



NRUNNER

ТВОЙ НАПАРНИК ПО КИБЕРРАЗВЕДКЕ

Презентация для руководителей бизнеса и ИБ



ПОЧЕМУ МЕДЛЕННОЕ СКАНИРОВАНИЕ БЫСТРО ТЕРЯЕТ СМЫСЛ?

Команды ИБ тонут в рутине проверки ложных срабатываний, а реальные угрозы остаются незамеченными.



ВРЕМЯ — ЭТО ОКНО АТАКИ

Пока отчёт готовится днями, уязвимость уже может быть эксплуатирована. Команда реагирует на вчерашние данные.



БЮДЖЕТ УХОДИТ НА ШУМ

Аналитики часами разбирают ложные срабатывания вместо того, чтобы закрывать реальные риски для бизнеса.



РУЧНОЙ ТРУД = ОШИБКИ

Сопоставление с реестрами и приоритизация вручную — это медленно и зависит от конкретного человека в команде.

РЕШЕНИЕ

NRUNNER

Сканер, который сочетает скорость и точность —
главные ускорители команды ИБ

435K

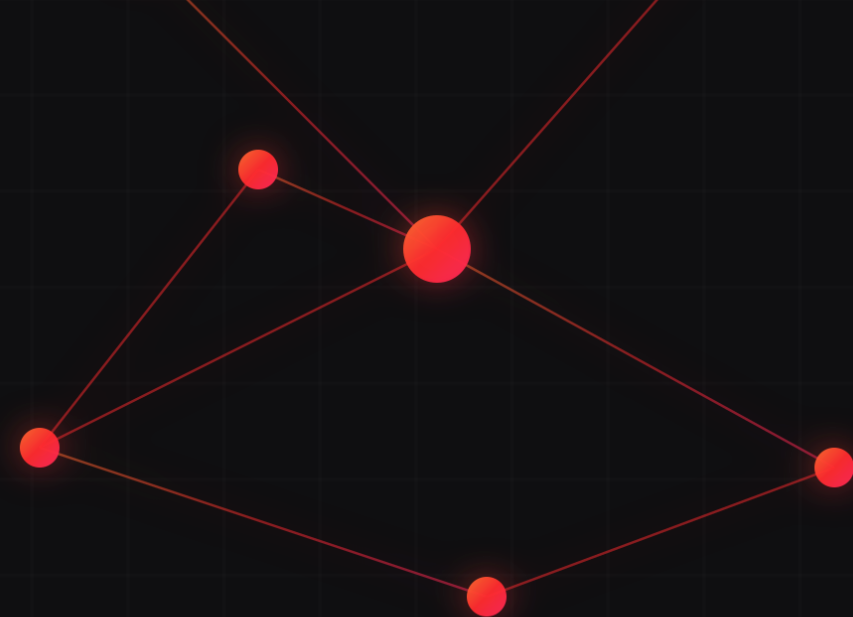
уязвимостей
в базе

EPSS

приоритет
по риску

RU

рекомендации на
русском



Реестр ПО РФ

Реестровая запись №31232 от 15.12.2025



Сертифицированные ОС

Полная поддержка Astra Linux, Альт СП и РЕД ОС



Закрытые контуры

Работает без доступа в Интернет — критично для госзаказчиков и КИИ



ЧТО ВЫ ПОЛУЧАЕТЕ



x5 К СКОРОСТИ КОМАНДЫ

Сканирование не тормозит вашу сеть и не мешает бизнесу работать.



ТОЧНОСТЬ СОПОСТАВЛЕНИЙ

База 435 000 уязвимостей (ФСТЭК + CVE). Мы находим только то, что реально угрожает вам.



ВИДИМОСТЬ 360°

Интерактивная карта сети показывает каждый хост в инфраструктуре — даже те, о которых забыли.

СКАНИРОВАНИЕ, КОТОРОЕ НЕ ТОРМОЗИТ БИЗНЕС

Каждый узел сети проверяется без лишней нагрузки на инфраструктуру. Результат — точная картина рисков без простоев и жалоб от бизнес-подразделений.

435 000

уязвимостей в базе — ФСТЭК и CVE одновременно

0 простоев бизнес-систем во время сканирования



Интерактивная карта сети — центральный элемент интерфейса NRunner. Даёт мгновенный визуальный срез состояния всей инфраструктуры.

НЕ ПРОСТО НАХОДИМ, А ПРИОРИТИЗИРУЕМ

Встроенный EPSS показывает реальную частоту эксплуатации каждой уязвимости. Вы точно знаете, что чинить прямо сейчас, а что можно запланировать на завтра — включая контроль «нулевого дня».

EPSS — ШКАЛА РИСКА

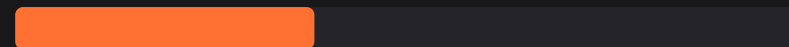
Критично — чинить сейчас 92%



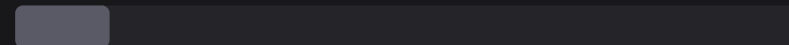
Высокий риск — на этой неделе 64%



Средний — в плановом окне 38%



Низкий — можно отложить 12%



ПРОВЕРКА УСТОЙЧИВОСТИ ПОД НАГРУЗКОЙ DDOS-АТАКИ

Специализированный модуль для анализа поведения инфраструктуры в условиях высокой и экстремальной нагрузки.



Моделирование стресс-сценариев

Симуляция пиковых и аварийных условий работы



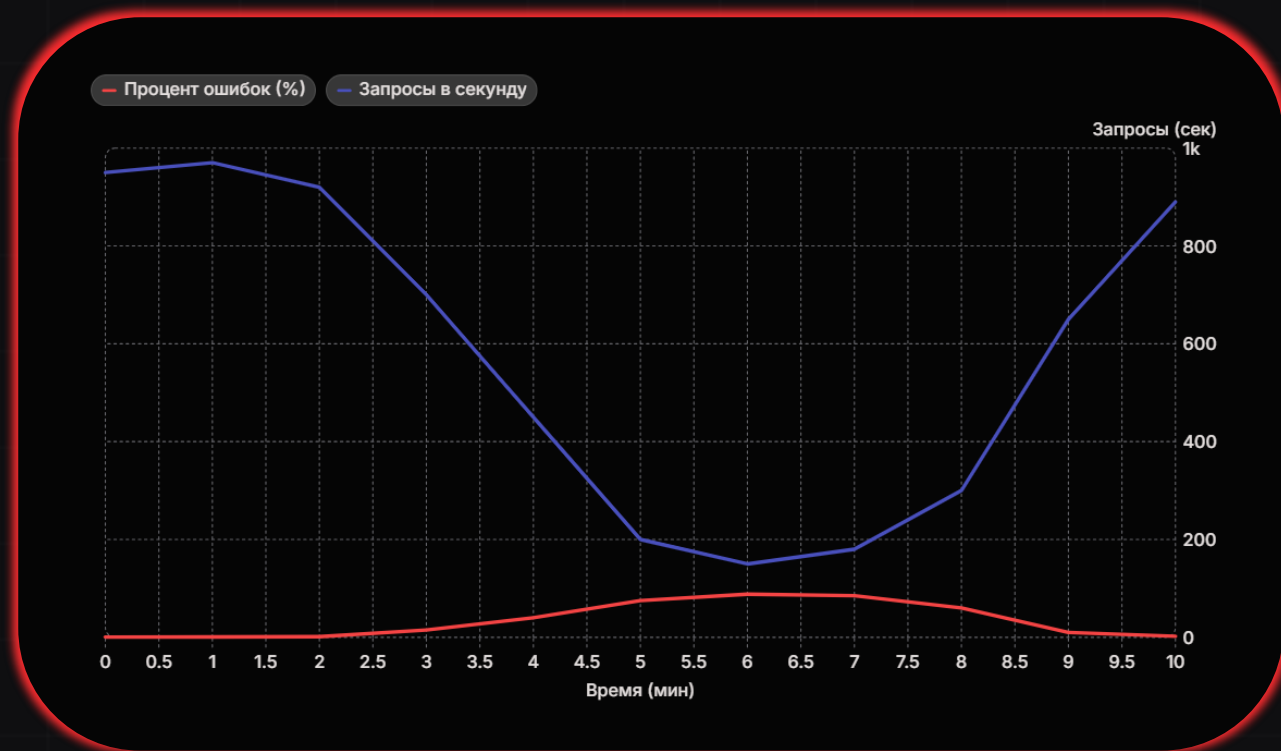
Выявление узких мест

Определение слабых звеньев до инцидента



Оценка отказоустойчивости

Стабильность и надёжность под нагрузкой



Этот график демонстрирует, как наша система ведёт себя под возрастающей нагрузкой DDOS-атаки. Видно резкое падение количества успешно обработанных запросов в секунду и экспоненциальный рост процента ошибок на пике атаки (минуты 5-7), после чего происходит постепенное восстановление показателей по мере снижения воздействия.

БЫЛО / СТАЛО

БЫЛО



Часы ожидания отчёта о сканировании



Ручная проверка ложных срабатываний



Сложно обосновать бюджет на устранение

СТАЛО



Обнаружение уязвимостей быстрее в 5 раз*

* на основании сравнения с отечественными продуктами сканирования уязвимостей



Автоматические рекомендации на русском языке



Прозрачные отчёты, готовые для начала работ

РАСПРЕДЕЛЕННАЯ АРХИТЕКТУРА

Современная распределенная архитектура, позволяющая балансировать нагрузку в инфраструктуре.

Агенты устанавливаются опционально.

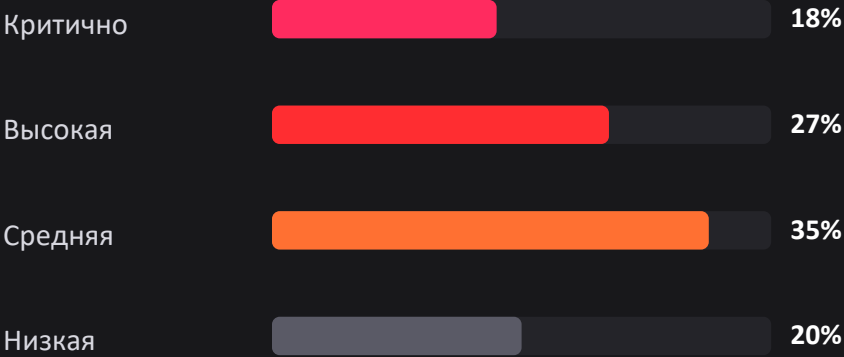


Привычная среда • Работает в закрытых сетях

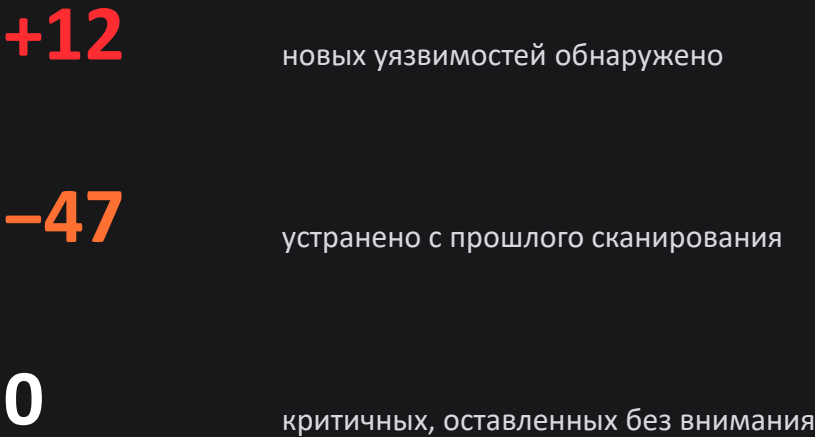
ОТЧЁТ, КОТОРЫЙ ПОНИМАЮТ ВСЕ

Наглядные дашборды, динамика устранения и дифференциальные отчёты — что появилось и что исчезло с прошлой проверки. Отдел ИБ тратит меньше времени на оформление и больше — на защиту.

РАСПРЕДЕЛЕНИЕ ПО КРИТИЧНОСТИ



ИЗМЕНЕНИЯ С ПРОШЛОЙ ПРОВЕРКИ



БЕЗ СКРЫТЫХ ПЛАТЕЖЕЙ И РОСТА ЦЕНЫ ЗА ПОЛЬЗОВАТЕЛЯ

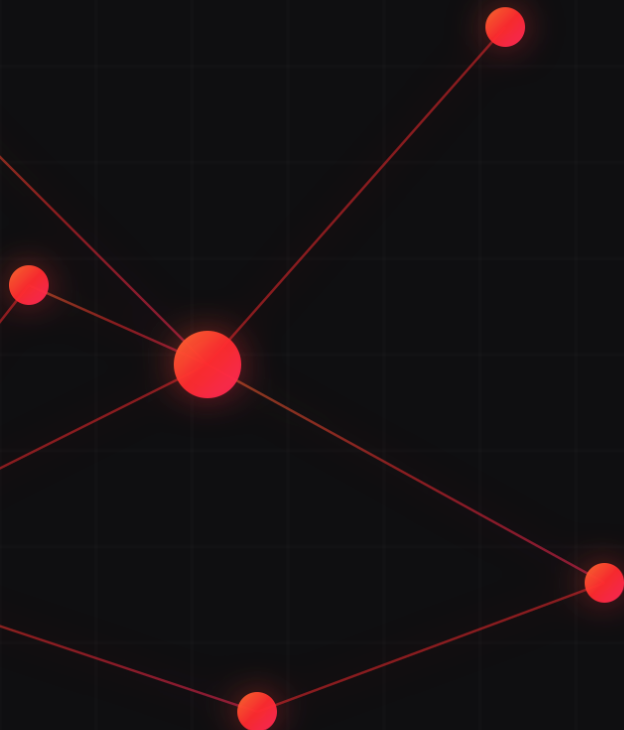
БЕССРОЧНАЯ ЛИЦЕНЗИЯ

- ВМЕСТО ПОДПИСКИ

Вы платите за право использования, техническую поддержку в первый год получаете бесплатно. А со второго года – платите только за техническую поддержку. Право использования остается у вас навсегда.



ЛЕГКИЙ СТАРТ



30 ДНЕЙ

Пробный период, чтобы убедиться в результате на своей инфраструктуре

1 ДЕНЬ

На полное внедрение и первый отчёт о состоянии сети



НАЧНИТЕ ЗАЩИЩАТЬ РЕАЛЬНЫЕ АКТИВЫ УЖЕ СЕГОДНЯ

Покажем NRunner на вашей инфраструктуре в формате демо-доступа.

ЗАКАЗАТЬ ДЕМО-ДОСТУП

<https://legionsecurity.ru/nrunner/> · legion@legionsecurity.ru · +7 (800) 500-64-47