TRUE TECH DAY

Безопасность контейнеров и Kubernetes

Luntry

Дмитрий Евдокимов

Founder&CTO LUNTRY

About me

- Основатель и технический директор Luntry
- Опыт в ИБ более 10 лет
- CFP ZeroNights, DevOpsConf
- Бывший автор статей и редактор рубрик в журнале “ХАКЕР”
- Автор 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, KuberConf, VK Kubernetes Conference, HighLoad++ и др.

Проблематика

Работа с 1day уязвимостями

Время

Обнаружение уязвимости разработчиком

Работа с 1day уязвимостями

Oday

Время

Обнаружение уязвимости разработчиком

Уязвимый компонент уже работает в Prod окружении

Работа с 1day уязвимостями

Oday

Время

Обнаружение уязвимости разработчиком

Выпуск патча и CVE

Уязвимый компонент уже работает в Prod окружении

Работа с 1day уязвимостями

Oday

Время

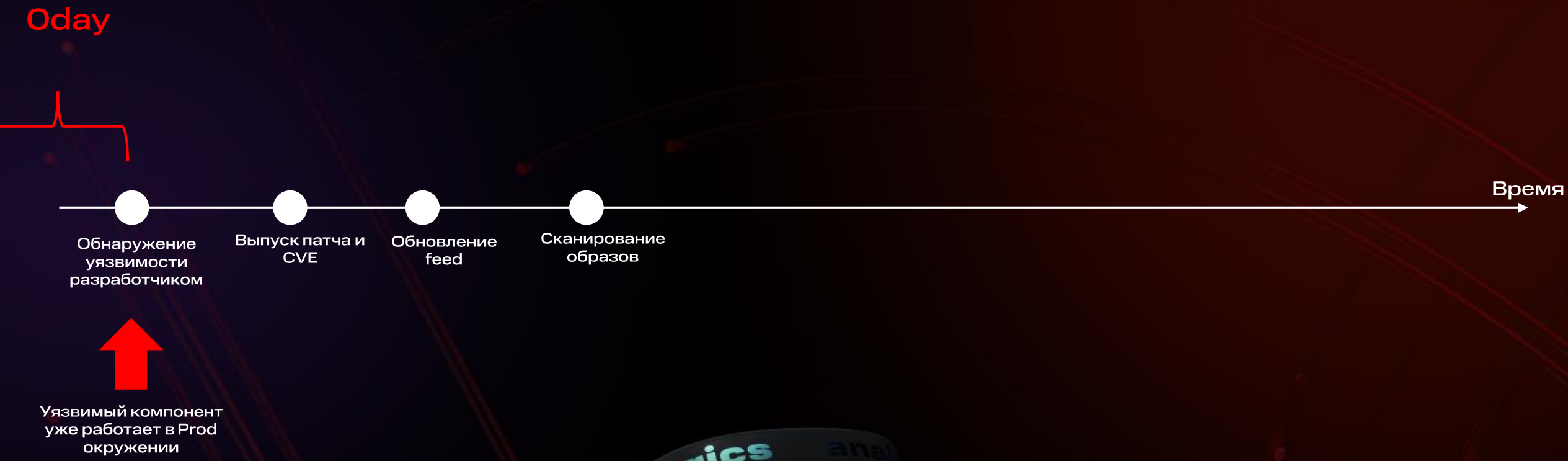
Обнаружение уязвимости разработчиком

Выпуск патча и CVE

Обновление feed

Уязвимый компонент уже работает в Prod окружении

Работа с 1day уязвимостями



Работа с 1day уязвимостями

Oday

Время

- Обнаружение уязвимости разработчиком
- Выпуск патча и CVE
- Обновление feed
- Сканирование образов
- Постановка задачи разработчикам

Уязвимый компонент уже работает в Prod окружении

Работа с 1day уязвимостями

Oday

Обнаружение уязвимости разработчиком

Выпуск патча и CVE

Обновление feed

Сканирование образов

Постановка задачи разработчикам

Обновление компонента

Время

Уязвимый компонент уже работает в Prod окружении

Работа с 1day уязвимостями

Oday

Обнаружение уязвимости разработчиком

Выпуск патча и CVE

Обновление feed

Сканирование образов

Постановка задачи разработчикам

Обновление компонента

Тестирование новой версии, QA, решение возможных проблем обратной совместимости, тестирование производительности т.д.

Время

Уязвимый компонент уже работает в Prod окружении

Работа с 1day уязвимостями

Oday

Обнаружение уязвимости разработчиком

Выпуск патча и CVE

Обновление feed

Сканирование образов

Постановка задачи разработчикам

Обновление компонента

Тестирование новой версии, QA, решение возможных проблем обратной совместимости, тестирование производительности т.д.

Запуск на Test, Pre Prod окружении

Время

Уязвимый компонент уже работает в Prod окружении

Работа с 1day уязвимостями

Oday

Обнаружение уязвимости разработчиком

Выпуск патча и CVE

Обновление feed

Сканирование образов

Постановка задачи разработчикам

Обновление компонента

Тестирование новой версии, QA, решение возможных проблем обратной совместимости, тестирование производительности т.д.

Запуск на Test, Pre Prod окружении

Разворачивание на всех Prod окружениях

Время

Уязвимый компонент уже работает в Prod окружении

Работа с 1day уязвимостями

1day
Все это время окружение уязвимо!

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

Oday

Время

- Обнаружение уязвимости разработчиком
- Выпуск патча и CVE
- Обновление feed
- Сканирование образов
- Постановка задачи разработчикам
- Обновление компонента
- Тестирование новой версии, QA, решение возможных проблем обратной совместимости, тестирование производительности т.д.
- Запуск на Test, Pre Prod окружении
- Разворачивание на всех Prod окружениях

Уязвимый компонент уже работает в Prod окружении

Работа с 1day уязвимостями

1day
Все это время окружение уязвимо!
(от патча до эксплоита примерно от нескольких часов до 2-3 дней)

Oday

Oday *

Время

- Обнаружение уязвимости разработчиком
- Выпуск патча и CVE
- Обновление feed
- Сканирование образов
- Постановка задачи разработчикам
- Обновление компонента
- Тестирование новой версии, QA, решение возможных проблем обратной совместимости, тестирование производительности т.д.
- Запуск на Test, Pre Prod окружении
- Разворачивание на всех Prod окружениях

Уязвимый компонент уже работает в Prod окружении

Работа с уязвимостями по факту

Oday/1day

Время

Обнаружение уязвимости разработчиками

Выпуск патча и CVE

Обновление feed

Сканирование образов

Постановка задачи разработчикам

Обновление компонента

Тестирование новой версии, QA, решение возможных проблем обратной совместимости, тестирование производительности т.д.

Запуск в Pre Prod окружении

Разворачивание на всех Prod окружениях

Уязвимый компонент уже работает в Prod окружении

Уязвимый компонент уже работает в Prod окружении

Уязвимый компонент уже работает в Prod окружении

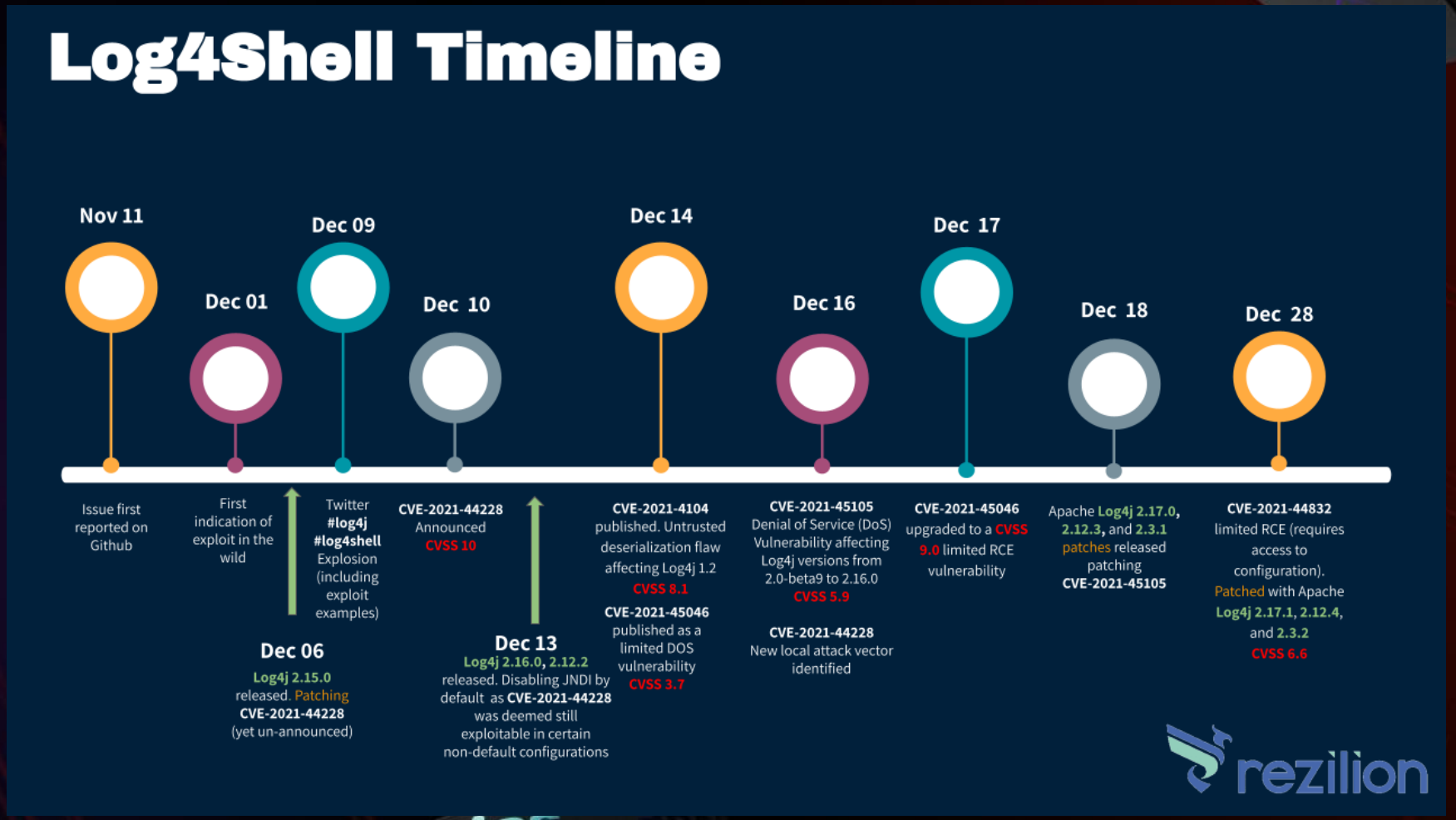
Уязвимый компонент уже работает в Prod окружении

Уязвимый компонент уже работает в Prod окружении

Уязвимый компонент уже работает в Prod окружении

Уязвимый компонент уже работает в Prod окружении

Пример: Log4shell

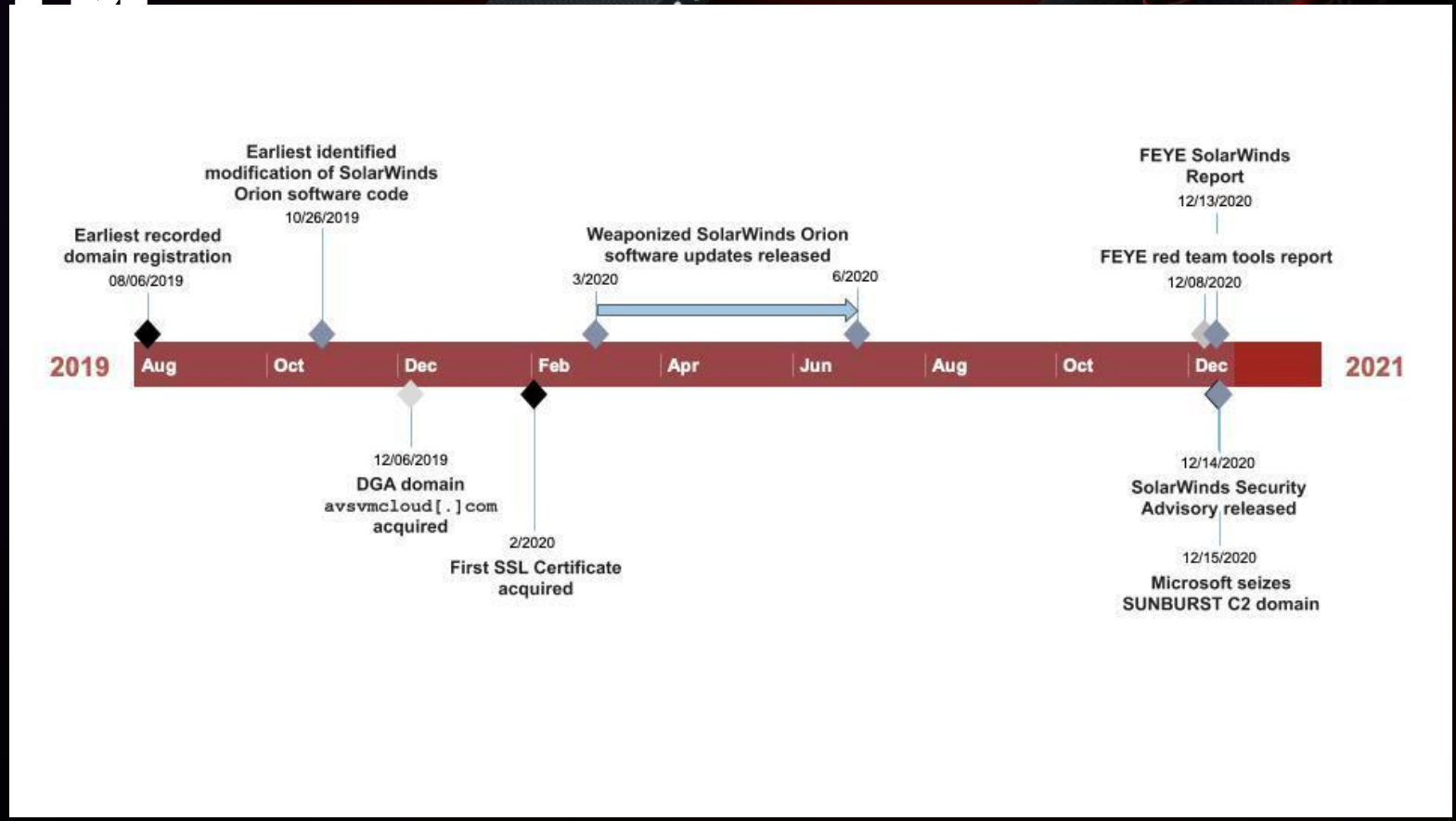


Источник: “Making Sense of the Constantly Changing Log4Shell Landscape”

Вредоносные зависимости

Угрозы:
- Malware
- Protestware
- Dependency Confusion
- Supply Chain Attacks
  - SolarStorm, SUNBURST

Современные приложения на
60-70% состоят из стороннего кода!



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

Kubernetes на страже ИБ

Kubernetes:

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

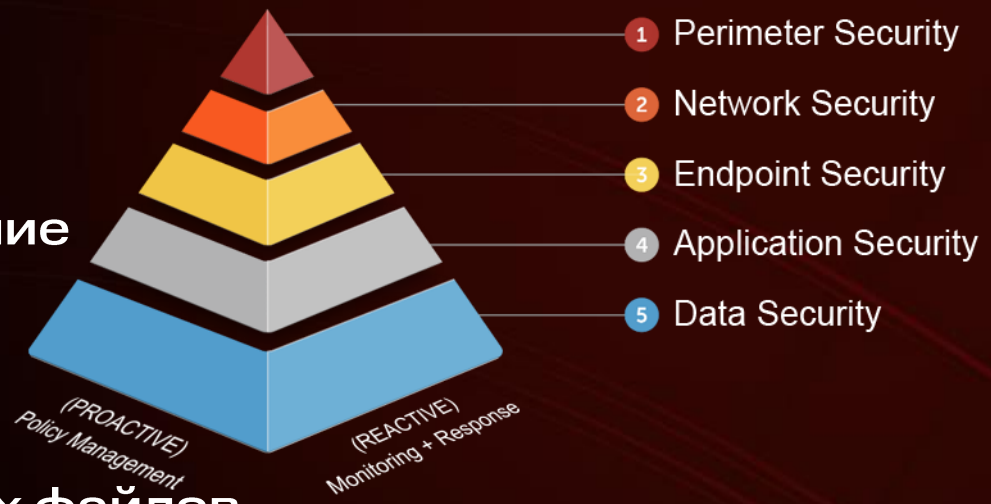
kubernetes

- Platform as a Service (PaaS)
- Configuration
- Function
- Applications
- Runtime
- Containers
- Operation Systems
- Hardware

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



Выводы и рекомендации

1. Меняйте/расширяйте парадигму построения ИБ: от реактивной к проактивной
2. Контейнеры и Kubernetes не только нужно защищать, но и использовать их свойства для построения эффективной, проактивной, эшелонированной защиты
3. Безопасность должна быть понятной, прозрачной и не тормозить бизнес и ИТ

TRUE TECH DAY 31.03

СПАСИБО ЗА ВНИМАНИЕ!

Luntry

Дмитрий Евдокимов

Founder&CTO LUNTRY

de@luntry.ru

CONTACTS:

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