XSpider

Выяви уязвимости в сетевых ресурсах до того,
как это будет сделано злоумышленниками.

О компании Positive Technologies

18 лет
опыта исследований и разработок

900 сотрудников:
инженеров по ИБ, разработчиков, аналитиков и других специалистов

250 экспертов
в нашем исследовательском центре безопасности

200+
обнаруженных уязвимостей нулевого дня в год

200+
аудитов безопасности корпоративных систем делаем ежегодно

50%
всех уязвимостей в промышленности и телекомах обнаружили наши эксперты

Защищаем крупные информационные системы от киберугроз:

- создаем продукты и решения
- проводим аудиты безопасности
- расследуем инциденты
- исследуем угрозы

Нам доверяют

Наши проекты

2018 МАРТА
ВЫБОРЫ ПРЕЗИДЕНТА РОССИИ

Задача
Усилить защищенность веб-портала ЦИК РФ во время проведения выборов.

Что сделано
Проверили защищенность веб-портала, внедрили PT Application Firewall для выявления и блокировки атак, провели мониторинг безопасности в день выборов.

Результат
Выявлены критичные уязвимости, обеспечена безопасность веб-портала и блокировка атак в режиме реального времени.

FIFA WORLD CUP
RUSSIA
2018

Задача
Обеспечить защиту сервисов, необходимых для перемещения болельщиков, регистрации компаний-перевозчиков и набора волонтеров.

Что сделано
Создали контур безопасности и проводили непрерывный мониторинг защищенности всей инфраструктуры.

Результат
Обеспечено непрерывное функционирование всех информационных систем

ptsecurity.com

phd
Positive Hack Days

Ежегодный международный форум по практической безопасности, который собирает более 6000 участников.

В рамках форума мы организуем 30-часовую кибербитву за контроль над эмуляцией городской инфраструктуры между командами атакующих и защитников. Формат соревнования максимально приближен к реальности.

Во время кибербитвы SOC на базе наших продуктов мониторит инфраструктуру и выявляет атаки.

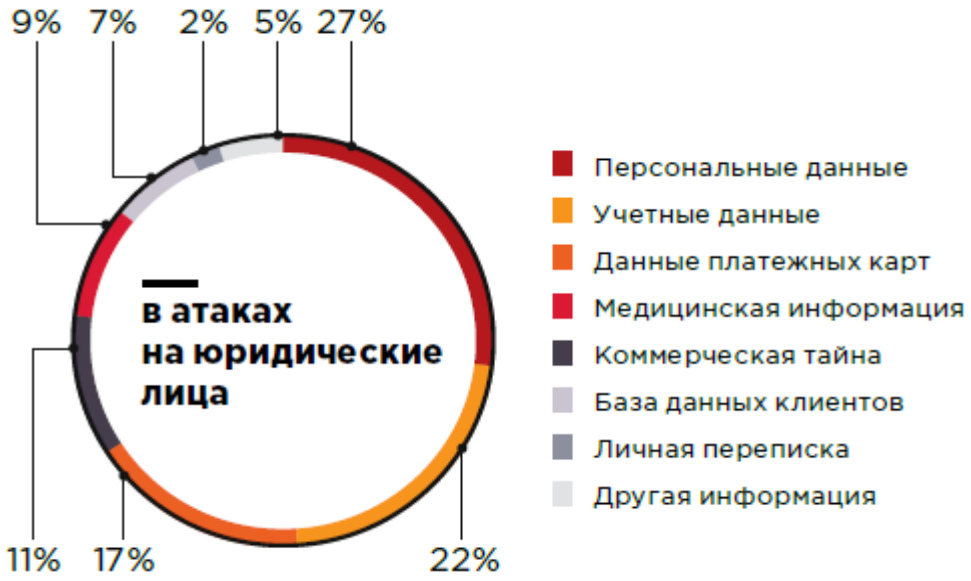
phdays.com

Как вовремя узнать об уязвимостях

и защитить свою компанию

Ландшафт угроз

Какие данные крадут*



Кого атакуют чаще всего*

20% государственный сектор

10% промышленные компании

8% медицинские учреждения

8% сфера образования

8% финансовая отрасль

5% IT-компании

4% сфера услуг

4% торговля

1500+ **Уникальных атак зафиксировали в 2019 году***

* «Актуальные киберугрозы — 2019. Тренды и прогнозы», Positive Technologies

Как злоумышленник может проникнуть в компанию

Вредоносное ПО

В 2019 году число заражений вредоносным ПО выросло на 38% по сравнению с 2018 годом*

Веб-уязвимости

Позволяет получить контроль над веб-приложением, а также провести атаку и на локальную сеть

Подбор учеток

Большинство паролей составлены предсказуемо

Уязвимости в ПО

Использование устаревших версий ПО является серьезным риском

Ошибки в настройках

Злоумышленники используют ошибки, которые допускают администраторы ИС

Социальная инженерия

Применяется для получения информации от клиента/ сотрудника компании или для доставки ВПО в инфраструктуру

* «Актуальные киберугрозы — 2019. Тренды и прогнозы», Positive Technologies

Как защититься

Выявлять и устранять уязвимости

Контролировать безопасность систем

- Своевременно обновлять используемое ПО по мере выхода патчей;
- Контролировать появление небезопасных ресурсов на периметре сети;
- Регулярно проводить инвентаризацию ресурсов, доступных для подключения из интернета.

Защищать данные

- Не допускать использование простых паролей;
- Использовать разные учетные записи и пароли для доступа к различным ресурсам.

Использовать эффективные средства защиты

- Регулярно проводить анализ защищенности инфраструктуры для выявления новых векторов атак и оценки эффективностей мер защиты;
- Автоматизировать процесс выявления уязвимостей.

Наше решение

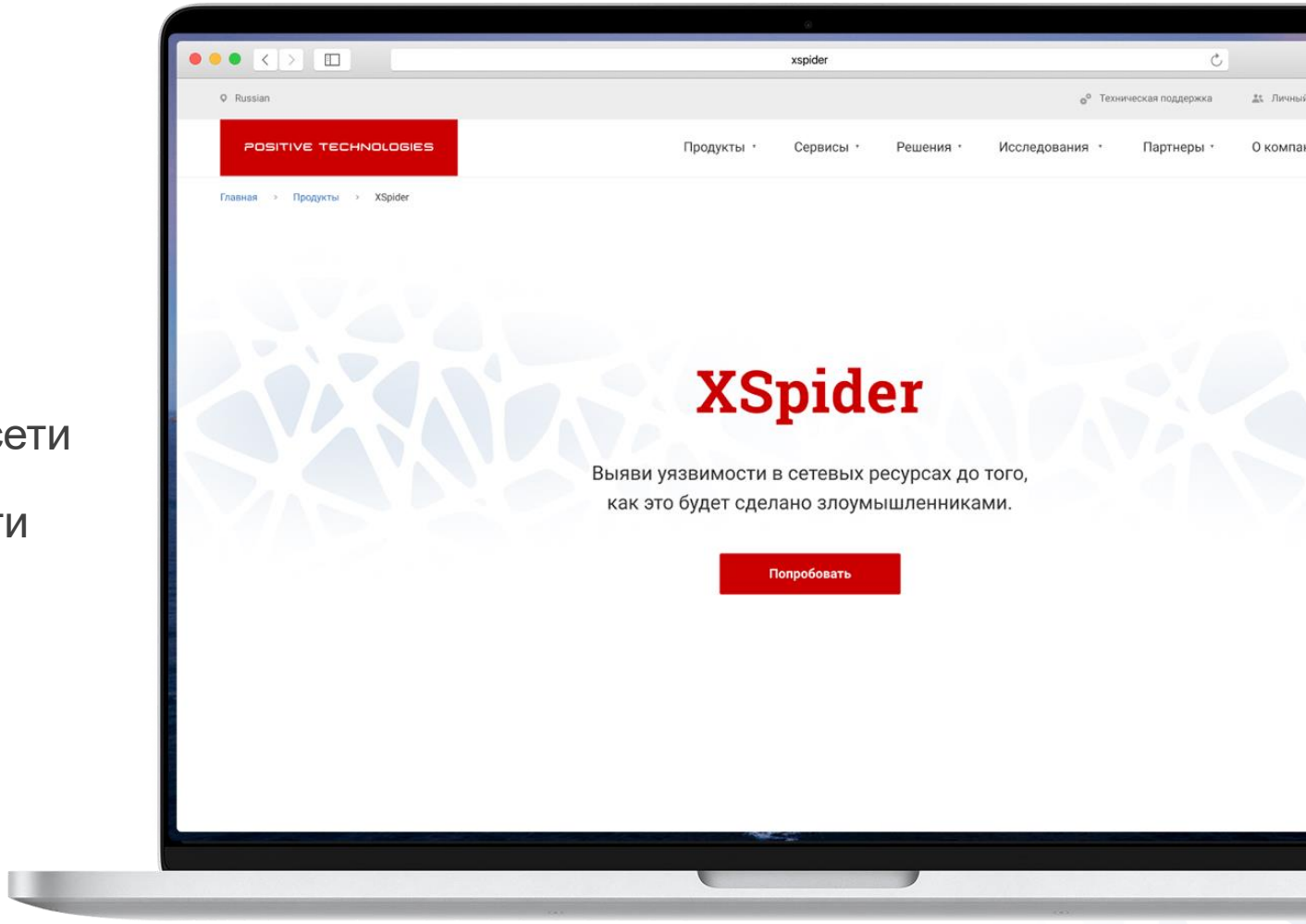
XSpider

Профессиональный сканер уязвимостей

- Быстро и точно определяет компоненты сети
- Сканирует сетевые ресурсы на уязвимости
- Выдает рекомендации по устранению уязвимостей

20+ ЛЕТ

XSpider является признанным лидером среди сканеров безопасности в России



Возможности XSpider

Проведет инвентаризацию

Определит сетевые узлы, открытые порты, идентифицирует операционную систему и серверные приложения, а также отследит изменения в состоянии информационной системы.

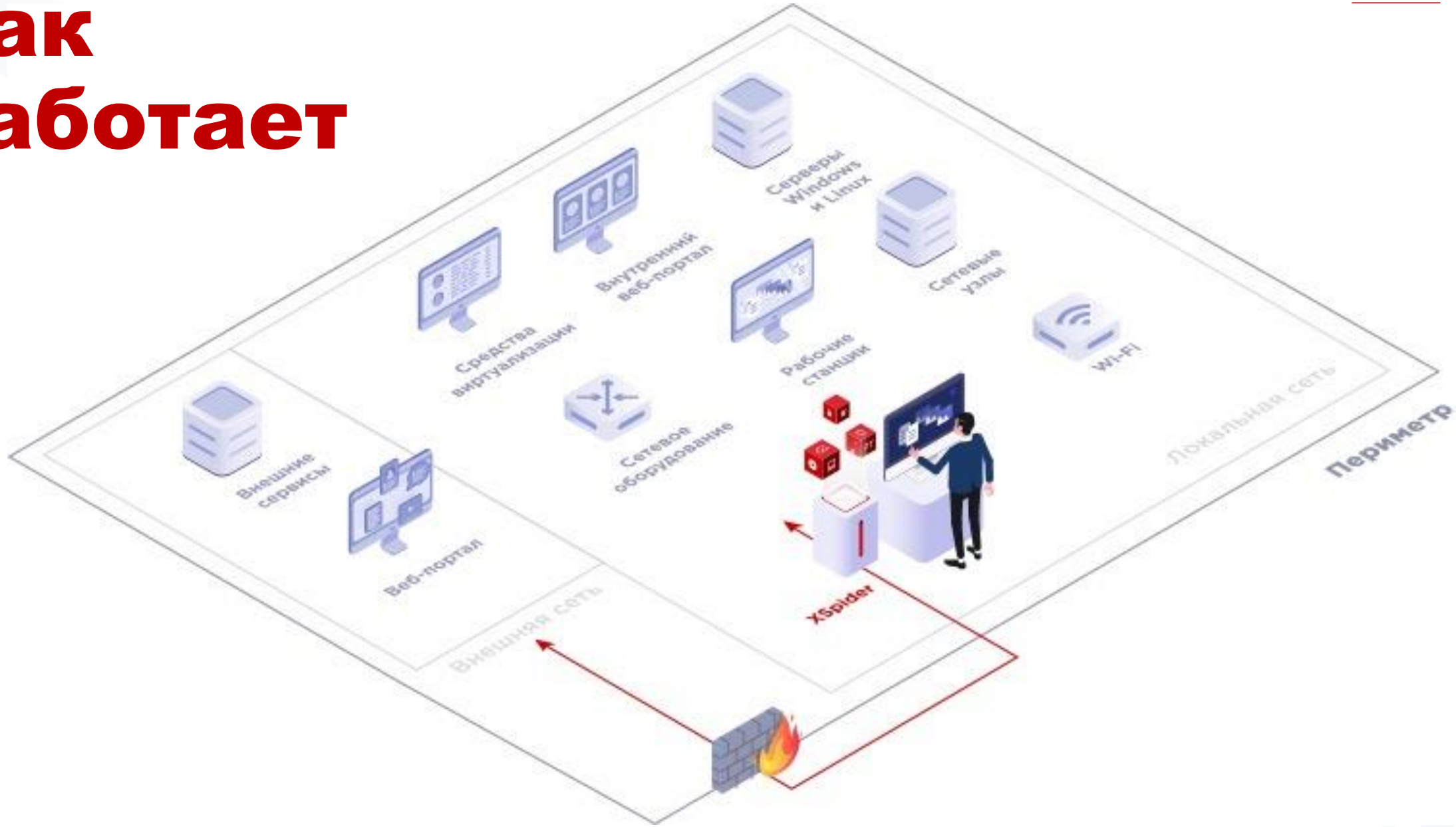
Выявит уязвимости

Найдет уязвимости на рабочих станциях, серверах, сетевом оборудовании, проведёт глубокий анализ веб-ресурсов. Проверит стойкость паролей для сервисов, требующих аутентификации. Позволит автоматизировать процесс поиска уязвимостей.

Подскажет решение

По всем обнаруженным уязвимостям XSpider даст подробную информацию и четкие и понятные рекомендации по их устранению. Также сформирует отчеты по результатам сканирования.

Как работает



Преимущества

- Обширная база уязвимостей с регулярными пополнениями
- Поддержка уязвимостей из БДУ ФСТЭК России
- Анализ веб-приложений по OWASP Top 10
- Русскоязычная техническая поддержка
- Автоматический запуск задач сканирования и выпуска отчета
- Качественная проверка парольной защиты
- Низкий уровень ложных срабатываний
- Низкие аппаратные требования
- Не требует установки дополнительного ПО и агентов

Помогает выполнять требования регуляторов

Сертификат ФСТЭК России №3247

подтверждает соответствие средствам контроля (анализа) защищенности и требованиям по 4 уровню отсутствия НДВ

Сканер может использоваться в составе автоматизированных систем, а также:

- в ИСПДн (закон № 152-ФЗ, приказ ФСТЭК № 21),
- ГИС (приказ ФСТЭК № 17),
- АСУ ТП КВО (приказ ФСТЭК №31),
- для защиты ЗО КИИ (приказ ФСТЭК №239).

Входит в реестр российского ПО

с 16 мая 2016 года, рег. номер 786
reestr.minsvyaz.ru/reestr/75106/

Сертификат соответствия МО РФ № 2910

позволяет применять XSpider для сканирования на уязвимости в сетях Минобороны

Обеспечение соответствия требованиям PCI DSS

Варианты поставки
и модель лицензирования

Поставка

Сертифицированная/ актуальная версия

поставляются по одной цене

Поддержка

Включена в стоимость

- оперативная техническая поддержка по телефону: +7(495)744-01-44, с 9:00 до 19:00
- портал технической поддержки: support.ptsecurity.ru/

Годовое лицензирование

Базовая лицезия

по проверяемым хостам (любое оборудование подключенное к локальной или глобальной сети, имеющее ip-адрес или DNS имя)

Продление

- по истечению срока базовой лицензии, но не позднее 12 месяцев
- продление лицензии составляет 40% от стоимости покупки

Наши контакты

Все вопросы по получению демоверсии,
стоимости и заказа лицензии можно задавать на:

xspider@ptsecurity.com