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»
- Член программного комитета CFP DevOpsConf и HighLoad++

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



LUNTRY

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
- 1.34
- 1.35
  - План 17 декабря





Release	Released	Active Support	Maintenance Support	Latest
1.34	3 months and 3 weeks ago (27 Aug 2025)	Ends in 8 months (27 Aug 2026)	Ends in 10 months (27 Oct 2026)	1.34.3 (09 Dec 2025)
1.33	7 months ago (23 Apr 2025)	Ends in 4 months (28 Apr 2026)	Ends in 6 months (28 Jun 2026)	1.33.7 (09 Dec 2025)
1.32	1 year ago (11 Dec 2024)	Ends in 1 week and 5 days (28 Dec 2025)	Ends in 2 months and 2 weeks (28 Feb 2026)	1.32.10 (11 Nov 2025)
~~1.31~~	1 year and 4 months ago (13 Aug 2024)	Ended 3 months and 2 weeks ago (28 Aug 2025)	Ended 1 month and 2 weeks ago (28 Oct 2025)	~~1.31.14 (11 Nov 2025)~~

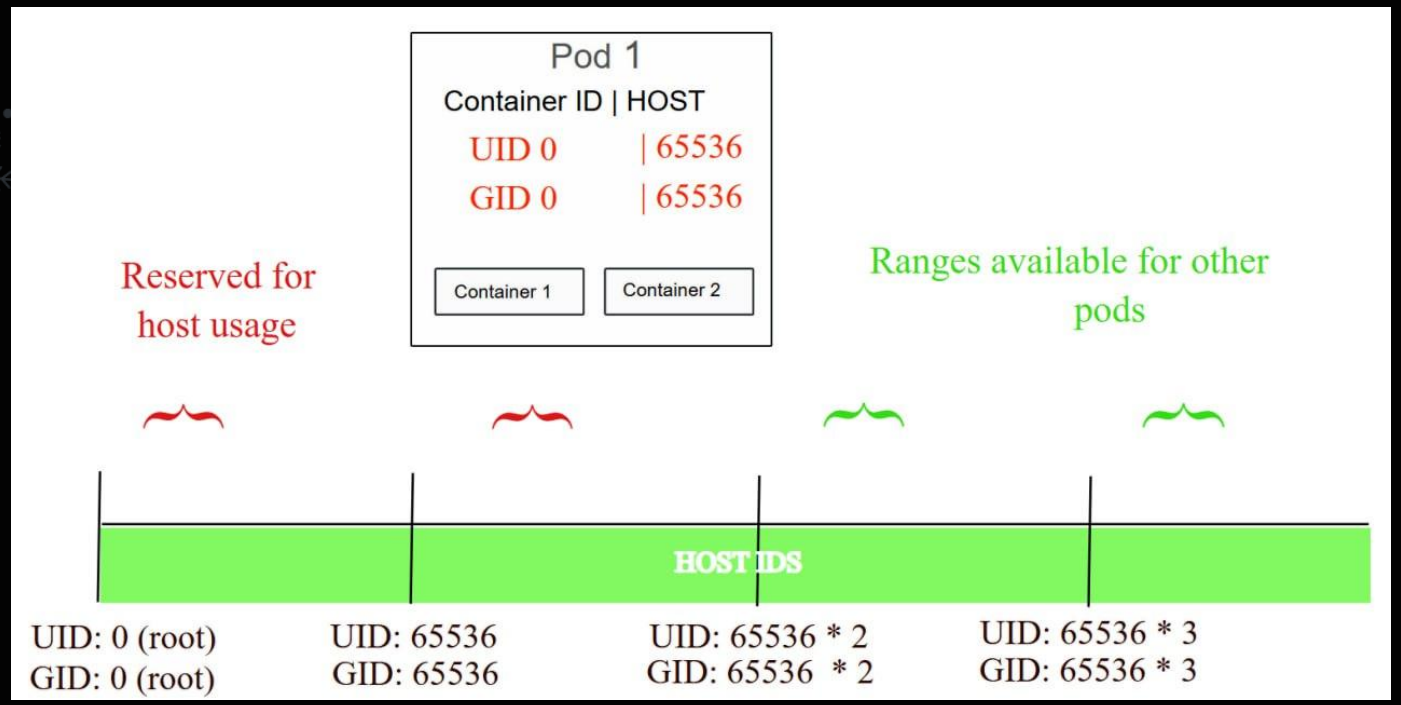
Новые версии CIS

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



User Namespaces в Pods

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



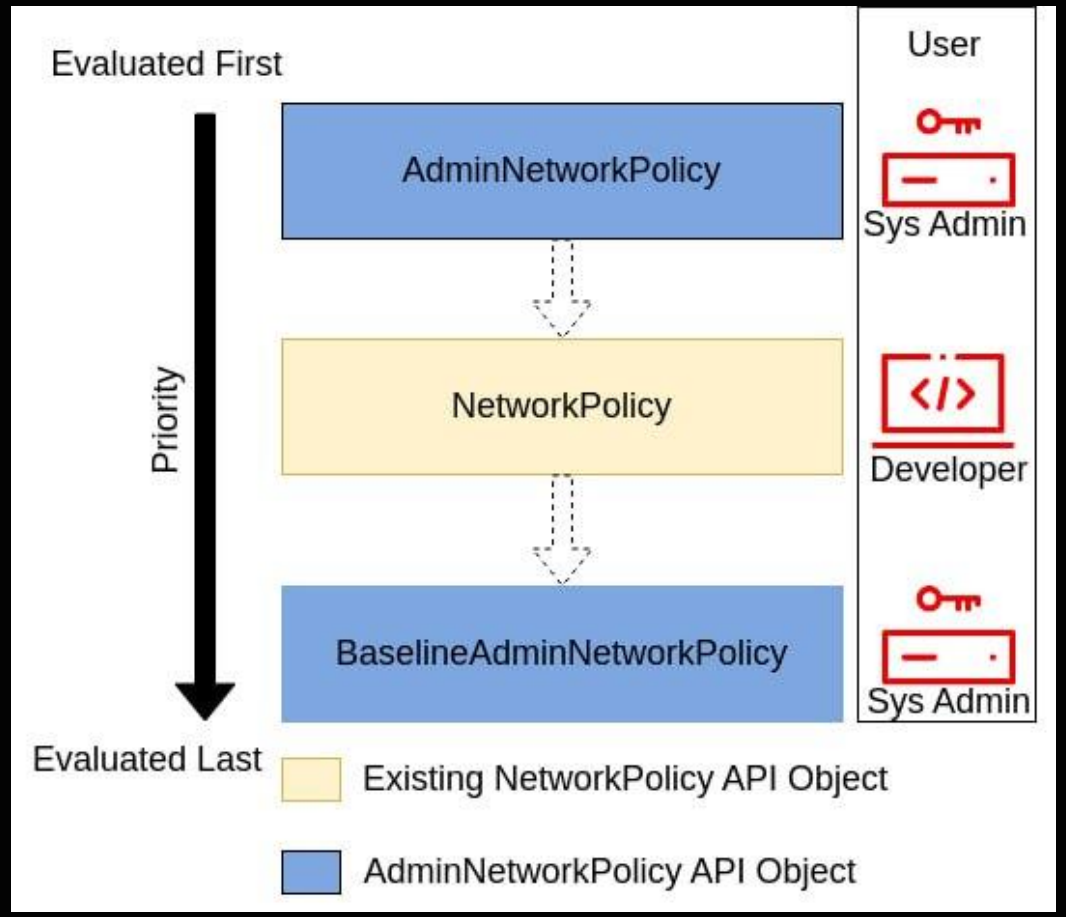

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: userns
spec:
  hostUsers: false
  containers:
  - name: shell
    command: ["sleep", "infinity"]
    image: debian
```

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

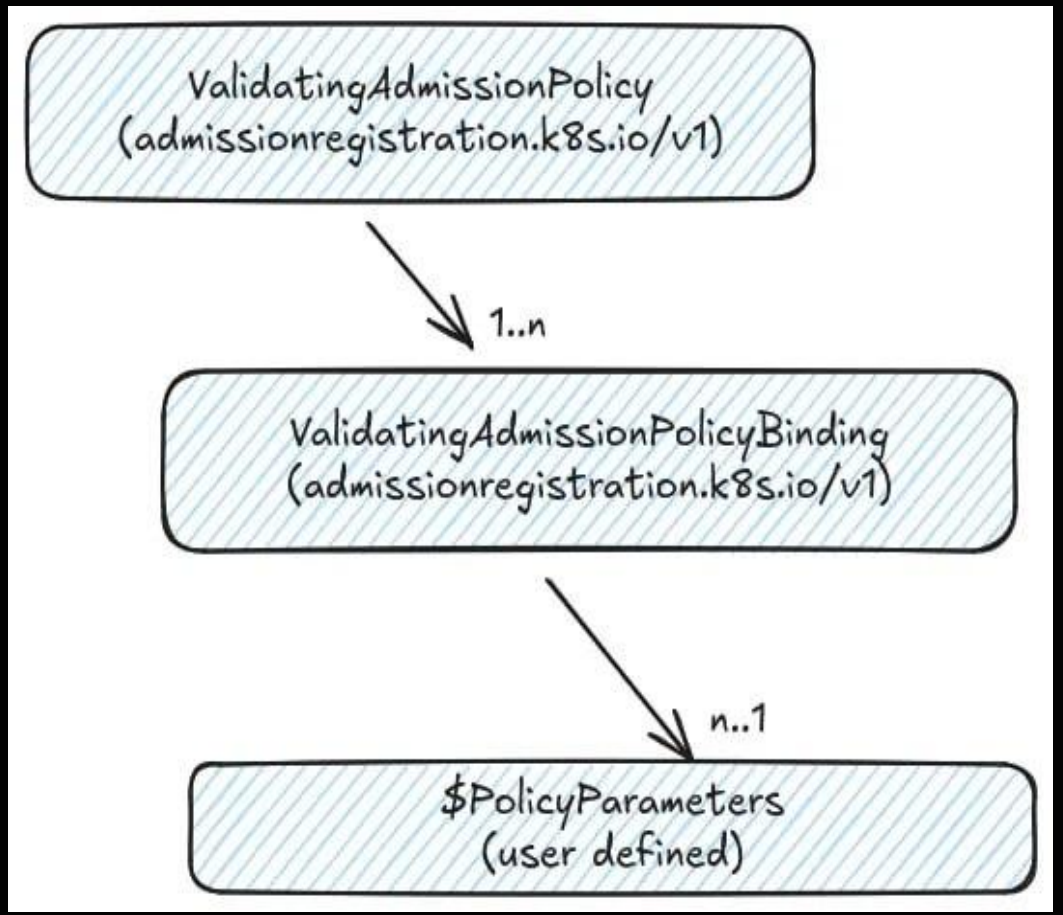
В Cilium пока безрезультатно - обсуждение идет тут



LUNTRY

Validating Admission Policies (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

Драма с Ingress NGINX

LUNTRY

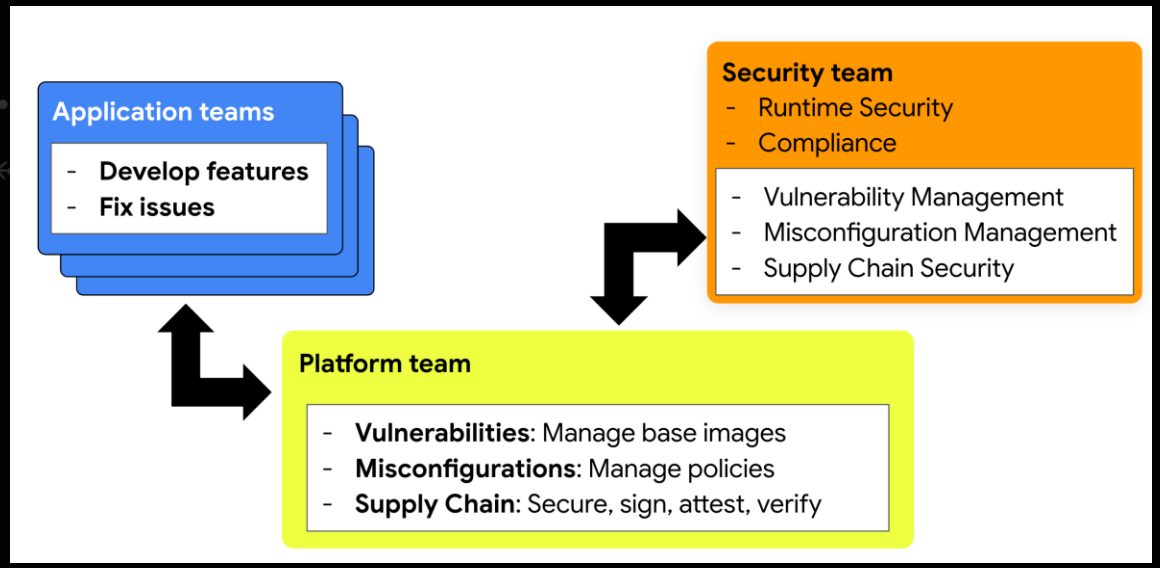
- Проект прекращает своё существование
  - После февраля 2026 года разработка остановятся
  - Ориентир на миграцию к Gateway API
  - “Ingress NGINX Retirement: What You Need to Know”
- Все помнят IngressNightmare, CVE-2024-7646, CVE-2023-5044, CVE-2023-5043, CVE-2022-4886, CVE-2021-25742, …

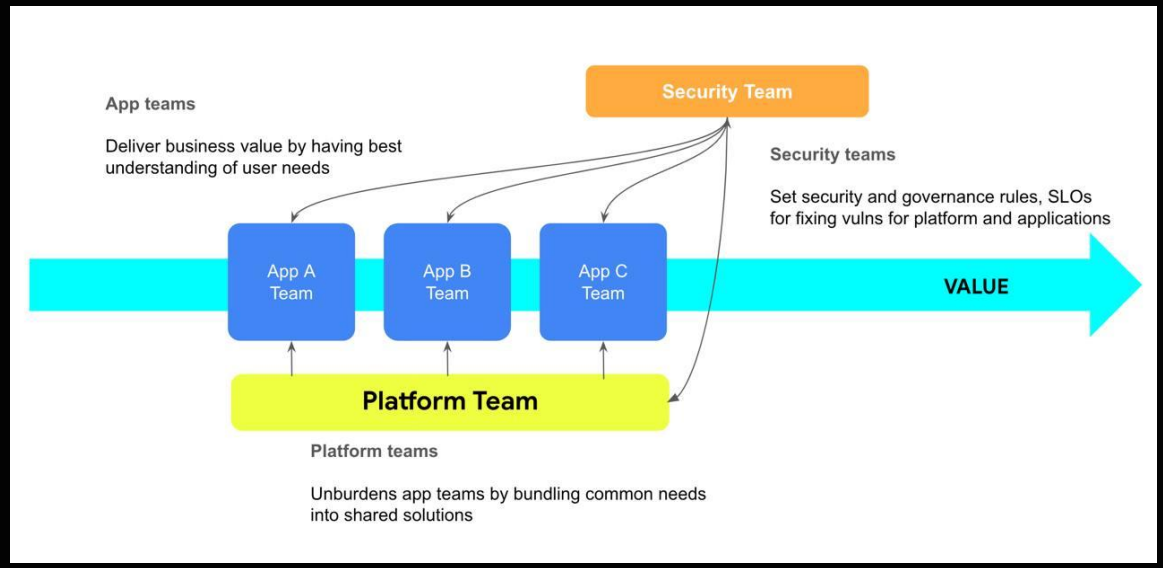
History and Challenges

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.

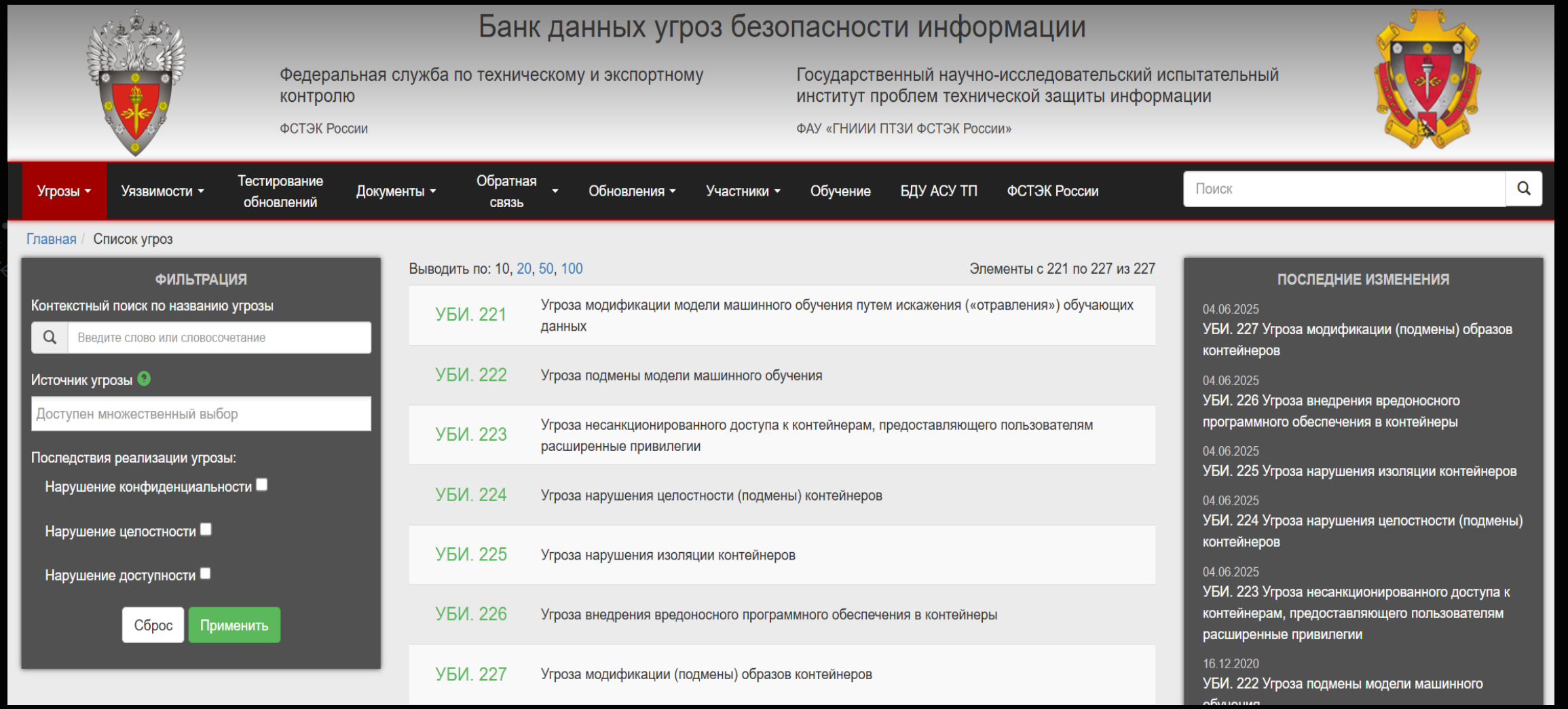
Shift Down Security

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





УБИ по контейнеризации



Сообщество K8s в России растет



https://k8sqday.ru/

KUBER CONF

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

https://aot-kuberconf.ru/

LUNTRY

LUNTRY

УЯЗВИМОСТИ, АТАКИ, ИНЦИДЕНТЫ 2025

Уязвимости Kubernetes за 2025 год

- 13 CVE

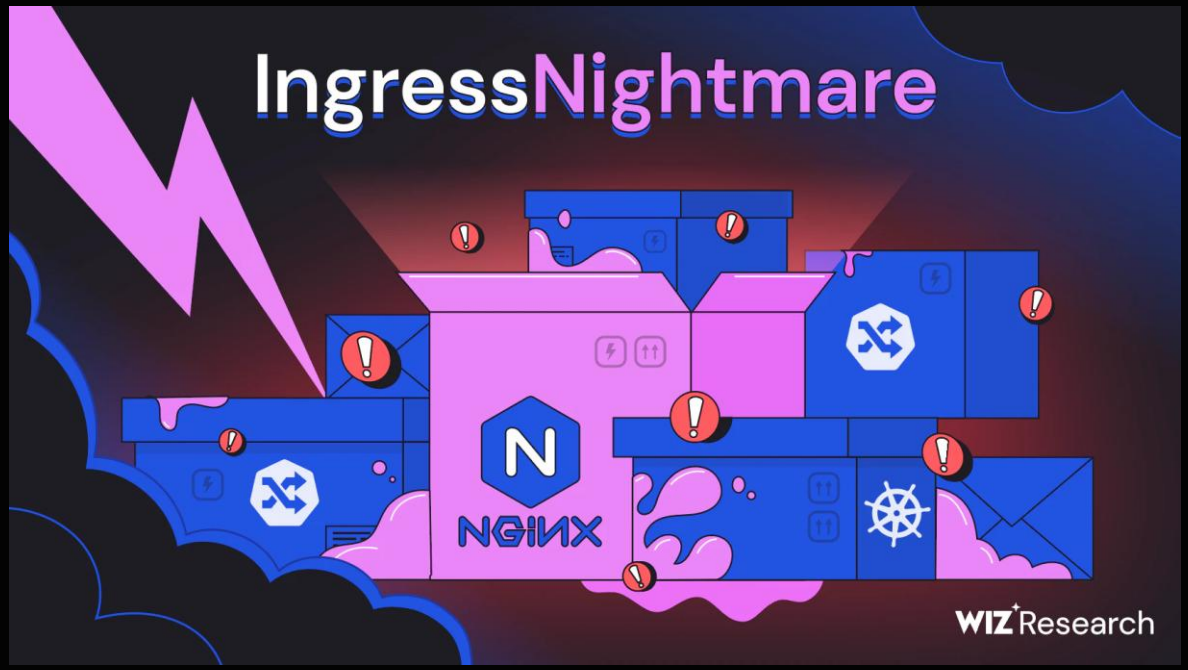
CVE ID	Issue Summary	Issue URL
CVE-2025-13281	Portworx Half-Blind SSRF in kube-controller-manager	#135525
CVE-2025-9708	Kubernetes C# Client: improper certificate validation in custom CA mode may lead to man-in-the-middle attacks	#134063
CVE-2025-7445	secrets-store-sync-controller discloses service account 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

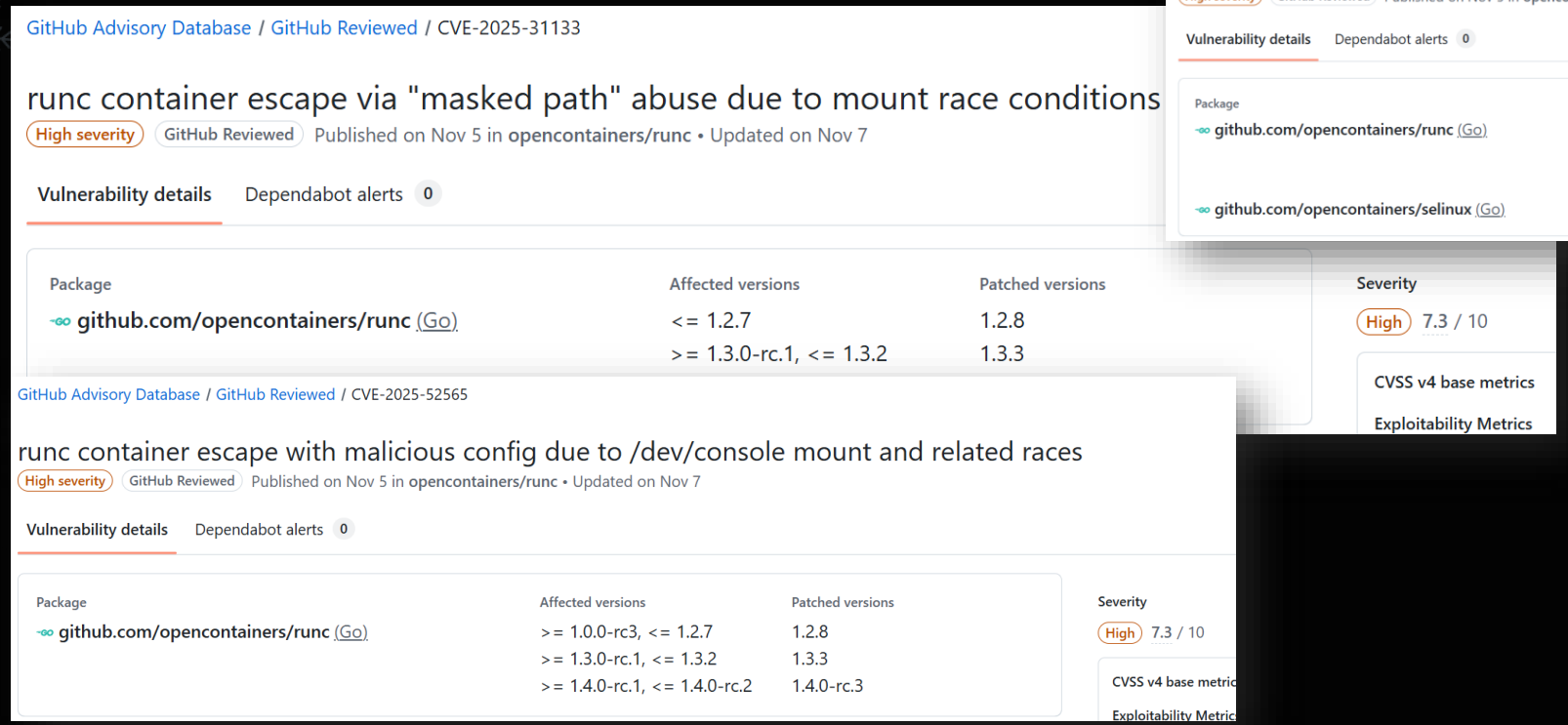
При использовании NetworkPolicy это вообще не проблема ;)

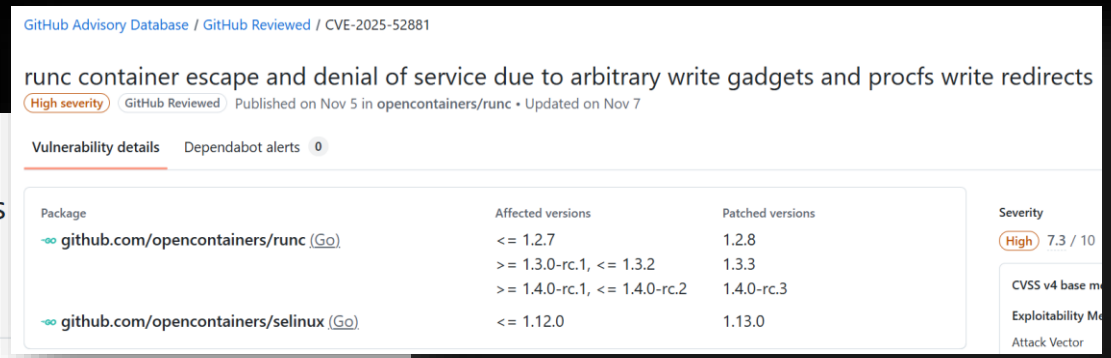


LUNTRY

Уязвимости runc

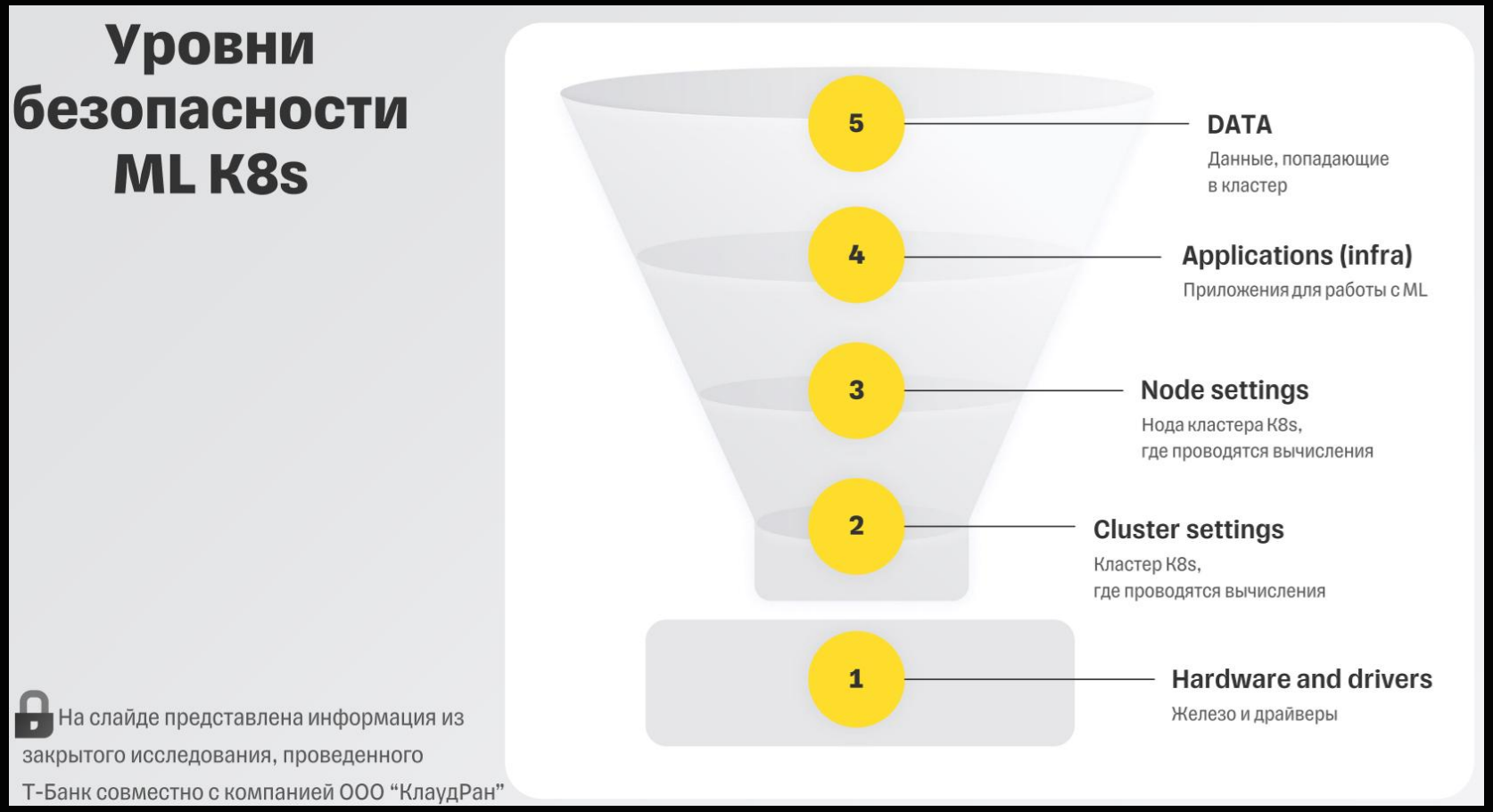
- Вышло 3 CVE
  - CVE-2025-31133
  - CVE-2025-52881
  - CVE-2025-52565
- Все из них дают побег из контейнера





Безопасность AI/ML кластеров

- 100% основной тренд 2025 года!



Уязвимости в NVIDIA Container Toolkit

LUNTRY

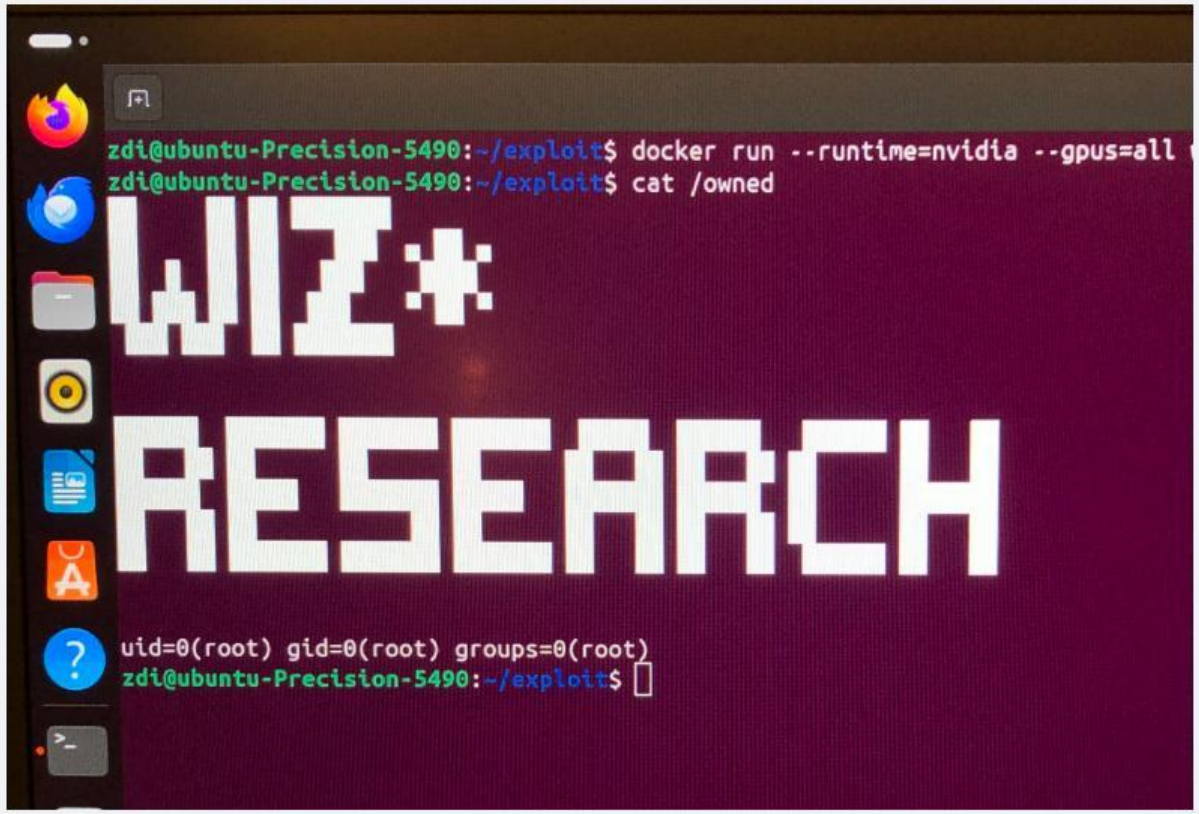
- NVIDIA Container Toolkit:
  - CVE-2025-23359
  - CVE-2025-23266
  - CVE-2024-0132

- NVIDIA CUDA driver:
  - CVE-2025-23282
  - CVE-2025-23332

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.



Zeroday Cloud

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



LUNTRY

LUNTRY

LUNTRY B 2025

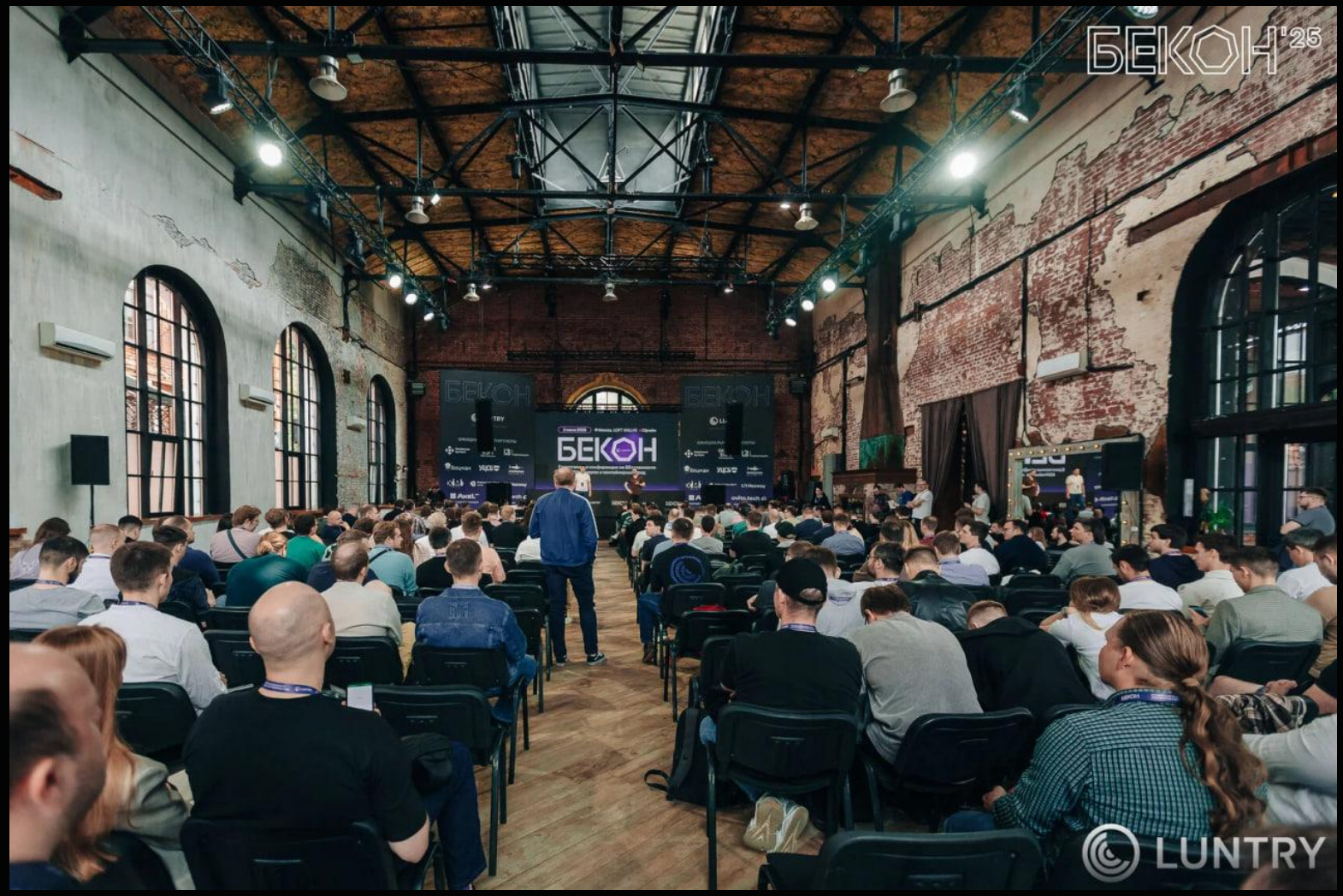
Канал k8s (in)security развивается!



LUNTRY

БеКон 2025

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



LUNTRY

???

- ???

LUNTRY

LUNTRY

ЧТО ТАМ В 2026?



Выводы

Выводы

01 ???

02 ???

03 ???

04 ???

LUNTRY

luntry_official
luntrysolution
luntrysolution

luntry.ru
info@luntry.ru



ДМИТРИЙ ЕВДОКИМОВ
Founder & CTO Luntry

de@luntry.ru
Qu3b3c
k8security

СПАСИБО ЗА ВНИМАНИЕ!

С НАСТУПАЮЩИМ НОВЫМ ГОДОМ ;)