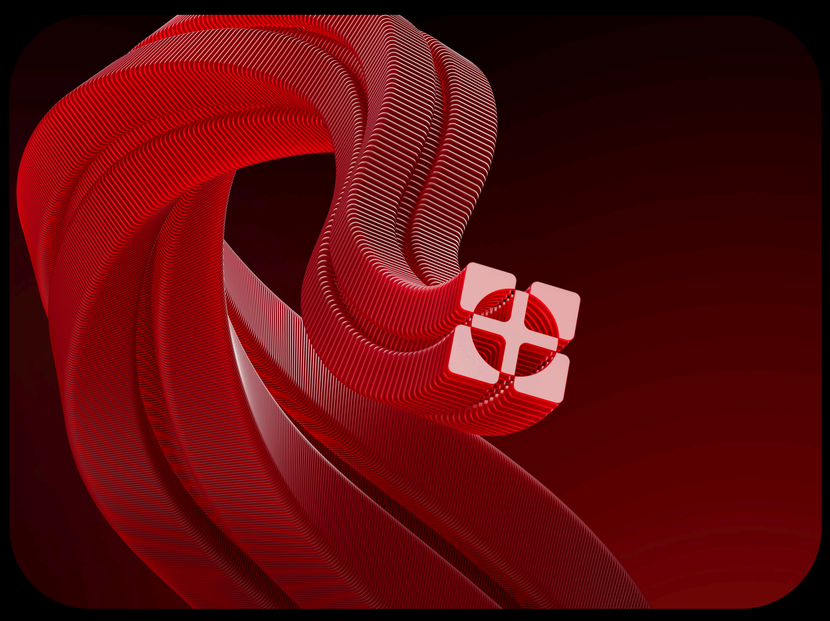
positive technologies

XSpider PRO

Сканер безопасности нового поколения, который покажет полную картину уязвимостей в вашей инфраструктуре

В мире киберугроз каждая уязвимость — потенциальная лазейка для хакера, которую важно вовремя устранить. Может казаться, что в небольших компаниях всё под контролем и риск взлома через уязвимости минимален. Однако стать жертвами кибератак могут даже инфраструктуры с несколькими десятками активов. На первый взгляд проблему могут решить сканеры с открытым исходным кодом, но они не поддерживают российское ПО, оставляя инфраструктуру уязвимой.



Регулярное обнаружение и устранение уязвимостей — это необходимость, а не опция. Но решать эти задачи вручную слишком сложно и затратно.

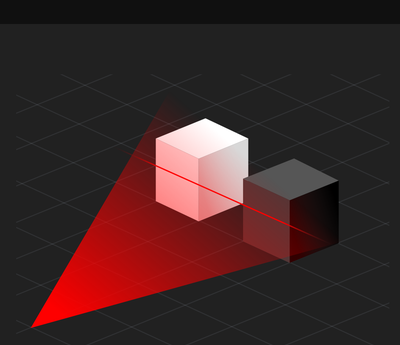
32%
атак

реализуются через эксплуатацию уязвимостей

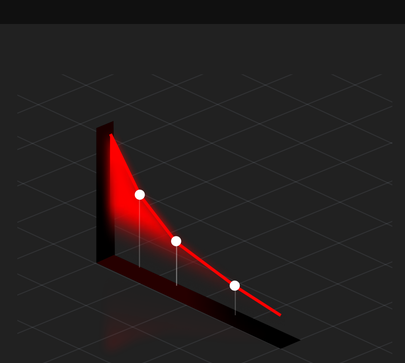
96%
компаний

не защищены от проникновения злоумышленников

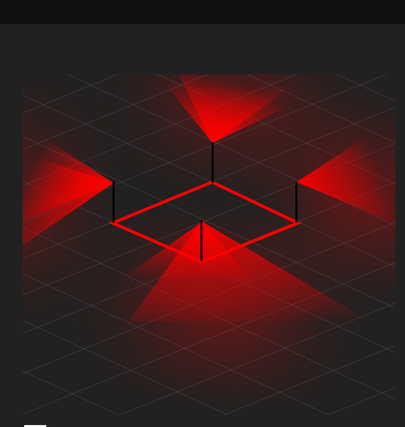
Решение — отечественный сканер уязвимостей XSpider PRO



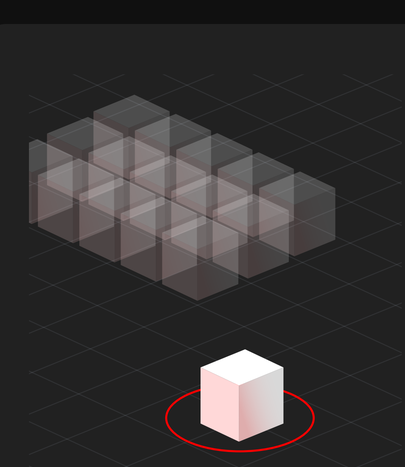
Помогает провести полное сканирование инфраструктуры методами черного и белого ящика



Снижает риск реализации атак с использованием уязвимостей ОС и ПО



Помогает контролировать безопасность внешнего периметра



Идеален для небольших инфраструктур

Сканер поможет

Обнаружить уязвимости в сети и системах

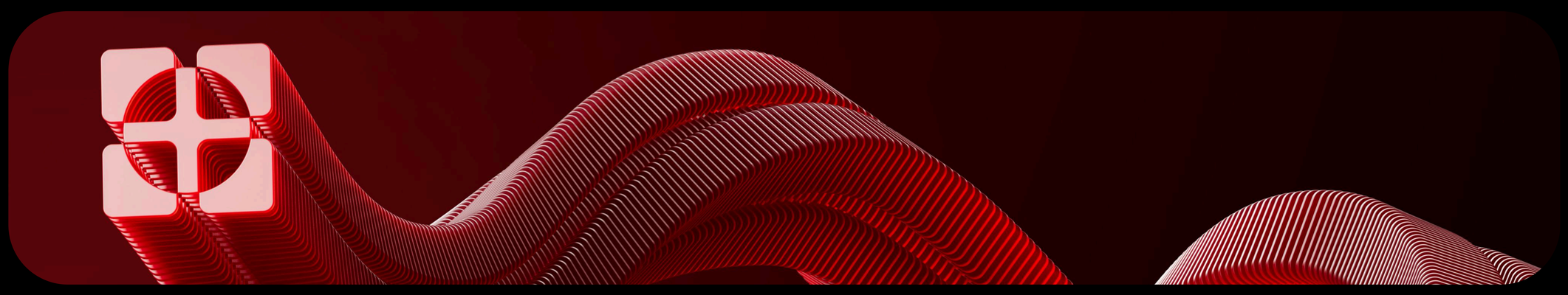
Выявляйте уязвимости на рабочих станциях, серверах и в ОС, сканируйте базы данных, веб-приложения и Docker-контейнеры, чтобы собрать полное представление об инфраструктуре

Вовремя обновить критически важные системы

Выявляйте активы с устаревшими версиями ПО и ОС, следуйте рекомендациям и устанавливайте актуальные патчи

Увидеть полную картину уязвимостей в инфраструктуре

Выгружайте понятный отчет о состоянии инфраструктуры после сканирования и выстраивайте работу с уязвимостями, учитывая их опасность по метрикам CWE и CVSS



Преимущества

Обширная база уязвимостей

Регулярно пополняем базу уязвимостей: БДУ ФСТЭК, CVE, OWASP Top 10, база Positive Technologies. Обнаруживаем уязвимости в том числе и в отечественных ОС и популярном ПО.

Низкие аппаратные требования

Мы сделали «легкий» сканер, чтобы вы могли быстро и эффективно внедрять его в любую инфраструктуру без дополнительных затрат.

Низкий уровень ложных срабатываний

Высокая точность и надежность результатов сканирования позволяют не тратить время на ошибочные срабатывания и сосредоточиться на устранении реальных угроз.

Сканирование Docker-контейнеров и веб-приложений

Проверяет сайты и окружение, в котором они работают, чтобы найти и устранить уязвимости до того, как ими воспользуются злоумышленники.

Работа на отечественных ОС

Сканер полностью адаптирован для работы на российских ОС — можно легко внедрить продукт в импортозамещенную инфраструктуру.

Многоуровневая защита

Продукт может работать в режимах черного и белого ящика, что позволяет оперативно оценить текущее состояние защищенности инфраструктуры.