LUNTRY

РЕАКТИВНАЯ БЕЗОПАСНОСТЬ НЕ УСПЕВАЕТ: КАК МЕНЯЕТСЯ ЗАЩИТА В ЭПОХУ AI

Дмитрий Евдокимов

Основатель
и технический
директор Luntry

Проактивный и реактивный подходы к безопасности

ПРОАКТИВНЫЙ

До обнаружения угрозы

Делает бесполезным или чрезвычайно трудным для использования уязвимости, как известные, так и не известные уязвимости

РЕАКТИВНЫЙ

После обнаружения угрозы

Закрывает уязвимость после выпуска информации о ней

КУЛЬТУРА КИБЕРУСТОЙЧИВОСТИ:

«При построении культуры киберустойчивости роль службы безопасности заключается не в предотвращении всех инцидентов, а в предотвращении негативного влияния инцидента безопасности на бизнес».

Уязвимости

≠

уязвимый

Сегодняшние реалии

NIST

Search NIST

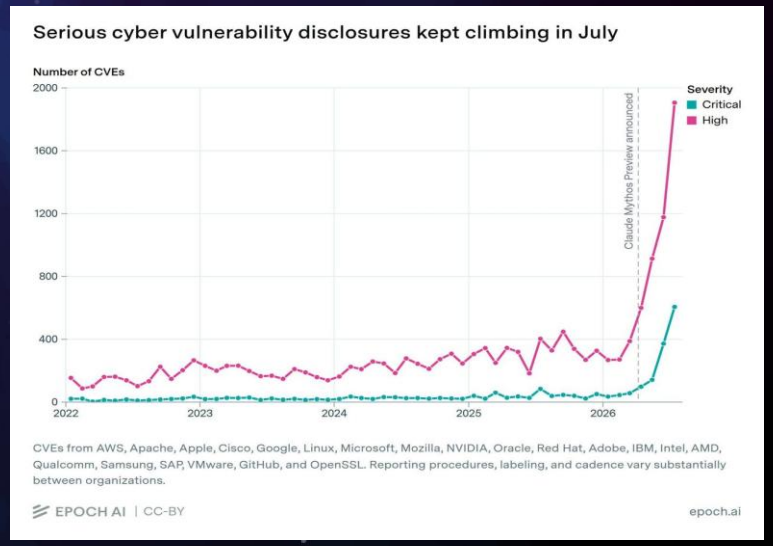
Menu

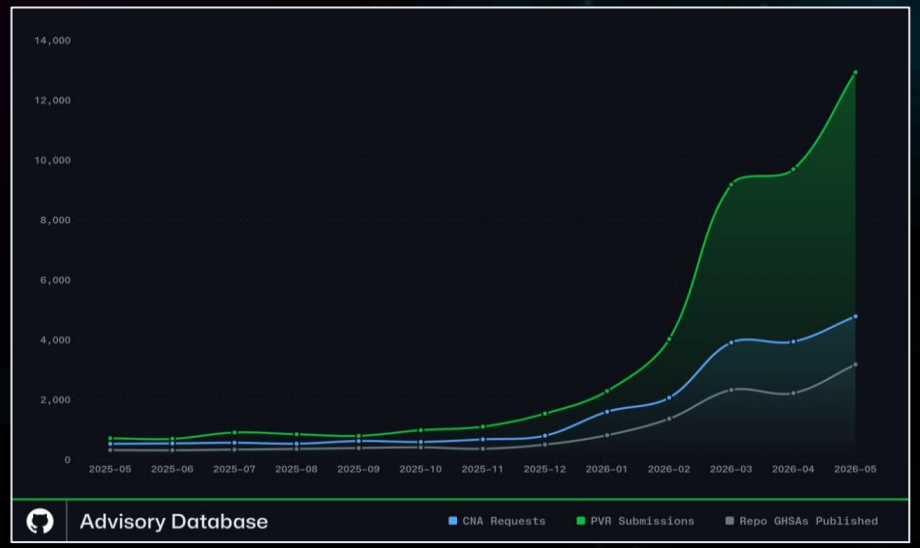
UPDATES

NIST Updates NVD Operations to Address Record CVE Growth

New risk-based model will allow NIST to manage current CVE volume while modernizing the NVD for long-term sustainability.

April 15, 2026





00:00

International Cyber Digest @IntCyberDigest

X.com

‼️ Pwn2Own Berlin 2026 just hit a wall. For the first time in 19-years, ZDI rejected dozens of working zero-day RCE submissions because organizers ran out of contest slots.

Rejected hackers are now going public with PoC demos and direct vendor disclosures, breaking Pwn2Own's usual secrecy.

- AI surfaces a massive wave of 0-day RCEs.
- Submissions overwhelm ZDI past max capacity.
- Slots run out. Researchers with working chains get rejected.
- "Revenge disclosures" begin. ← we are here.

Confirmed casualties so far:
- @xchglabs : 86 vulnerabilities prepared (PyTorch, NVIDIA, Linux KVM, Oracle, Docker, Ollama, Chroma, LiteLLM, llama.cpp). All rejected. Now reporting directly to vendors with writeups dropping as patches land.
- @ggwhyp : full-chain Firefox RCE on Windows. Rejected. Publicly demoed (HTML page → cmd.exe → calc.exe). Responsibly disclosed to Mozilla.
- @yunsu_dev : working RCE chain, rejected. Submitting elsewhere.
- @ryotkak : tried to register for 3+ weeks. ZDI

LUNTRY

Лавина уязвимостей

46 407

новых CVE за 2025 год

+16 % к 2024 · это 127 CVE в день

28 %

новых CVE без полного анализа NVD

официальная статистика уже отстаёт

66-118тыс.

уязвимостей на 2026 год

прогноз

< 4 ч

от находки до эксплойта (2024 год)

было 771 день в 2018 · тренд — минуты

Вывод. Больше CVE ≠ автоматически хуже — иногда это просто лучшее обнаружение. Но скорость эксплуатации и объём потока делают стратегию «найти и закрыть всё быстрее атакующего» физически невыполнимой.

Реактивную модель ломают три асимметрии

LUNTRY

1 Асимметрия времени

Атака — в цикле часов. Защита — недель и месяцев.

- Атакующий: часы
- Патчинг: недели / месяцы
- триаж → согласование → тест → rollout

2 Асимметрия масштаба

Нужен один рабочий путь против всего ландшафта.

- Атакующему нужен 1 путь
- Защитнику — все инфраструктуры, окружения, зависимости, конфиги, legacy части, …

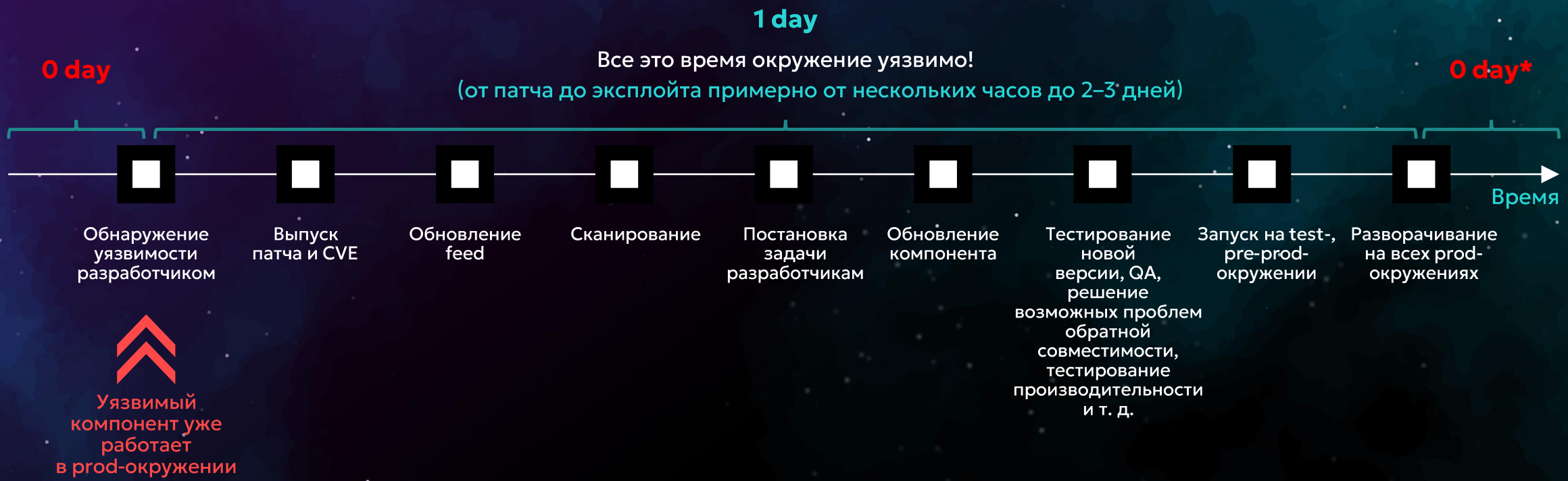
3 Асимметрия стоимости

AI резко удешевляет одну попытку атаки.

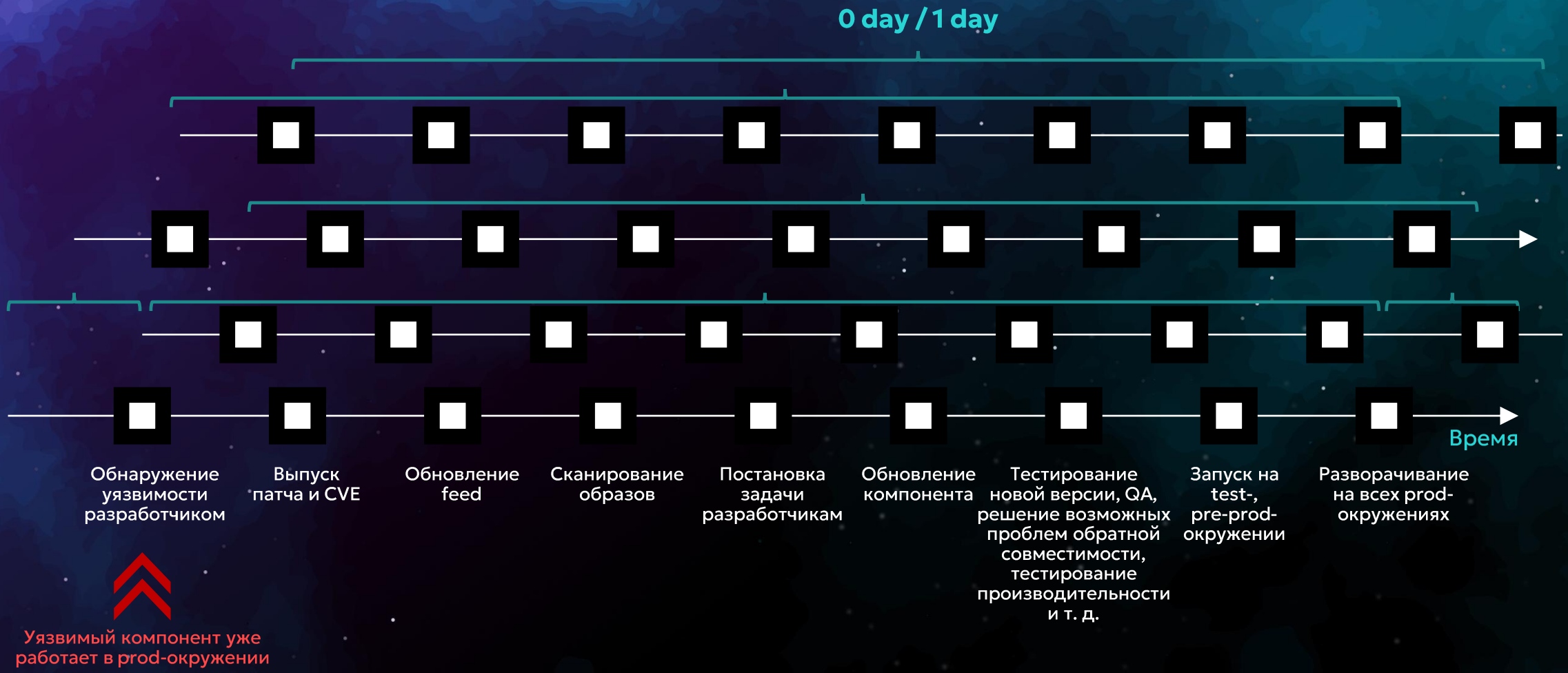
- может и один оператор, а не команда
- дешевле масштабировать
- понятная монетизация

Найти и закрыть все уязвимости быстрее атакующего — уже нельзя. Скорости больше не сопоставимы.

Патчинг остаётся обязательным, но не выигрывает гонку



Реальная ситуация



- **Патчинг — гигиена. Но он слишком медленный, чтобы быть единственной стратегией.**

CVE, сканеры, SBOM, патчи — на спаде

Включаются ПОСЛЕ появления дефекта

Дефект в коде / дизайне

↓

CVE / disclosure

↓

NVD / enrichment

↓

Scanner / VM

↓

SBOM / зависимости

↓

Patch / IR

Что дают

- видимость
- инвентаризацию
- приоритизацию
- реакцию
- ускорение расследования

Чего НЕ дают

- не снижают эксплуатируемость
- не уменьшают поверхность атаки
- не устраняют 0-day
- не ограничивают blast radius
- не исправляют архитектуру

Прозрачность ≠ устойчивость. Реактивные механизмы помогают понять проблему, проактивные — пережить её.

SBOM — это радар, а не броня

«Из чего собрано?»

Инструмент прозрачности

- зависимости, версии, компоненты
- supply-chain видимость
- поиск известных уязвимых библиотек
- ускорение расследования (triage)
- связка с VEX улучшает решения

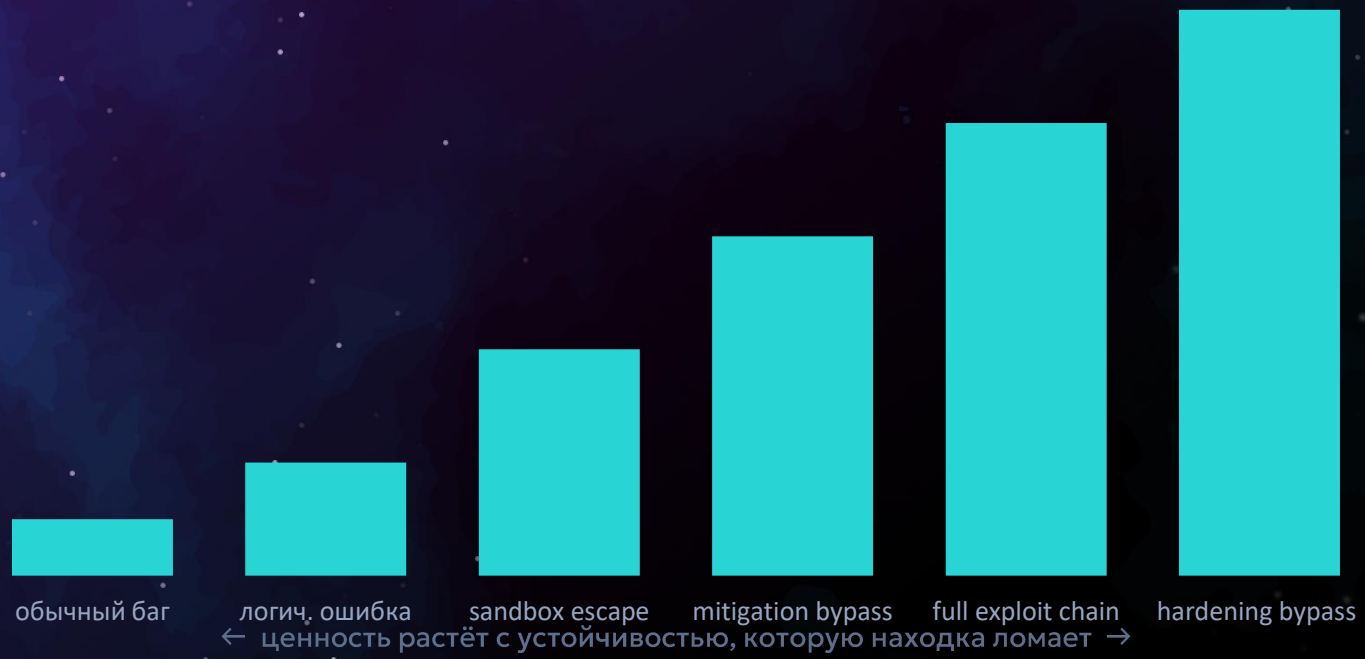
«Насколько трудно взломать?»

На это SBOM не отвечает

- не закрывает 0-day
- не чинит собственный код
- не уменьшает поверхность атаки
- не изолирует процесс, не режет привилегии
- не защищает от bypass архитектуры

SBOM отвечает «из чего собрано?», но не «насколько трудно это взломать?». Радар не заменяет броню.

Рынок уже платит за обход защиты, а не за отдельный баг



Apple · Google · Microsoft

- Apple: топ-награда удвоена до $2 млн (+бонусы до $5 млн) за обход Lockdown Mode
- Google и Microsoft повышают выплаты за bypass и exploit chain
- Ценят sandbox escape, mitigation/hardening bypass, full-chain — не «ещё один баг»

Такие находки проверяют не баг, а стойкость всей архитектуры.

AI ускоряет атаку и перегружает защиту

LUNTRY

Offensive AI

- поиск сигналов, triage
- fuzzing / reverse engineering
- прототипы exploit-цепочек
- быстрая адаптация под цель

AI-assisted development

- больше кода и «glue code»
- больше вариаций одной логики → variant explosion
- 45 % AI-кода содержит уязвимости (OWASP Top-10)
- меньше глубина понимания кода

Больше кода + больше вариативности + та же ёмкость review = больше риска

Индустрия уже проходила этот перелом не раз

LUNTRY

Антивирусы

Было: лечить заражённые файлы

Стало: изоляция, EDR

Браузеры

Было: бесконечно патчить плагины / Flash

Стало: убрать класс риска, sandboxing

AppSec

Было: фильтрация, WAF против SQLi / XSS

Стало: prepared statements, auto-escaping, CSP

Аутентификация

Было: сложные пароли + обучение

Стало: MFA, phishing-resistant, passkeys

Когда реакция перестаёт масштабироваться — защита уходит в архитектуру и безопасные дефолты.

С vulnerability management происходит тот же сдвиг

LUNTRY

Реактивное ядро

Раньше: найти и закрыть

- CVE
- triage
- сканирование
- приоритизация
- patching
- backlog remediation

Сдвиг

Проактивное ядро

Теперь: заранее снизить эксплуатируемость и ущерб

- hardening, secure-by-default
- attack surface reduction
- sandboxing / isolation
- least privilege
- memory safety
- blast radius reduction, policy-as-code

Реактивные меры остаются обязательными, но перестают быть стратегией.

Проактивная защита дешевле постоянного реагирования

LUNTRY

Реагирование после факта

- экстренный triage, forensic
- простой сервисов, переработки
- юр. и регуляторные риски
- коммуникации, потеря доверия
- штрафы, репутационный ущерб

Дорого, срочно, под давлением

Снижение риска заранее

- hardening baseline, secure configs
- least privilege, segmentation
- sandboxing, secure-by-default
- policy-as-code, контроль зависимостей
- изоляция секретов, blast radius

Планово, управляемо, один раз на класс рисков

Ожидаемый ущерб

вероятность × стоимость инцидента

Харденинг бьёт по обоим множителям:

↓ вероятность успешной эксплуатации

↓ blast radius, если инцидент всё же случился

Проактивная защита — это не доп. статья расходов, а замена непредсказуемых аварий управляемыми инвестициями.

Проактивный подход

1. Secure design
2. Hardening baseline
3. Least privilege
4. Isolation / sandboxing
5. Memory safety
6. Blast radius reduction

ЦЕЛЬ

Даже если баг есть — он не должен автоматически становиться инцидентом

Сделать эксплуатацию дорогой, ненадёжной и малорезультативной — для целого класса атак.

LUNTRY

Наша специфика

LUNTRY

Что уже есть

- ГОСТ Р 56939-2024 — безопасная разработка ПО
- Приказ ФСТЭК N° 117 (с 01.03.2026) — защита ГИС
- Приказ ФСТЭК N° 118 — защита средств контейнеризации
- Приказ ФСТЭК N° 21 — меры защиты ПДн
- Приказ ФСТЭК N° 31 — защита АСУ ТП / КВО
- Приказ ФСТЭК N° 239 — значимые объекты КИИ
- ГОСТ Р 57580.1 — для финансового сектора

Задаёт, ЧТО защищать — но не всегда даёт современный hardening baseline

Где пробелы

- Нет единых baseline уровня CIS Benchmarks / STIG
- Нет профилей для cloud / контейнеров / Kubernetes / …
- Нет упора на exploitability и blast radius (только на соответствие)
- …

Описано «что должно быть защищено», слабее — «как именно harden-ить современные стеки»

Итог

LUNTRY

Реактивная безопасность — гигиена.
Проактивная безопасность — стратегия.

Не отказываться от реактивных мер, но перестать строить на них всю стратегию.

Проактивная защита - это не дополнительная статья расходов.
Это способ заменить непредсказуемые аварийные расходы управляемыми инвестициями.

LUNTRY

luntry_official
luntrysolution
luntrysolution

luntry.ru
info@luntry.ru

ДМИТРИЙ ЕВДОКИМОВ

Основатель и технический директор Luntry

de@luntry.ru
Qu3b3c
k8security

СПАСИБО ЗА ВНИМАНИЕ!