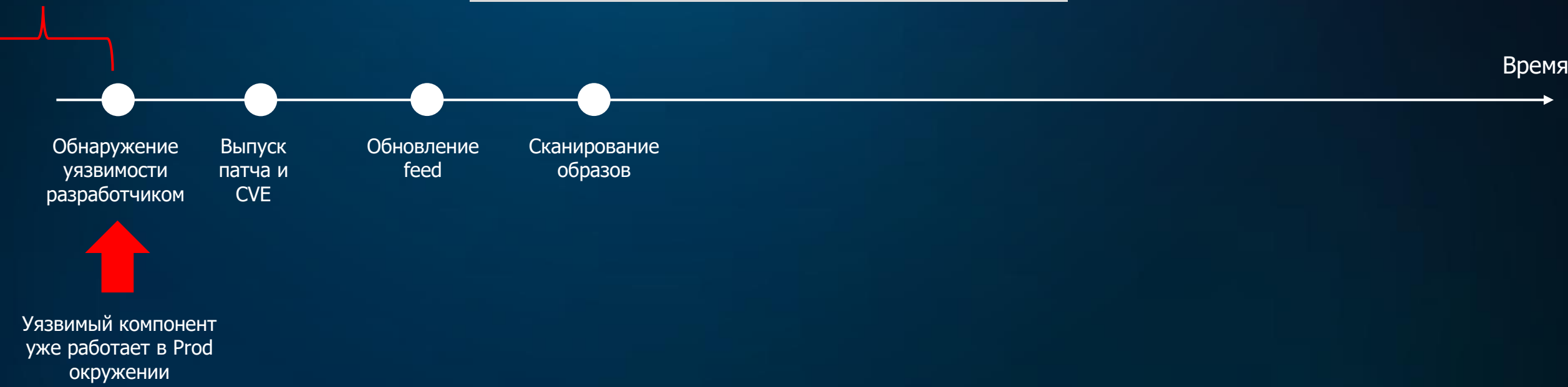
Корректность feed
Постоянный контроль и доступ до обновлений

0day



Работа с 1day уязвимостями

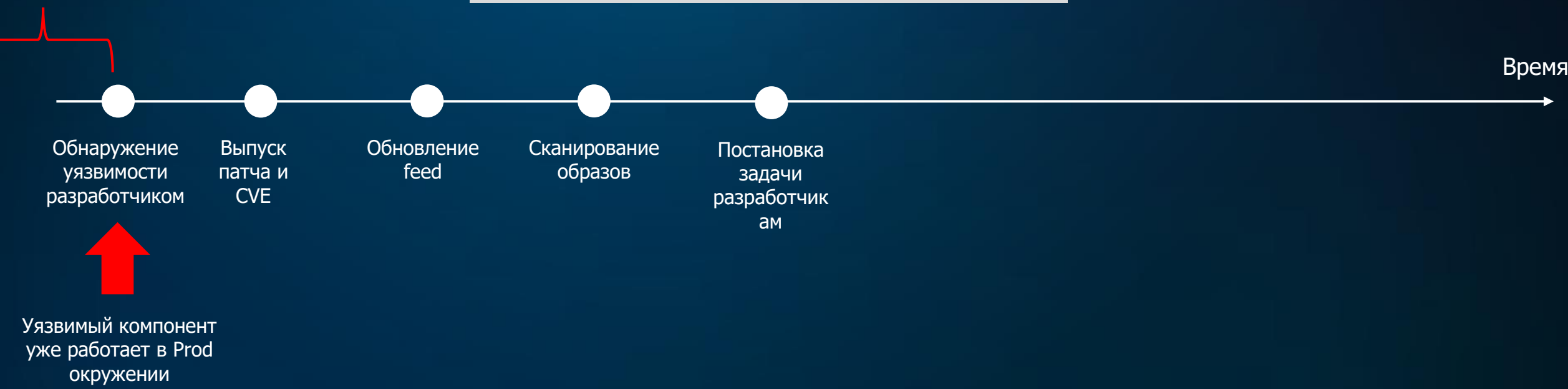
Запуск сканирований
Количество образов
Размеры образов
…
Обход сканирований
…



Рекомендация: "Malicious Compliance: Reflections on Trusting Container Image Scanners"

Работа с 1day уязвимостями

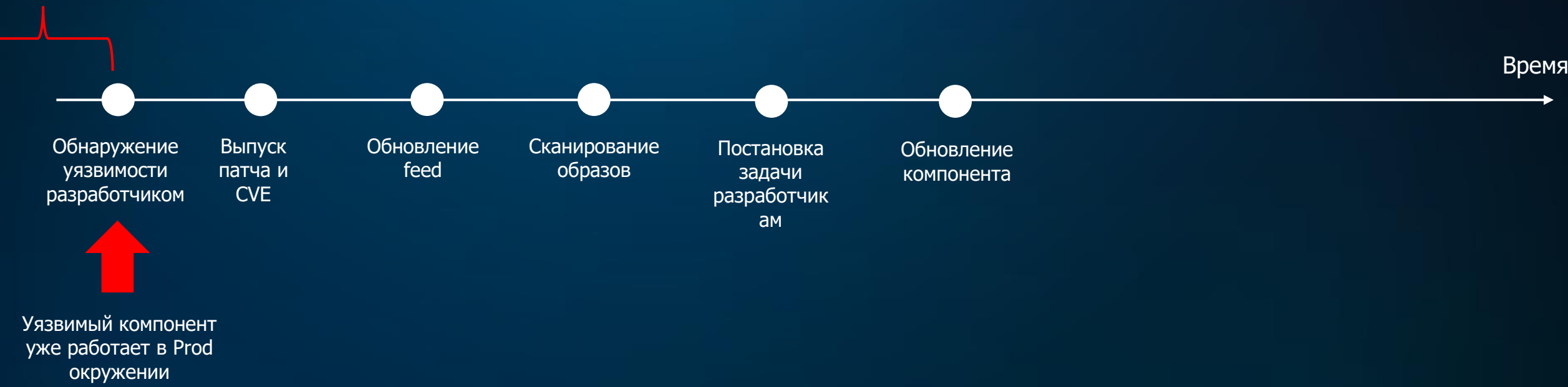
В ручную или автоматически
Работа с 1000000000000 срабатываний
Приоритезация
Директивные и транзитивные зависимости
…
Проблемы с Security Gate
…



Работа с 1day уязвимостями

Взятие фикса в работу
Коммуникация с разработкой
Сложность обновления
Не идеальность кода
…

0day

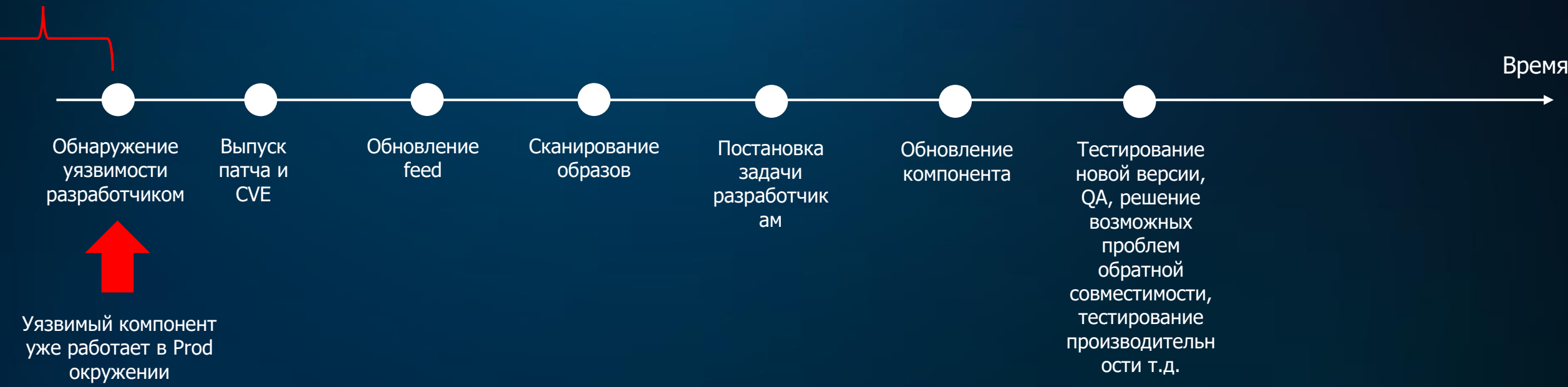


Рекомендация: "SCAзка о SCAнерах"

Работа с 1day уязвимостями

Работа QA команды
Автоматизация тестирования
Pipelines
Не идеальность кода
…

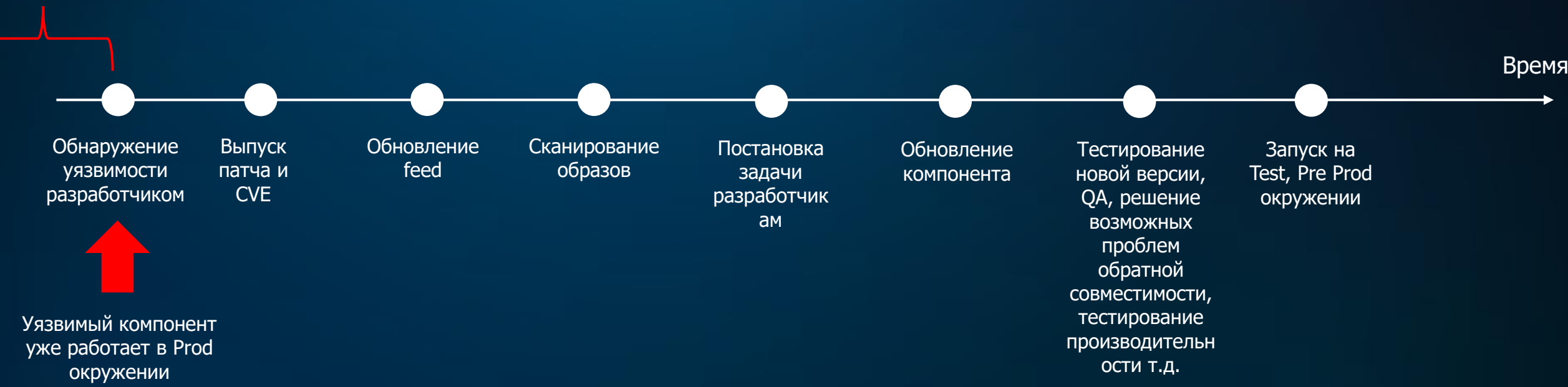
0day



Работа с 1day уязвимостями

Постепенная выкатка через дополнительные окружения

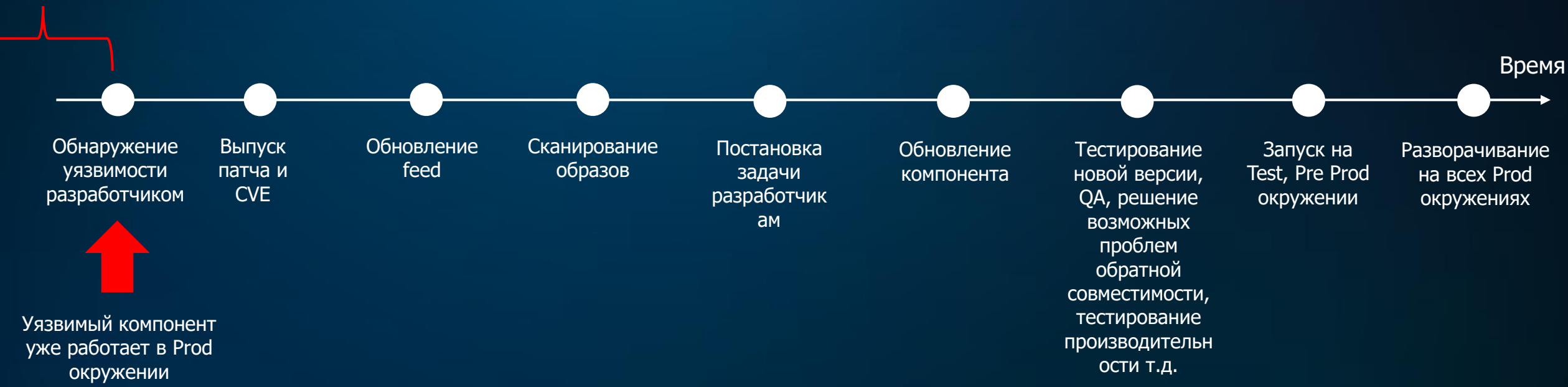
0day



Работа с 1day уязвимостями

Регламентные окна, периоды обновления
Постепенная выкатка
Размер 3rod окружения
Расположение Prod окружения
Сертифицированное ПО
…

0day



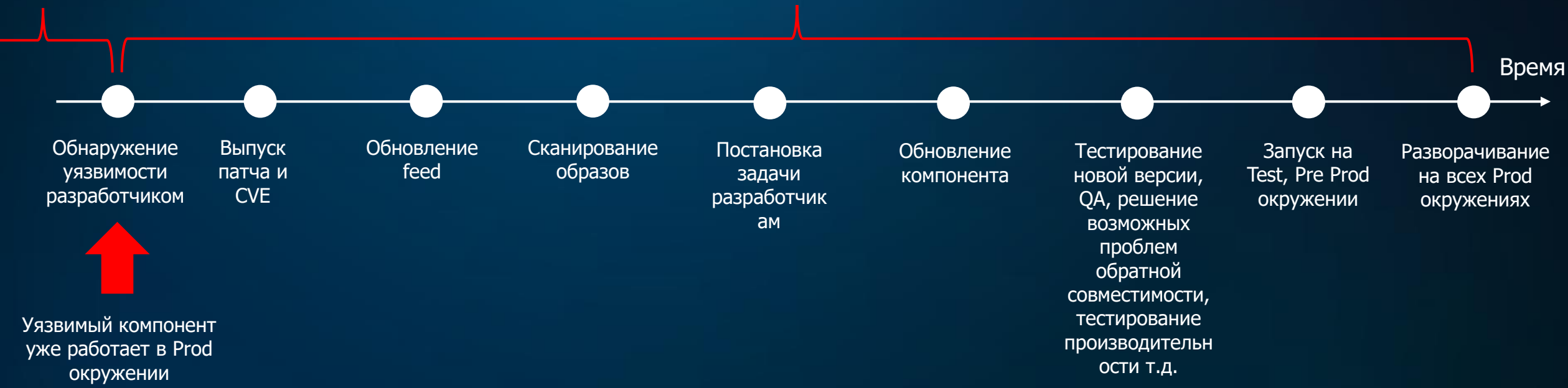
Работа с 1day уязвимостями

0day

1day

Все это время окружение уязвимо!

(от патча до эксплоита примерно от нескольких часов до 2-3 дней)



Работа с 1day уязвимостями

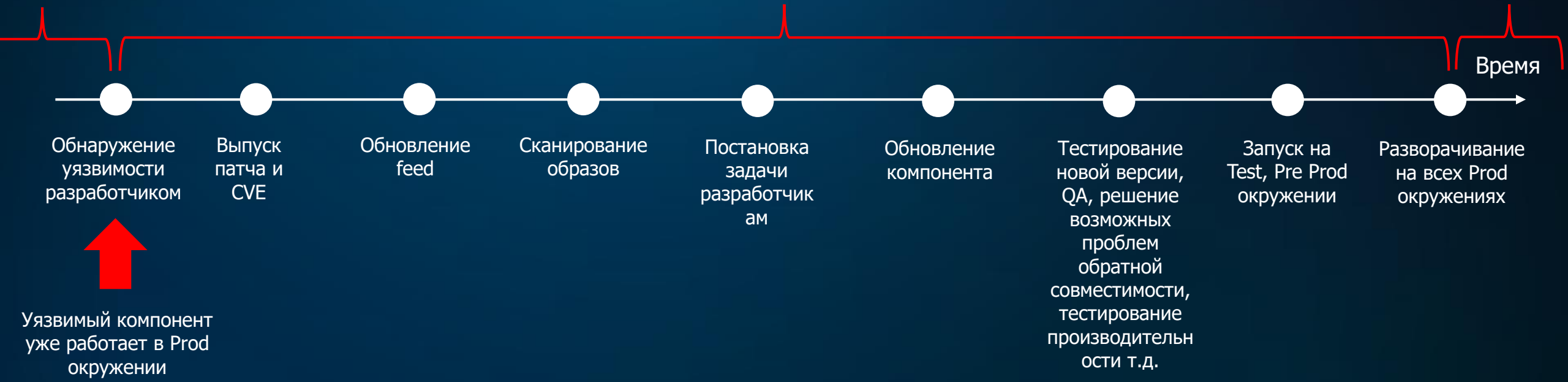
0day

1day

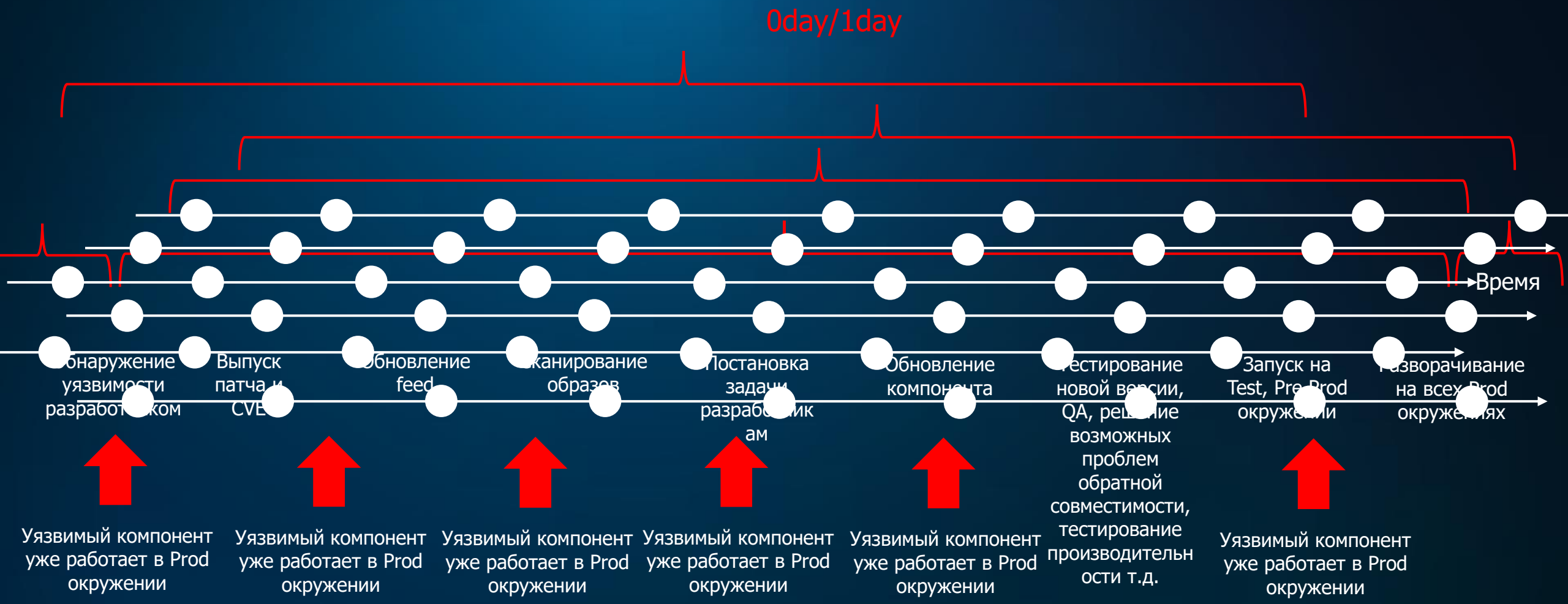
0day*

Все это время окружение уязвимо!

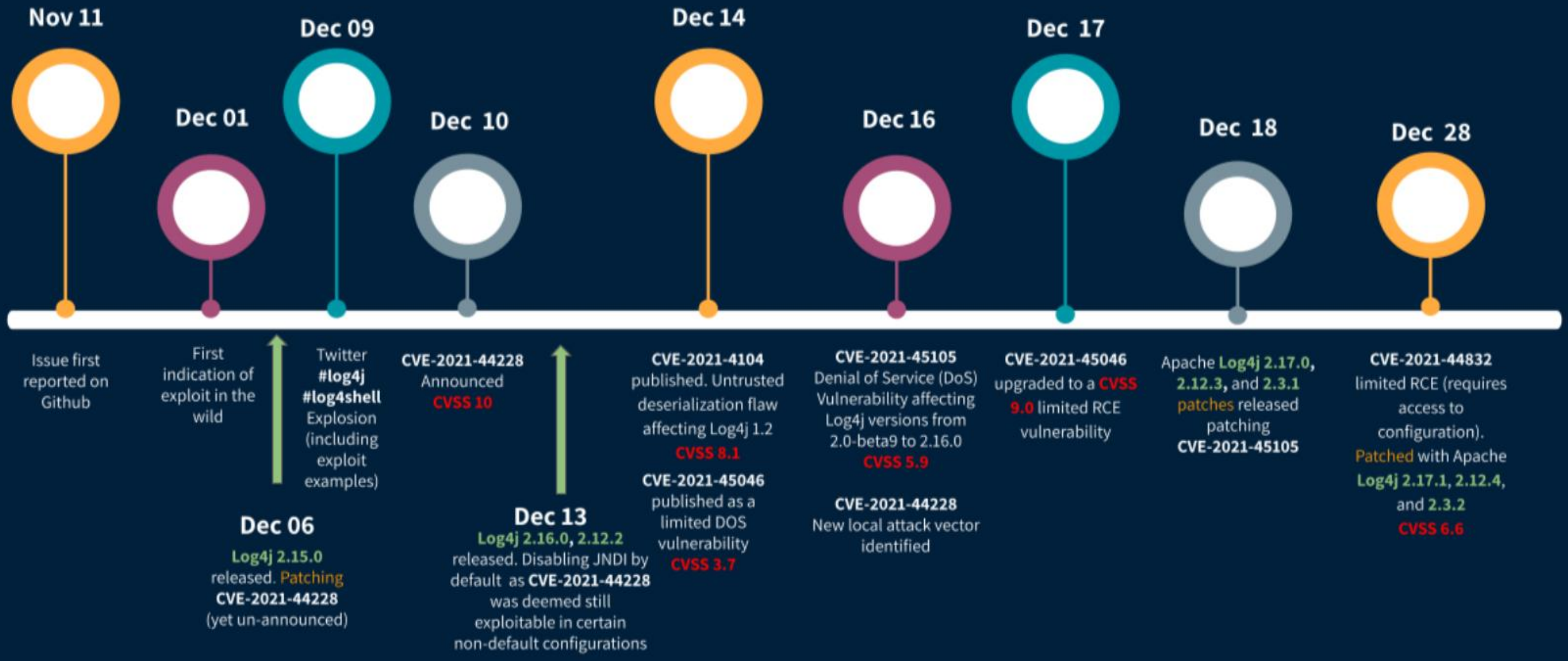
(от патча до эксплоита примерно от нескольких часов до 2-3 дней)



Работа с уязвимостями по факту



Пример: Log4shell Timeline



Источник: "Making Sense of the Constantly Changing Log4Shell Landscape."

Вредоносные зависимости

Угрозы:

- Malware
- Protestware
- Dependency Confusion
- Supply Chain Attacks
  - **SolarStorm, SUNBURST**

Источник: "SolarStorm Supply Chain Attack Timeline"

Легитимные инструменты на стороне злоумышленника

LOLBAS

☆ Star 4,616

Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our contribution guide. Our criteria list sets out what we define as a LOLBin/Script/Lib.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the ATT&CK® Navigator.

If you are looking for UNIX binaries, please visit gtfobins.github.io.

GTFOBins

☆ Star 7,188

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to ~~get the f**k~~ break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a collaborative project created by Emilio Pinna and Andrea Cardaci where everyone can contribute with additional binaries and techniques.

If you are looking for Windows binaries you should visit LOLBAS.

Attackers Abusing Legitimate Cloud Monitoring Tools to Conduct Cyber Attacks

Written by **Nicole Fishbein** - 8 September 2020

Решение

Проактивный и реактивный подход к безопасности

Cyber-resilient culture: "In building a cyber-resilient culture, the **role of security is not to stop all incidents. It is to prevent a security incident from impacting the business**."

Vulnerabilities != vulnerable

Контейнеры на страже ИБ

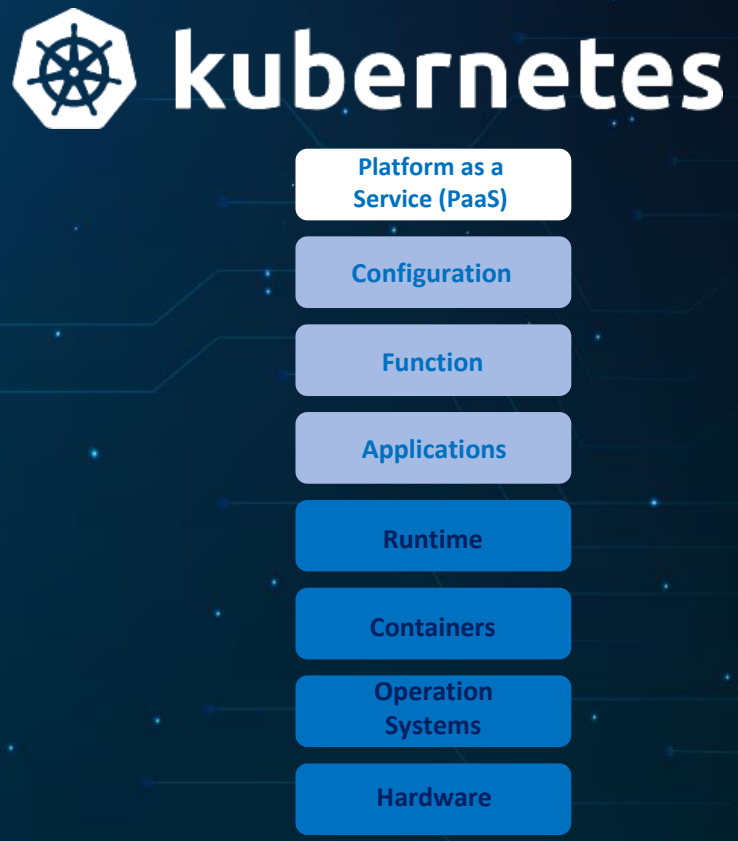
- Микросервисы (контейнеры)
  - Дополнительная изоляция
    - Дополнительный слой защиты
  - Простота
    - Микросервис проще ОС и монолитов
  - Иммутабельность образа контейнера
    - Предсказуемость поведения
  - Распредленность
    - Работа микросервисов в несколько копий
  - Эфемерность
    - Высокая скорость модификации без простоя системы

Рекомендация: "Специфика расследования инцидентов в контейнерах"

Kubernetes на страже ИБ

Kubernetes:

- Декларативность
  - Security/Policy-as-Code
    - PolicyEngines
  - Прозрачное взаимодействие с ИТ
- ZeroTrust
  - Whitelisting
  - Micro segmentation
    - NetworkPolicy
- ShiftLeftSecurity
  - SecDevSecOpsSec

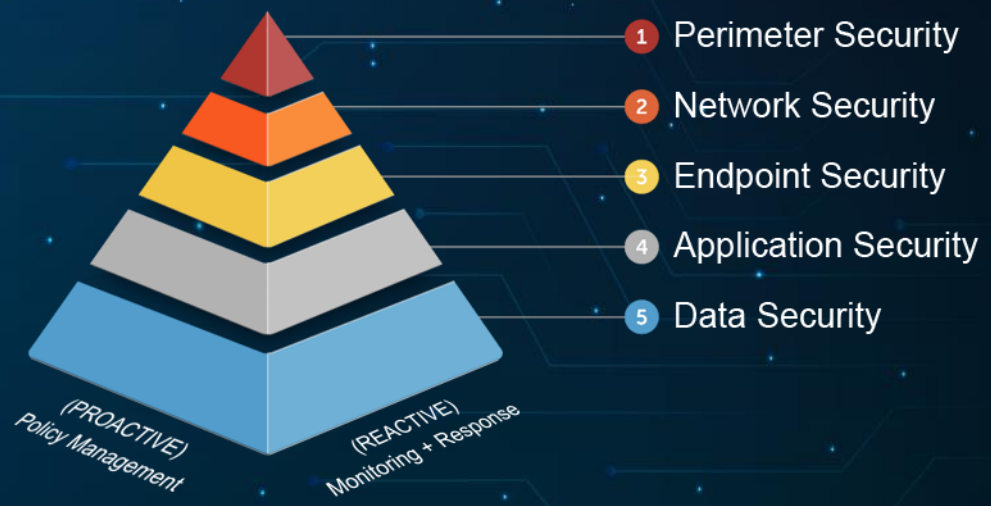


Рекомендация: "Kubernetes: трансформация к SecDevSecOpsSec“,
"Классификация и систематизация средств безопасности для Kubernetes“

Пример проактивной защиты

Микросервис:

- На базе минимального образа
  - distroless
- С файловой системой доступной только на чтение
  - SecurityContext.readOnlyRootFilesystem.true
- Без лишних возможностей
  - SecurityContext.capabilities.drop.all
- Со строго определённым набором исполняемых файлов
  - AppArmor profile
- С ограниченной активностью по сети
  - NetworkPolicy



Рекомендация: "Сочетание несочетаемого в Kubernetes: удобство, производительность, безопасность"

Выводы и рекомендации

1. Понимайте задачу/проблемы на всем ее жизненном цикле
2. Стройте свою безопасность с мыслью, что вас точно взломают
3. Помогайте бизнесу/ИТ/разработке, а не просто соответствуйте требованиям

Спасибо за внимание!

Дмитрий Евдокимов
Founder&CTO

Email: de@luntry.ru
Twitter: @evdokimovds
@Qu3b3c
Channel: @k8security
Site: www.luntry.ru

k8security luntrysolution