LUNTRY

ИТОГИ 2025

Дмитрий Евдокимов

Founder&CTO Luntry

Обо мне

”

Я не верю в то, что систему можно сделать надежной и безопасной, не понимая того, как она устроена.

Основатель и технический директор Luntry

Более 15 лет опыта в ИБ

Специализация – безопасность контейнеров и Kubernetes

Автор ТГ-канала k8s(in)security

Эксперт в сфере безопасности контейнерных сред

- Организатор конференции «БеКон» по БЕзопасности КОНтейнеров
- Бывший редактор рубрик в журнале «ХАКЕР», автор серии статей
- Автор курса «Cloud Native безопасность в Kubernetes»
- Участник программного комитета CFP DevOpsConf и KUBER CONF

Спикер

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

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 всех 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	Kubernetes в 2025
02	Уязвимости, атаки, инциденты 2025
03	Luntry в 2025
04	Что там в 2026?
05	Выводы

KUBERNETES B 2025

Релизы 2025 года

- 1.33 - Octarine: The Color of Magic
- 1.34 - Of Wind & Will (O' WaW)
- 1.35 - World Tree

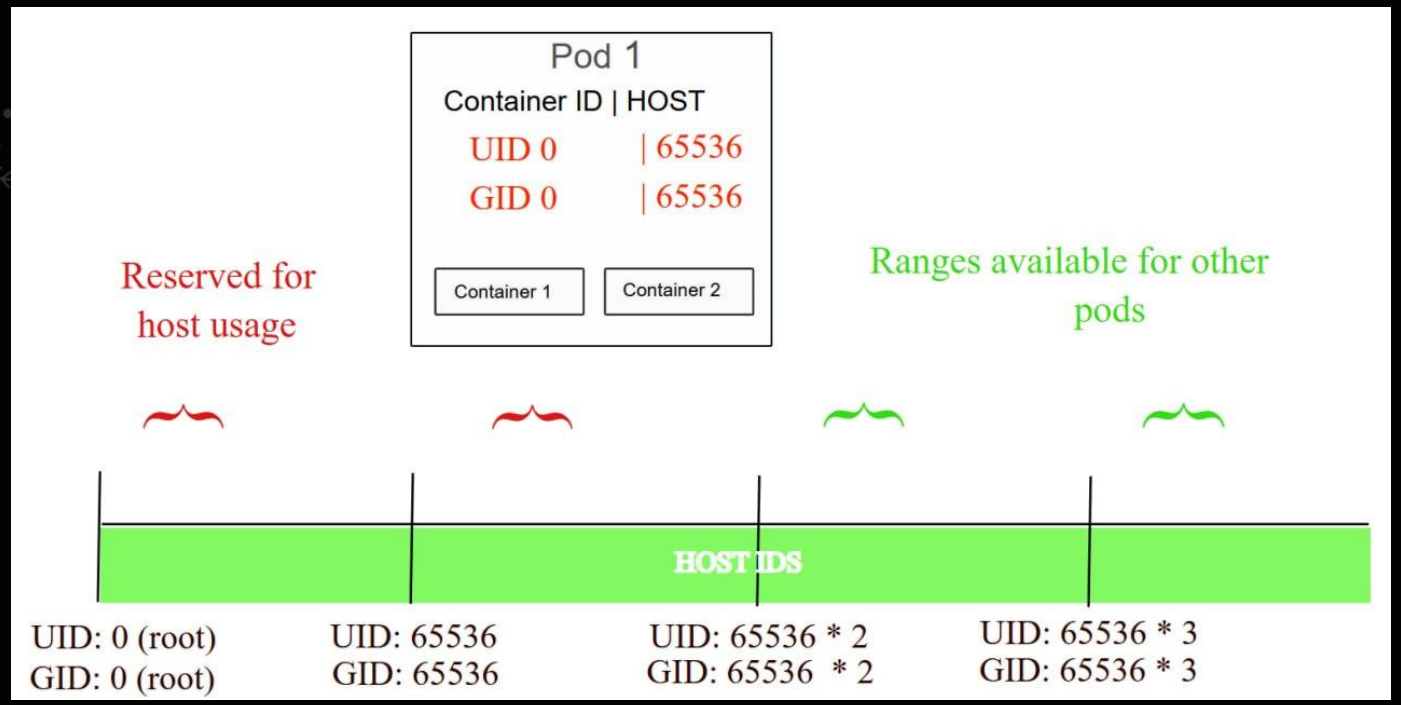
LUNTRY

Новая версия CIS

- Выпуск CIS Kubernetes Benchmark – 1.12
  - Для 1.32 – 1.34

User Namespaces в Pods

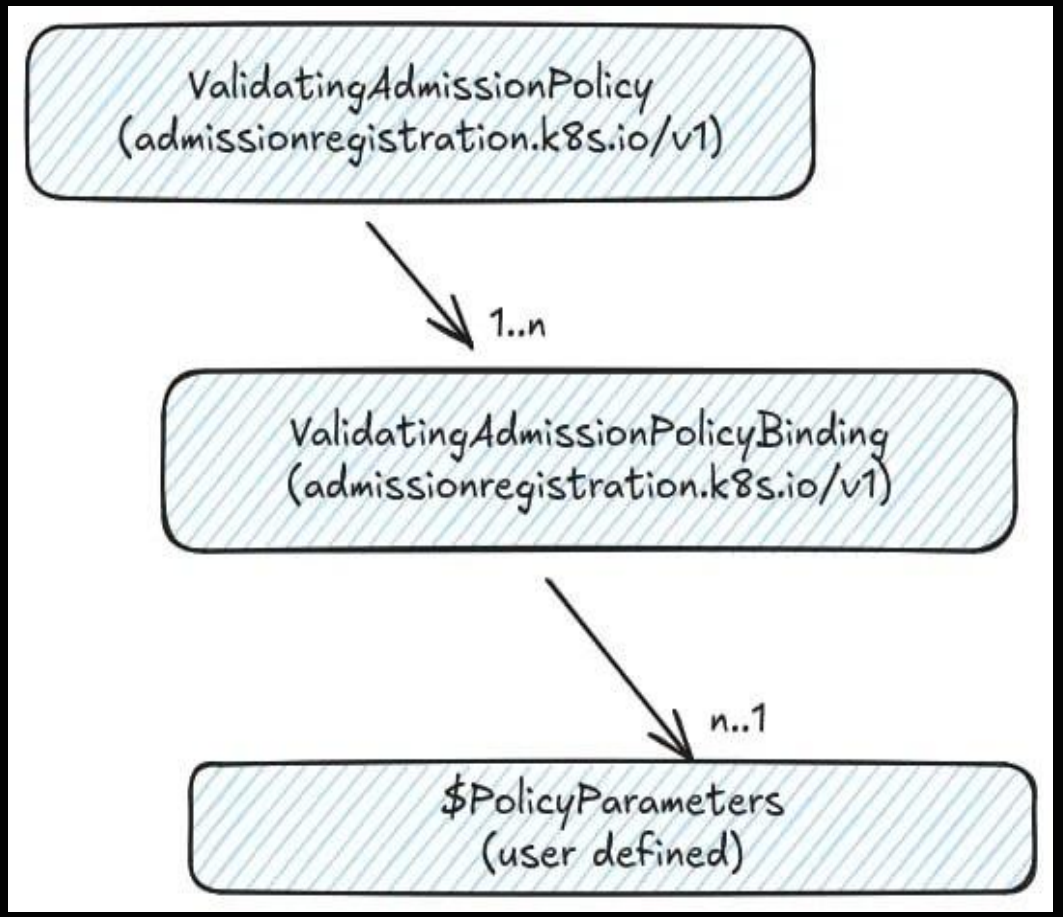
- Функциональность шла до GA целых 9 лет!
- "Kubernetes v1.33: User Namespaces enabled by default!"




```yaml
apiVersion: v1
kind: Pod
metadata:
  name: userns
spec:
  hostUsers: false
  containers:
  - name: shell
    command: ["sleep", "infinity"]
    image: debian
```

Validating Admission Policy (VAP)

- VAP
  - В alpha с 1.26
  - В stable с 1.30
- Поддержка VAP сторонними PolicyEngine:
  - Gatekeeper с версии 1.13
  - Kyverno с версии 1.11
- MutatingAdmissionPolicy (MAP)
  - В alpha с 1.30
  - В beta с 1.34



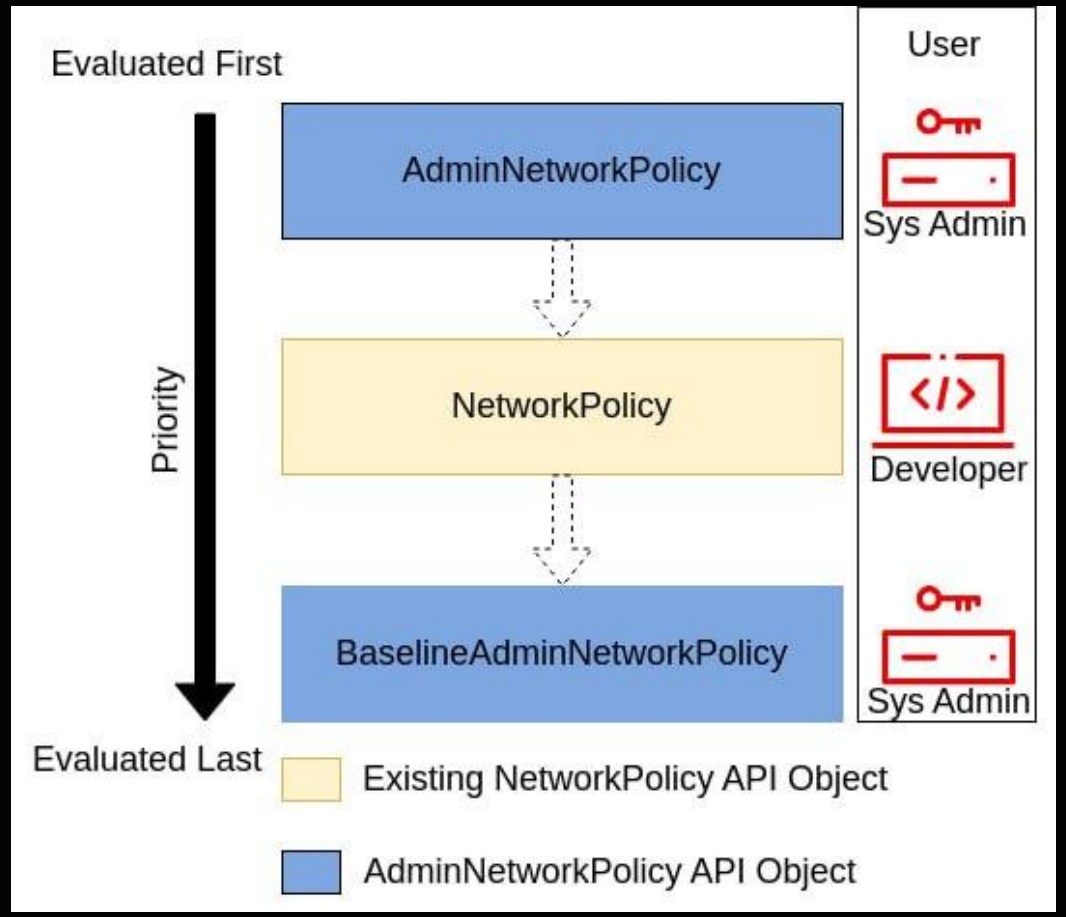
LUNTRY

Развитие NetworkPolicy

В Calico:
- AdminNetworkPolicy с версии 3.29
- BaselineAdminNetworkPolicy с версии 3.30

В Antrea:
- AdminNetworkPolicy с версии 1.13
- BaselineAdminNetworkPolicy с версии 1.13

В Cilium пока безрезультатно - обсуждение идет тут



LUNTRY

Драма с Ingress NGINX

LUNTRY

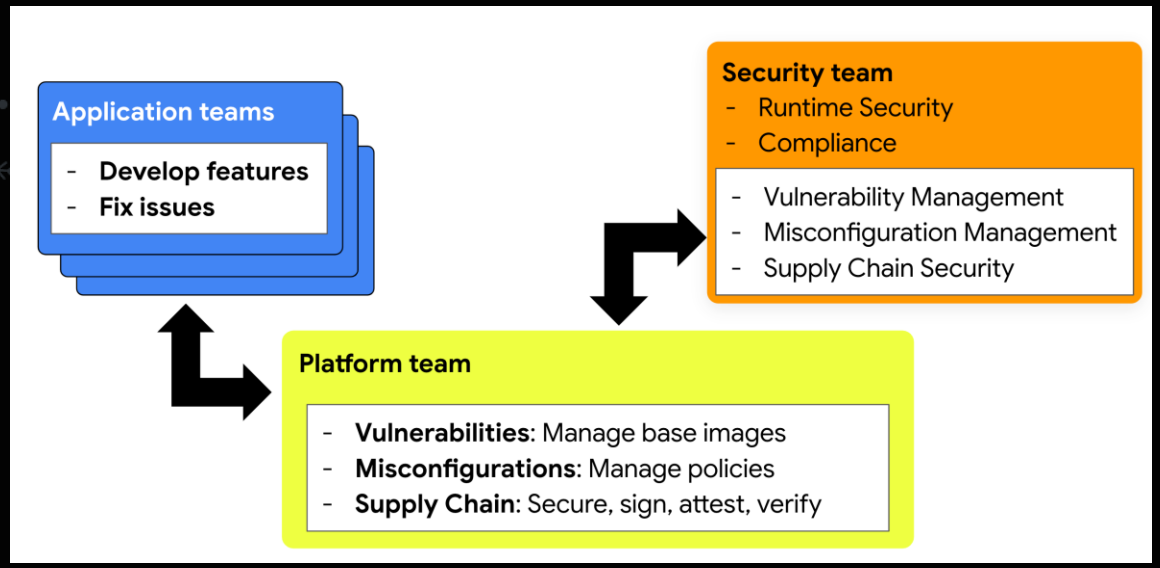
- Проект прекращает своё существование
  - После февраля 2026 года разработка остановится
  - Ориентир на миграцию к Gateway API
  - “Ingress NGINX Retirement: What You Need to Know”
- Все помнят IngressNightmare, CVE-2024-7646, CVE-2023-5044, CVE-2023-5043, CVE-2022-4886, CVE-2021-25742, ...

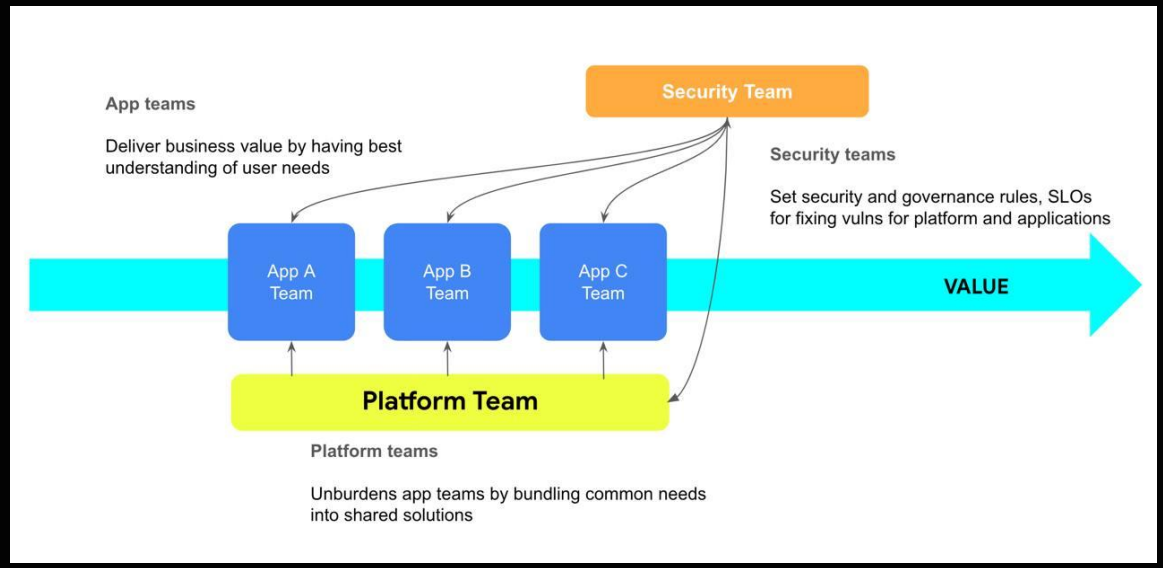
History and Challenges

The breadth and flexibility of Ingress NGINX has caused maintenance challenges. Changing expectations about cloud native software have also added complications. What were once considered helpful options have sometimes come to be considered serious security flaws, such as the ability to add arbitrary NGINX configuration directives via the "snippets" annotations. Yesterday's flexibility has become today's insurmountable technical debt.

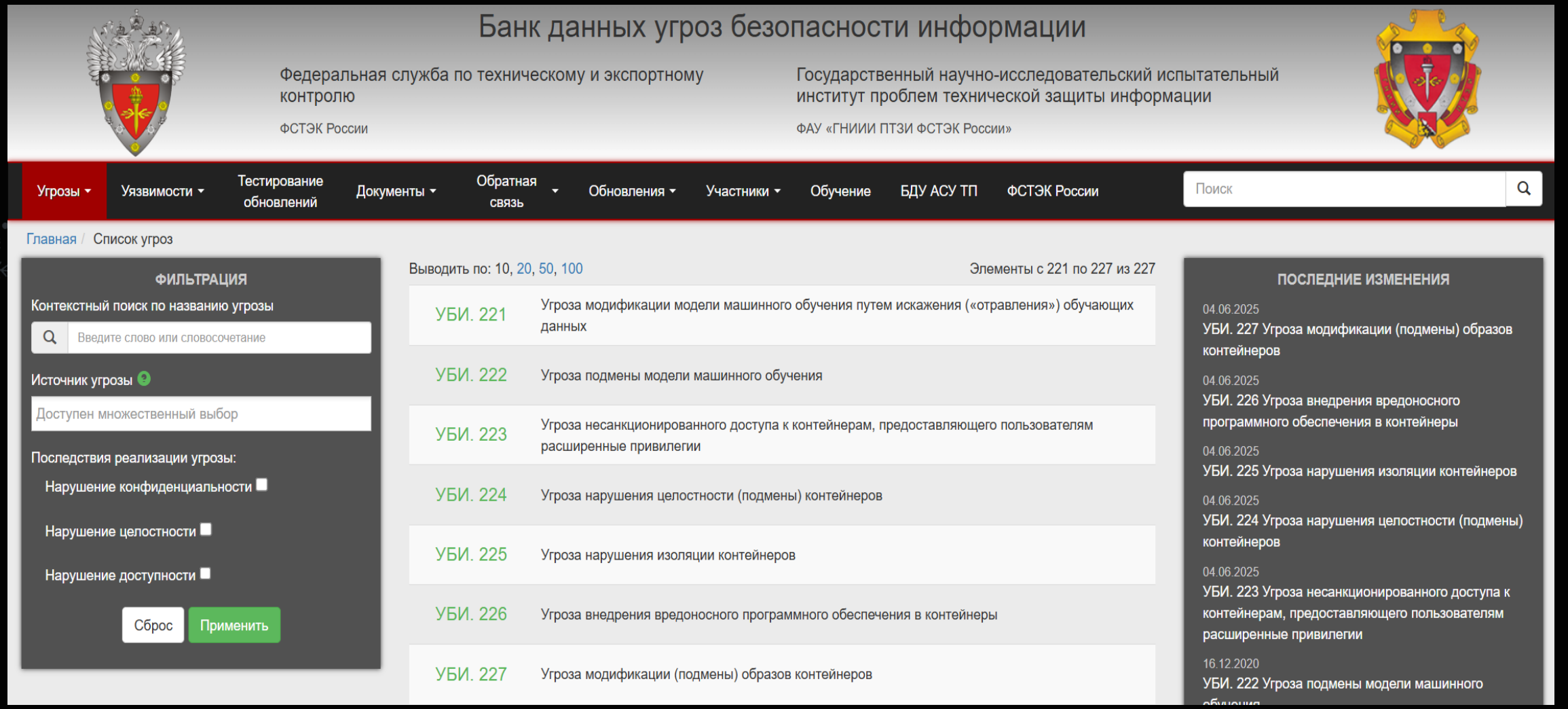
Shift Down Security

- SIG Security Kubernetes опубликовала документ под названием “Shift Down Security”

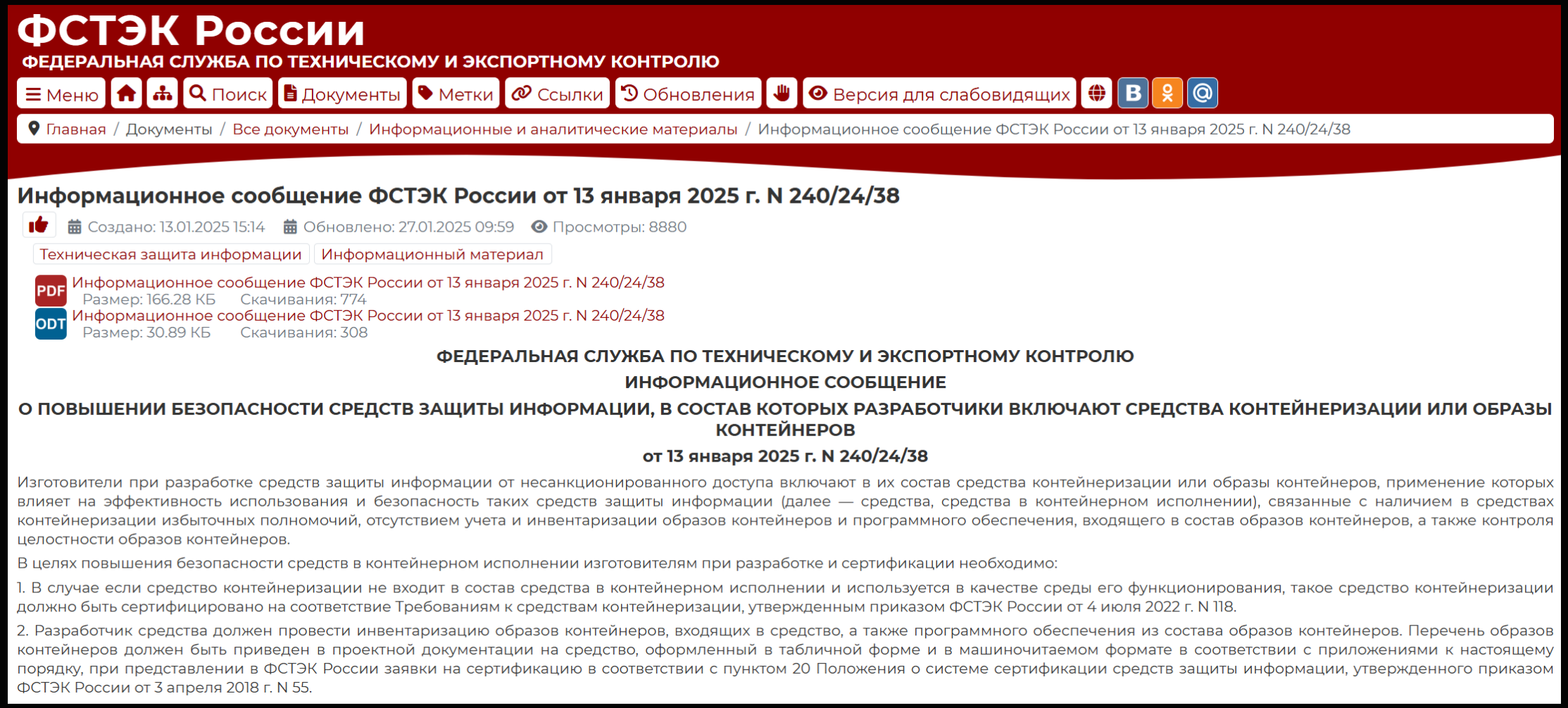




УБИ по контейнеризации



Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38



ФСТЭК России
ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Меню | Поиск | Документы | Метки | Ссылки | Обновления | Версия для слабовидящих

Главная / Документы / Все документы / Информационные и аналитические материалы / Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38

Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38

Создано: 13.01.2025 15:14 Обновлено: 27.01.2025 09:59 Просмотры: 8880

Техническая защита информации | Информационный материал

PDF Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38
Размер: 166.28 КБ Скачивания: 774

ODT Информационное сообщение ФСТЭК России от 13 января 2025 г. N 240/24/38
Размер: 30.89 КБ Скачивания: 308

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

О ПОВЫШЕНИИ БЕЗОПАСНОСТИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ, В СОСТАВ КОТОРЫХ РАЗРАБОТЧИКИ ВКЛЮЧАЮТ СРЕДСТВА КОНТЕЙНЕРИЗАЦИИ ИЛИ ОБРАЗЫ КОНТЕЙНЕРОВ

от 13 января 2025 г. N 240/24/38

Изготовители при разработке средств защиты информации от несанкционированного доступа включают в их состав средства контейнеризации или образы контейнеров, применение которых влияет на эффективность использования и безопасность таких средств защиты информации (далее — средства, средства в контейнерном исполнении), связанные с наличием в средствах контейнеризации избыточных полномочий, отсутствием учета и инвентаризации образов контейнеров и программного обеспечения, входящего в состав образов контейнеров, а также контроля целостности образов контейнеров.

В целях повышения безопасности средств в контейнерном исполнении изготовителям при разработке и сертификации необходимо:

1. В случае если средство контейнеризации не входит в состав средства в контейнерном исполнении и используется в качестве среды его функционирования, такое средство контейнеризации должно быть сертифицировано на соответствие Требованиям к средствам контейнеризации, утвержденным приказом ФСТЭК России от 4 июля 2022 г. N 118.

2. Разработчик средства должен провести инвентаризацию образов контейнеров, входящих в средство, а также программного обеспечения из состава образов контейнеров. Перечень образов контейнеров должен быть приведен в проектной документации на средство, оформленный в табличной форме и в машиночитаемом формате в соответствии с приложениями к настоящему порядку, при представлении в ФСТЭК России заявки на сертификацию в соответствии с пунктом 20 Положения о системе сертификации средств защиты информации, утвержденного приказом ФСТЭК России от 3 апреля 2018 г. N 55.

Сообщество K8s в России растет

KUBER CONF

Первая некоммерческая коммьюнити конференция по K8s в РФ. Объединим экспертов на одной площадке, чтобы поговорить про новые подходы в разработке Kubernetes®.

https://k8sqday.ru/

https://aot-kuberconf.ru/

LUNTRY

УЯЗВИМОСТИ, АТАКИ, ИНЦИДЕНТЫ 2025

Уязвимости Kubernetes за 2025 год

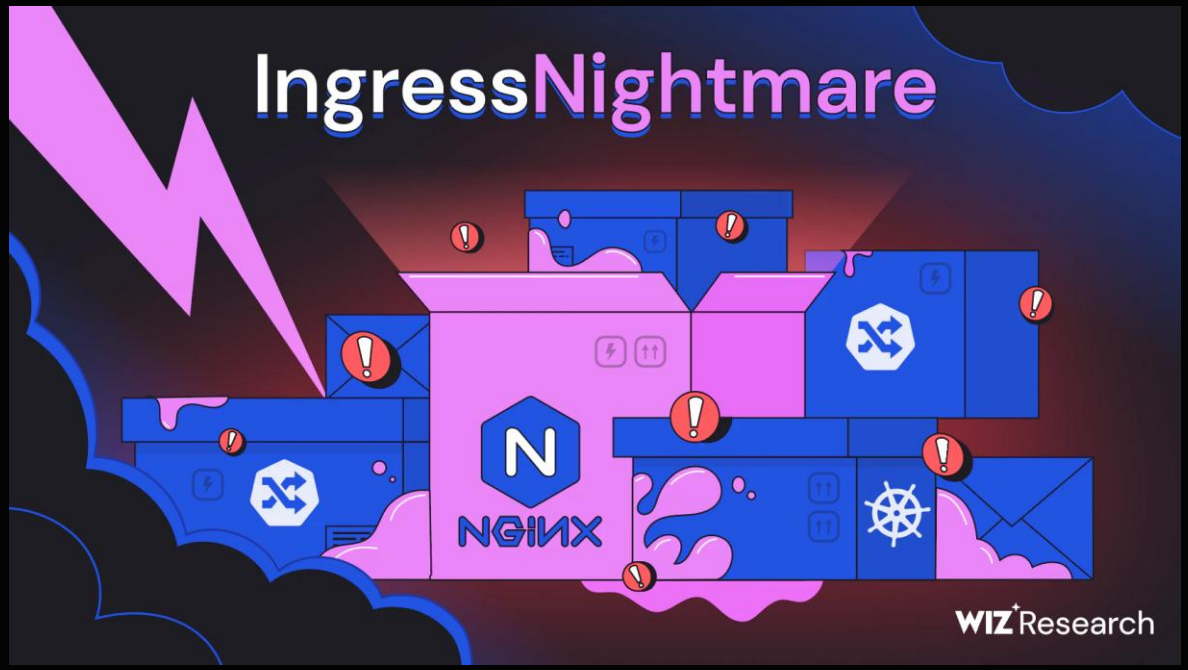
- 13 CVE

CVE ID	Issue Summary	Issue URL
CVE-2025-13281	Portworx Half-Blind SSRF in kube-controller-manager	#135525
CVE-2025-9708	Kubernetes C# Client: improper certificate validation in custom CA mode may lead to man-in-the-middle attacks	#134063
CVE-2025-7445	secrets-store-sync-controller discloses service account tokens in logs	#133897
CVE-2025-5187	Nodes can delete themselves by adding an OwnerReference	#133471
CVE-2025-7342	VM images built with Kubernetes Image Builder Nutanix or OVA providers use default credentials for Windows images if user did not override	#133115
CVE-2025-4563	Nodes can bypass dynamic resource allocation authorization checks	#132151
CVE-2025-1974	ingress-nginx admission controller RCE escalation	#131009
CVE-2025-1098	ingress-nginx controller configuration injection via unsanitized mirror annotations	#131008
CVE-2025-1097	ingress-nginx controller configuration injection via unsanitized auth-tls-match-cn annotation	#131007
CVE-2025-24514	ingress-nginx controller configuration injection via unsanitized auth-url annotation	#131006
CVE-2025-24513	ingress-nginx controller auth secret file path traversal vulnerability	#131005
CVE-2025-1767	GitRepo Volume Inadvertent Local Repository Access	#130786
CVE-2025-0426	Node Denial of Service via kubelet Checkpoint API	#130016

LUNTRY

Ingress Nightmare

- CVE-2025-1097
- CVE-2025-1098
- CVE-2025-24514
- CVE-2025-1974
  - 9.8 Critical Unauthenticated Remote Code Execution

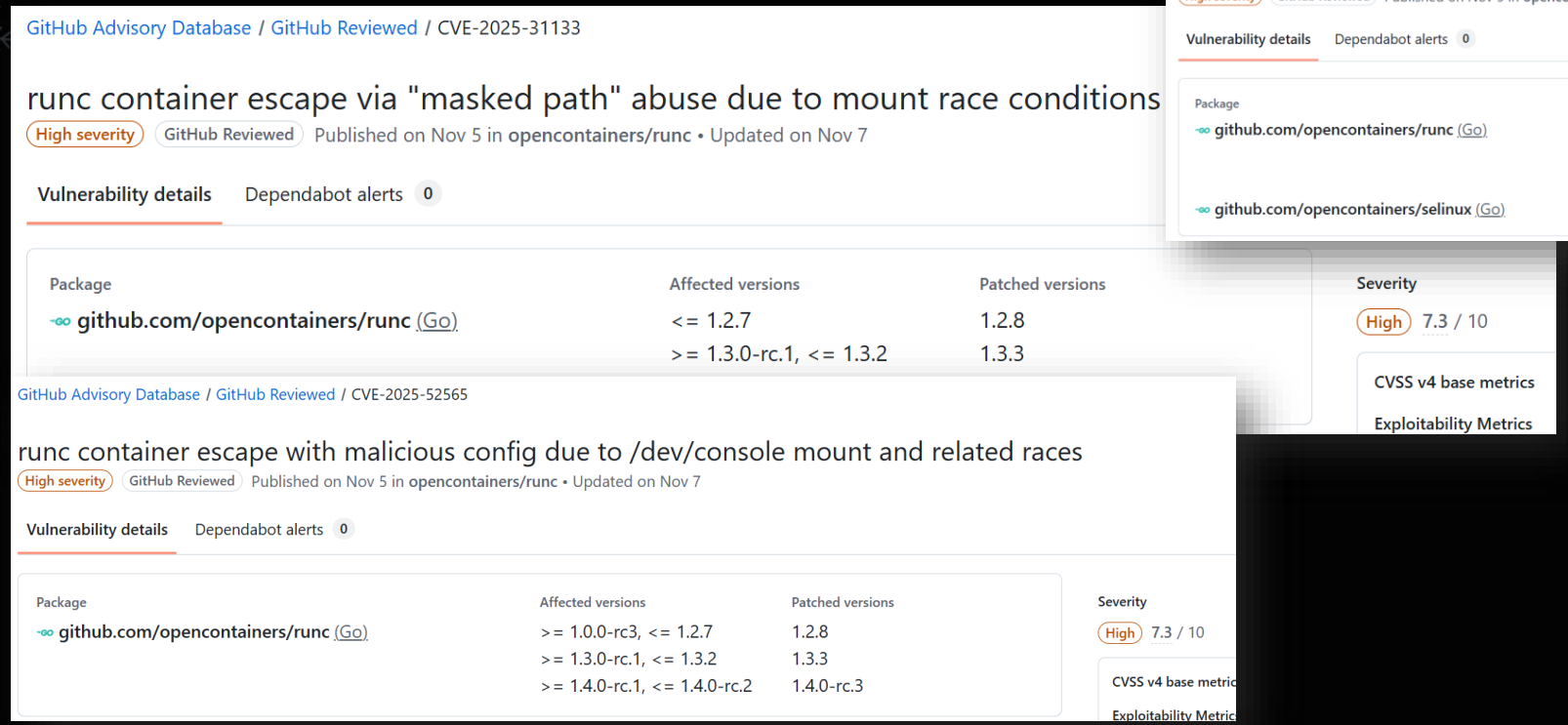


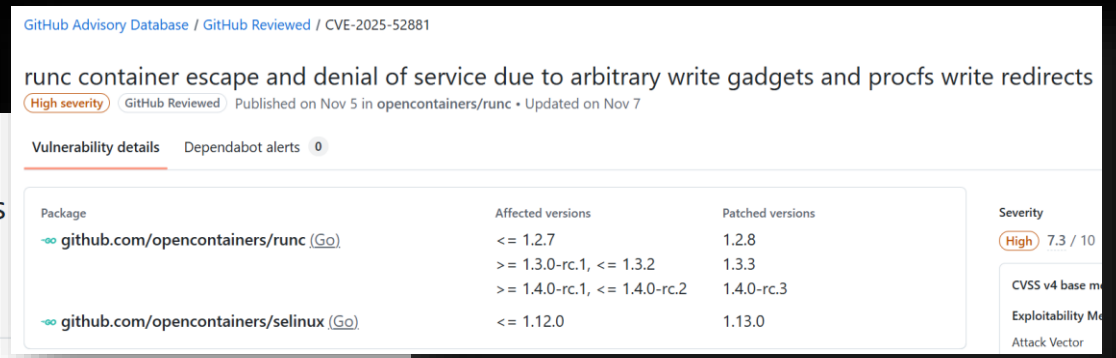
При использовании NetworkPolicy это вообще
не проблема ;)

LUNTRY

Уязвимости runc

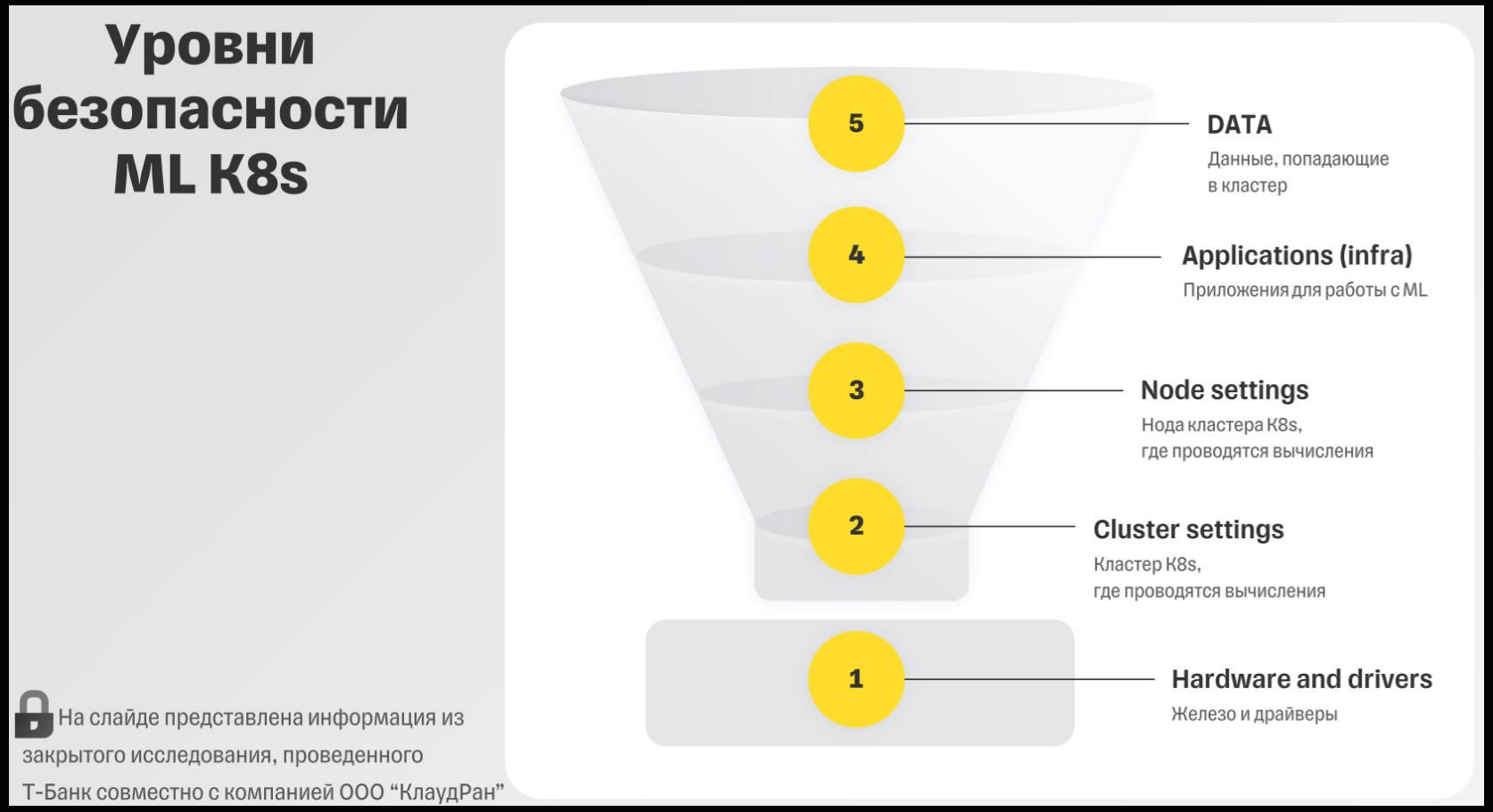
- Вышло 3 CVE
  - CVE-2025-31133
  - CVE-2025-52881
  - CVE-2025-52565
- Все из них дают побег из контейнера





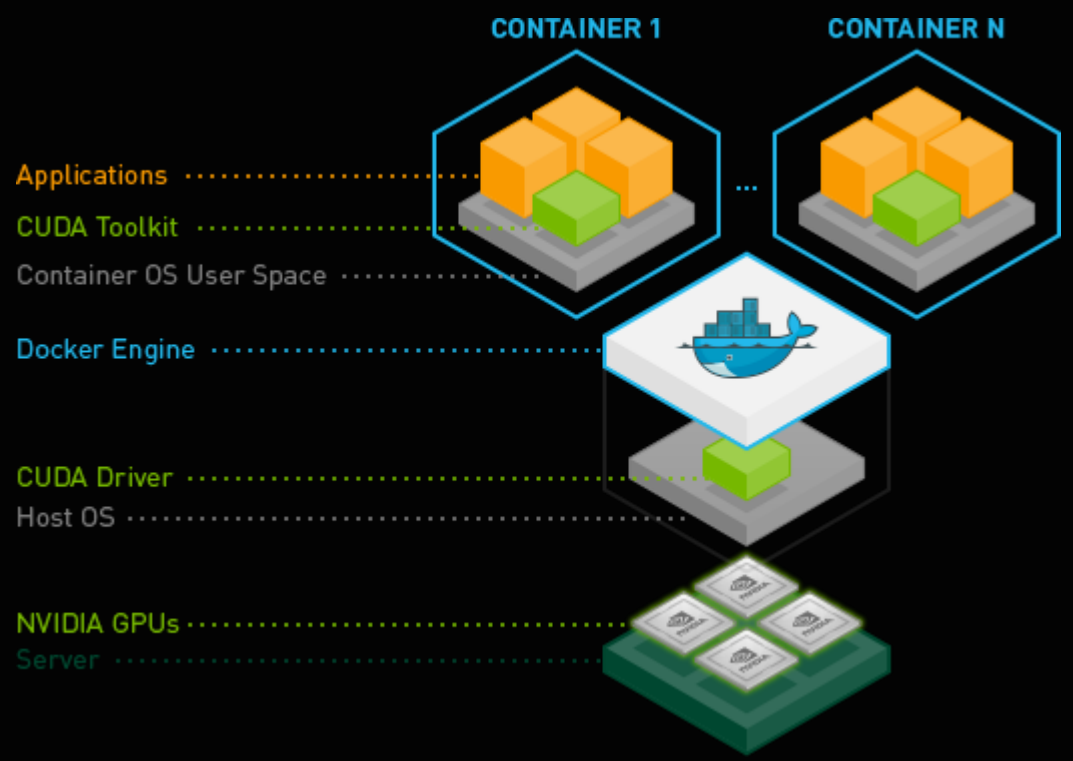
Безопасность AI/ML кластеров

- 100% основной тренд 2025 года!



Уязвимости в NVIDIA Container Toolkit

- NVIDIA Container Toolkit:
  - CVE-2025-23359
  - CVE-2025-23266
  - CVE-2024-0132
- NVIDIA CUDA driver:
  - CVE-2025-23282
  - CVE-2025-23332

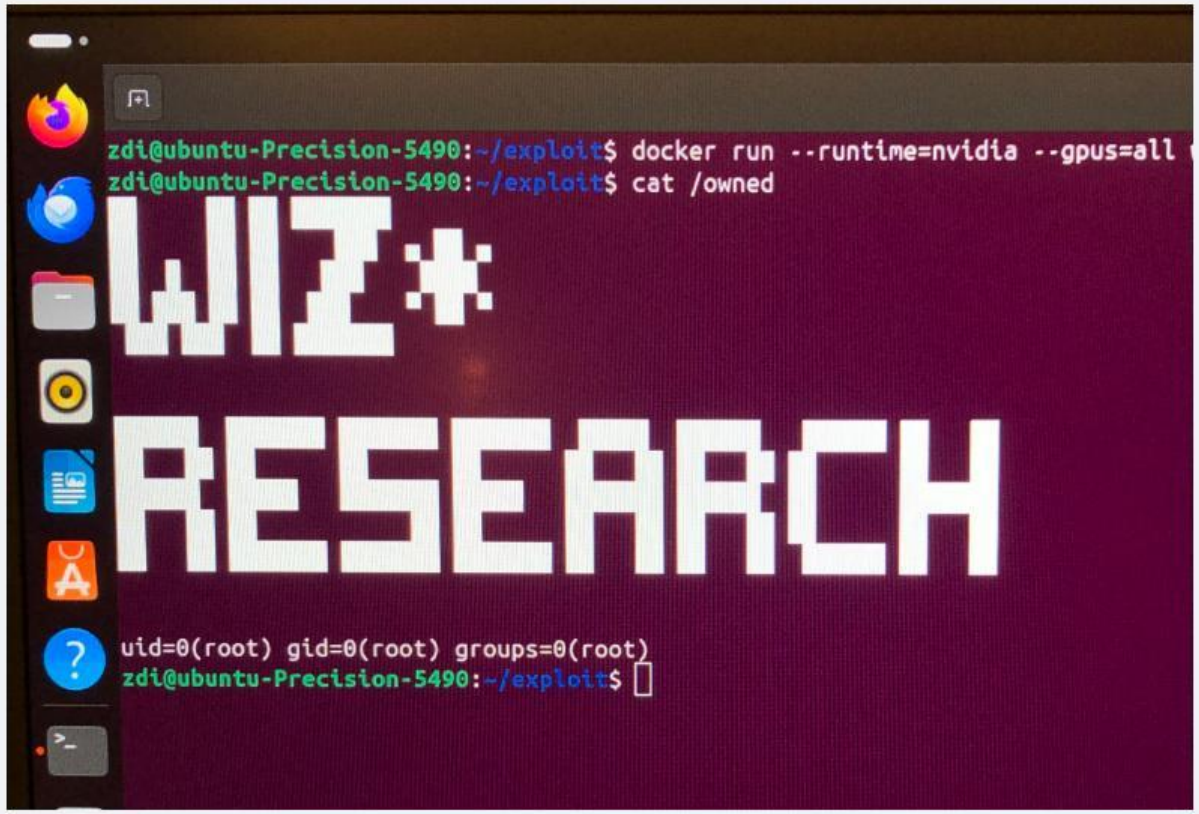


LUNTRY

Pwn2Own

- Chroma
- Postgres pgvector
- Redis
- Ollama
- NVIDIA Triton Inference Server
- NVIDIA Container Toolkit

SUCCESS - Nir Ohfeld (@nirohfeld) Shir Tamari (@shirtamari) of Wiz Research used a External Initialization of Trusted Variables bug to exploit the #NVIDIA Container Toolkit. This unique bug earns them $30,000 and 3 Master of Pwn points.



LUNTRY

Zeroday Cloud

- Kubernetes
- Docker
- Containerd
- Grafana
- GitLab CE
- NVIDIA Container Toolkit
- PostgreSQL

LUNTRY

0/0,5 day в Kubernetes

- Демонстрировали в рамках секретного доклада на БеКон 2025

LUNTRY

LUNTRY

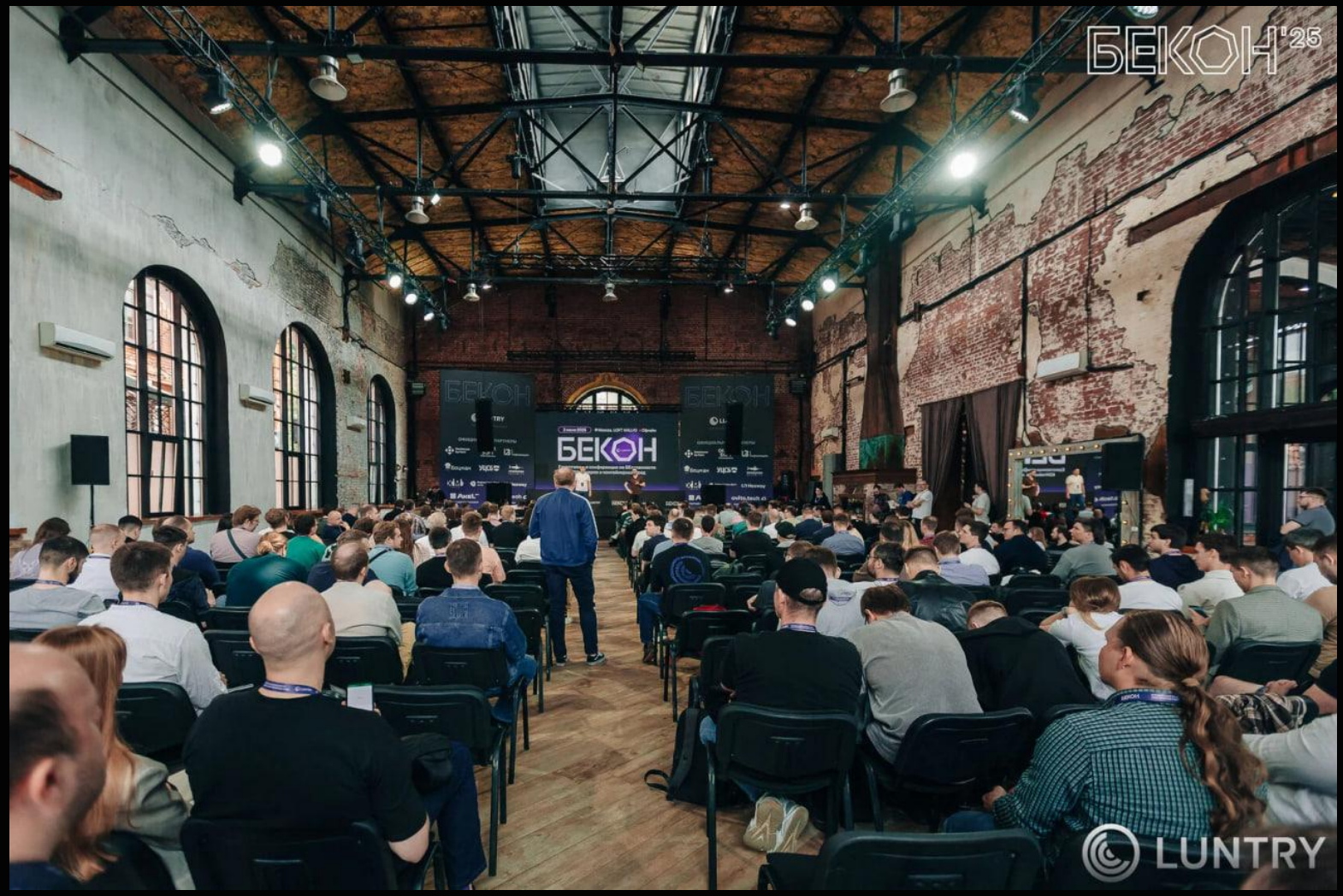
LUNTRY B 2025

Канал k8s (in)security развивается!

LUNTRY

БеКон 2025

- Прошла 3-я конференция
- 2026 будет 4-я!



LUNTRY

Решение Luntry

- 2 крупных релиза
  - До конца года должен выйти 3-й
    - Новая и улучшенная функциональность:
      - Приоритезация уязвимостей
      - Поддержка российских ОС и БДУ ФСТЭК
      - Оптимизации сканера образов
      - Гибридный способ детектирования runtime угроз
      - Политики предотвращения на базе eBPF LSM
      - Security Gates для CI, Image registry и Runtime
      - Анализ Kubernetes Audit Log
- Более 15 технических докладов, 10 вебинаров!
- Публикация карты безопасности для контейнерных сред

LUNTRY

LUNTRY

ЧТО ТАМ В 2026?

Выводы

Выводы

LUNTRY

01 В Kubernetes появляется долгожданная и новая функциональность по безопасности

02 В Kubernetes и в его экосистеме проходит больше исследований и как следствие боле находок/уязвимостей/векторов атак

03 AI/ML основной тренд

04 Luntry продолжает активно развиваться и предоставлять новую функциональность и инструменты

LUNTRY

luntry_official
luntrysolution
luntrysolution

luntry.ru
info@luntry.ru

ДМИТРИЙ ЕВДОКИМОВ
Founder & CTO Luntry

de@luntry.ru
Qu3b3c
k8security

СПАСИБО ЗА ВНИМАНИЕ!

С НАСТУПАЮЩИ НОВЫМ ГОДОМ ;)