

XSpider

Как продавать средства информационной безопасности

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





Задача

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

Что сделано

Проверили защищенность веб-портала, внедрили РТ 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.



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





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



XSpider

Профессиональный сканер уязвимостей

Как злоумышленник может проникнуть в компанию



Вредоносное ПО

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

Уязвимости в ПО

Использование устаревших версий ПО является серьезным риском

Веб-уязвимости

Позволяет получить контроль над вебприложением, а также провести атаку и на локальную сеть

Ошибки в настройках

Злоумышленники используют ошибки, которые допускают администраторы ИС

Подбор учеток

Большинство паролей составлены предсказуемо

Социальная инженерия

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

^{* «&}lt;u>Актуальные киберугрозы — 2019. Тренды и прогнозы</u>», 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.

XSpider



Класс решений

Анализ защищенности (security assessment)

Продукт

Сетевой сканер уязвимостей

Задачи заказчика

- Проверить инфраструктуру компании на наличие уязвимостей
- Получить достоверные данные о составе сети
- Отслеживать изменения в состоянии защищенности
- Автоматизировать контроль защищенности в организации
- Выполнять требования законодательства

Возможности XSpider







Проведет инвентаризацию

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

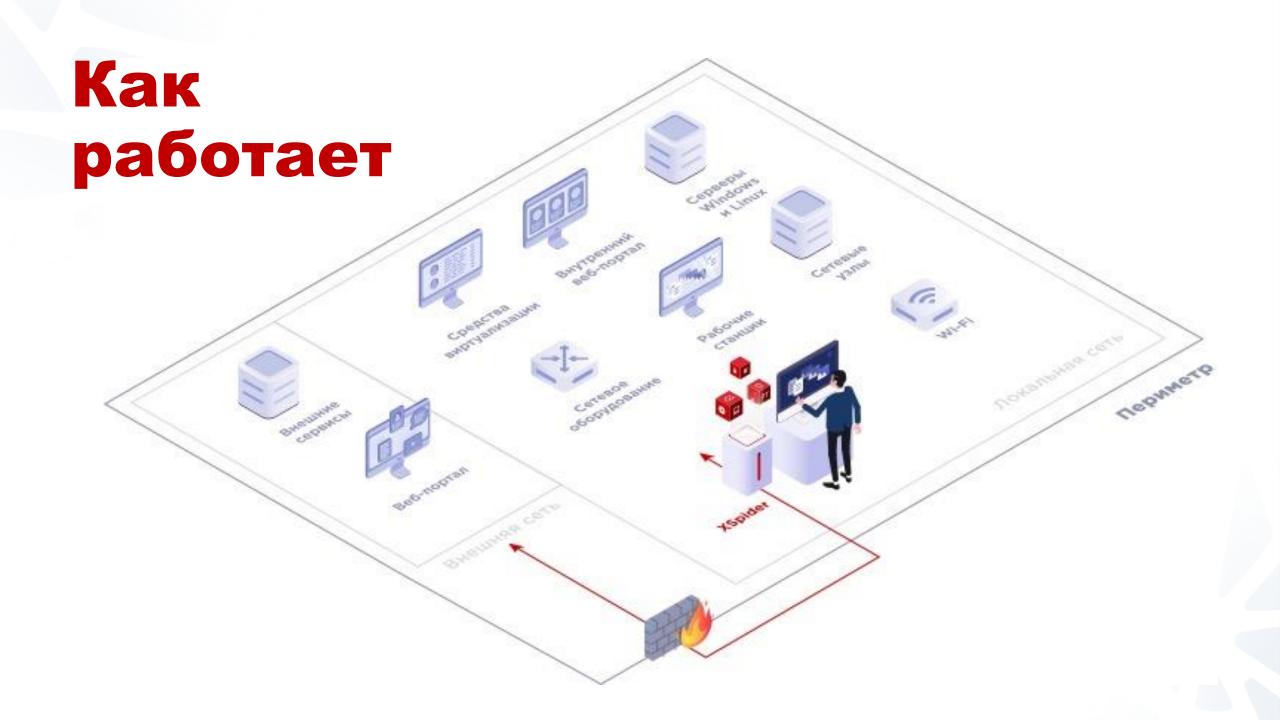
Выявит уязвимости

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.









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-Ф3, приказ ФСТЭК № 21),
- ГИС (приказ ФСТЭК № 17),
- АСУ ТП КВО (приказ ФСТЭК №31),
- для защиты 3О 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

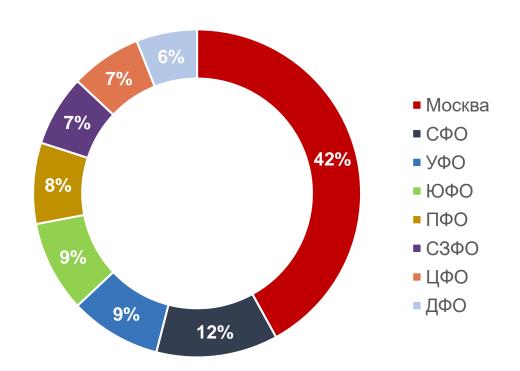


Обеспечение соответствия требованиям PCI DSS

Портрет заказчика



География продаж 2019 года



Клиенты по отраслям за 2019 год



43%

государственны сектор



13% ТЭК



10%

финансовая отрасль



10/0 пром

промышленные компании



6%

медицинские учреждения



6%

сфера образования



6%

СВЯЗЬ



4%

транспорт

Портрет заказчика



Message для заказчика

Государственный сектор, медицина, образование

Необходимость использовать средства анализа защищенности в ГИС (приказ ФСТЭК № 17), и при работе с перс. данными (152-ФЗ, приказ ФСТЭК № 21).

Промышленность, ТЭК

Основные атаки из-за слабых паролей и незащищенных протоколов связи. Реализация системы защиты информации 30 КИИ.

Финансовые организации, телеком-операторы

Большое количество критически важных веб-приложений, работа с персональными данными. Для банков необходимость соответствия PCI DSS.

SMB сектор



От **4х до 10 000** узлов

сканирования



Средний заказ —

на 32 хоста

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

Прайс-лист



Количество хостов	Стоимость	Стоимость доп. хоста
4	14 000 руб.	3 000 руб.
8	23 400 руб.	2 500 руб.
16	35 000 руб.	1 700 руб.
32	50 400 руб.	1 100 руб.
64	71 000 руб.	800 руб.
128	99 000 руб.	500 руб.
256	138 600 руб.	450 руб.
512	219 000 руб.	430 руб.
1024	378 000 руб.	400 руб.
2048	640 000 руб.	380 руб.
3072	890 000 руб.	350 руб.
4096	1 100 000 руб.	320 руб.
10240	2 200 000 руб.	300 руб.

Регистрация проекта



Авторизация проекта

Дополнительная скидка

на новые проекты от 350 к.

Нужно первым предоставить информацию об интересе заказчика с определением необходимой технической конфигурации.

Конкурентное замещение

+20% скидки

При замещении конкурента в заказчике.

Продление

Специальные условия

Для партнера, который привел клиента.

Продажа XSpider



Positive Technologies



Дистрибьютор



Авторизованные партнеры





Заказчики

Партнерская программа



	А Базовый	Серебряный	Т Золотой
Партнерская скидка	20%	30%	35%
Договор с дистрибьютором	✓	✓	✓
Годовой объем продаж	×	1 млн рублей	2 млн рублей
Обучение специалистов	×	×	✓
Маркетинговые активности	×	×	✓
Реклама на веб-сайте партнера	×	✓	✓

Партнерские сертификаты

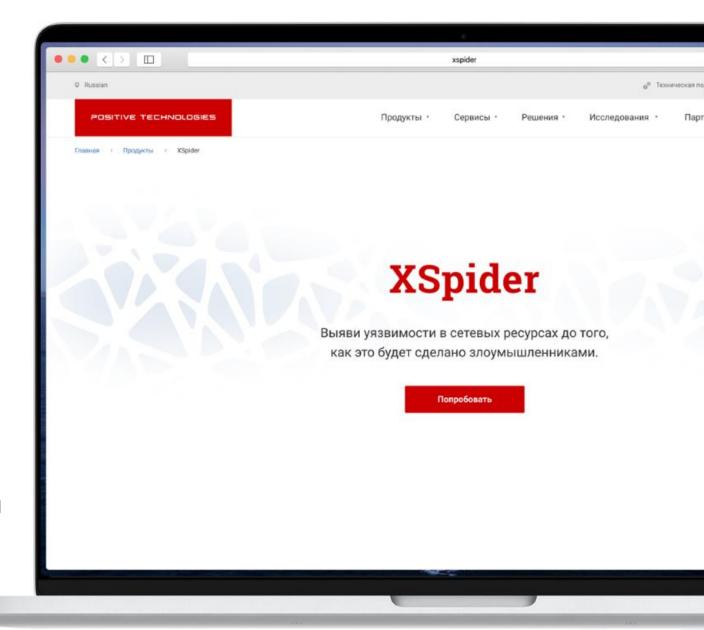






Поддержка продаж

- Предоставление актуальной информации и материалов по решению;
- Предоставление триальных лицензий;
- Обучение по продукту;
- Презентация решения для заказчиков;
- Совместные маркетинговые активности, нацеленные на лидогенерацию;
- Акции для заказчиков и спец предложения для партнеров.





Наши контакты

По вопросам сотрудничества, закупки, получения триальных лицензий:

xspider@ptsecurity.com

Маркетинговые и технические материалы по продукту, новости, акции:

partners.ptsecurity.com