POSITIVE TECHNOLOGIES

Позитивный подход

к кибербезопасности

ptsecurity.com

POSITIVE TECHNOLOGIES

О компании

ptsecurity.com

Обеспечиваем практическую кибербезопасность бизнеса

18 лет
исследований
и опыта в обеспечении
кибербезопасности

500+
экспертов в крупнейшем
исследовательском
центре в Европе

10+ продуктов
для мониторинга
и обеспечения ИБ в нашем
портфолио

в 3 раза
быстрее растем по
сравнению с рынком
в России

80%
отечественных компаний
из списка **Expert 400**
используют наши продукты

9 лет
проводим самые
крупные в Европе
открытые киберучения

Нам доверяют
не только в России

SAMSUNG
LLOYDS BANK FOUNDATION England & Wales
UniCredit Bank
Terna Rete Elettrica Nazionale
enel

Обладаем экспертизой
во всех областях кибербезопасности

200+
уязвимостей нулевого дня наши эксперты обнаруживают ежегодно

500+
уязвимостей нулевого дня в системах класса SCADA найдены нами

500+
работ по анализу безопасности мобильных и веб-приложений в год

30+
нулевого дня в mobile telco найдены нами

НАШИ ПРОЕКТЫ

sochi.ru 2014

2018 МАРТА
ВЫБОРЫ ПРЕЗИДЕНТА РОССИИ

FIFA WORLD CUP RUSSIA 2018

Наши исследования

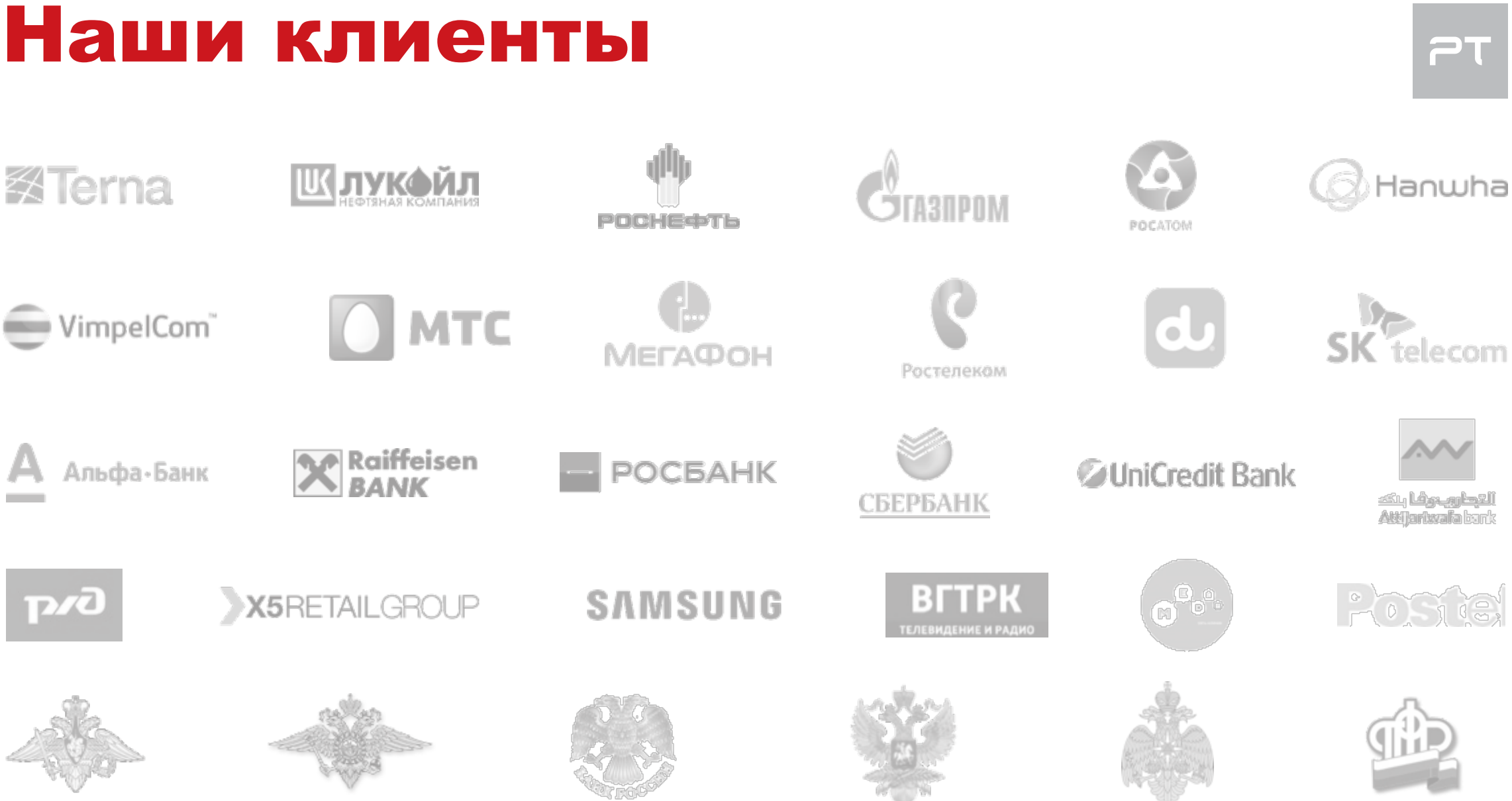
Выпускаем более

20 исследований в год

Ежеквартальные отчеты об актуальных киберугрозах и трендах, прогнозы, расследования активностей хакерских группировок, отраслевые исследования

ptsecurity.com/ru-ru/research/analytics

Наши клиенты



Positive Hack Days

Ежегодно проводим

международный ИБ-форум,

собирающий тысячи участников

phdays.com

- В рамках форума мы организуем **30-часовую кибербитву** за эмулированную инфраструктуру крупного города. Формат соревнования максимально приближен к реальности

- Во время кибербитвы работает **SOC на базе наших продуктов**, который мониторит инфраструктуру и на практике доказывает свою эффективность

Портфолио
Positive Technologies

ptsecurity.com

Продуктовое портфолио

ПРОДУКТЫ

- **MaxPatrol 8**
- **MaxPatrol SIEM**
- **MaxPatrol VM**
- **PT ISIM**
- **PT MultiScanner**
- **PT Sandbox**
- **PT Network Attack Discovery**
- **PT Application Firewall**
- **PT Application Inspector**
- **XSpider**
- **ПТ Ведомственный центр**
- **PT Platform 187**

РЕШЕНИЯ

- Для раннего **выявления сложных угроз**
- Для обеспечения **безопасности объектов КИИ**
- Для построения **центра ГосСОПКА**

Портфолио услуг

Сервисы 2.0

услуги для непрерывного повышения защищенности бизнеса от киберугроз

Услуги

мониторинга и реагирования на инциденты ИБ

Услуги

по глубокому анализу защищенности

Продукты
Positive Technologies

ptsecurity.com

MaxPatrol 8

MaxPatrol 8

Универсальное средство автоматизированного анализа защищенности и контроля соответствия стандартам

- Позволяет регулярно и комплексно контролировать состояние защищенности всей IT-инфраструктуры.
- Позволяет построить процесс управления уязвимостями на KPI, прозрачных для руководства.
- Гибко масштабируется и подходит как для небольших компаний, так и для крупных территориально-распределенных предприятий.

MaxPatrol 8

Охватывает все информационные ресурсы компании

Поддерживает и позволяет контролировать параметры 1000+ платформ и приложений: сетевую и системную инфраструктуры, серверы, беспроводные сети и сети IP-телефонии, базы данных, приложения, системы ERP, веб-приложения, АСУ ТП.

Выявляет уязвимости с максимальной точностью

Выявляет уязвимости, ошибки конфигурации компонентов ИС, проверяет соответствие настроек ИС требованиям ИБ. Использует методы черного и белого ящиков для анализа защищенности узлов, проверяет актуальность уязвимостей, обеспечивая низкое число ложных срабатываний.

Упрощает анализ соответствия стандартам и политикам ИБ

Содержит встроенные политики безопасности, позволяющие оценить соответствие инфраструктуры основным стандартам (ISO 27001/27002, PCI DSS и CIS). Также дает возможность настроить специальные политики для контроля выполнения собственных корпоративных правил безопасности.

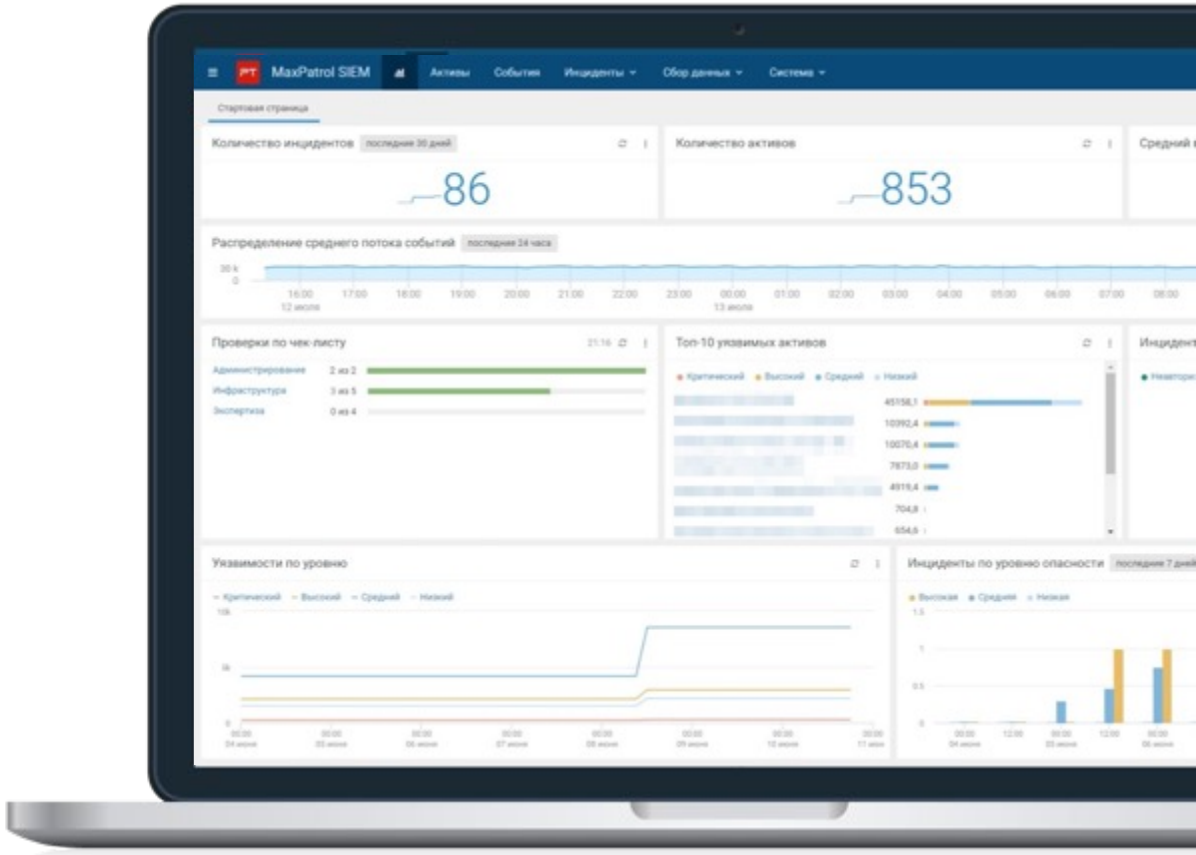
MaxPatrol SIEM

Второе место
на российском рынке SIEM
(согласно исследованию компании IDC)

MaxPatrol SIEM

Система выявления инцидентов с уникальным подходом к обеспечению прозрачности IT-инфраструктуры и глубокой экспертизой в обнаружении угроз

- Дает видимость IT-инфраструктуры.
- Позволяет выявлять самые актуальные угрозы.
- Снижает трудозатраты специалистов по ИБ на мониторинг состояния инфраструктуры и написание правил выявления атак.



MaxPatrol SIEM

Лидирующее отечественное SIEM-решение

Продукт внедрен более чем в 200 промышленных, транспортных, финансовых компаниях, в частном и государственном секторе, в органах власти. Согласно исследованию IDC, MaxPatrol SIEM входит в тройку лидеров российского рынка SIEM. Другие отечественные SIEM-системы занимают не более 6% рынка.

Регулярно получает экспертизу для обнаружения угроз

Раз в два месяца MaxPatrol SIEM пополняется пакетам экспертизы с новыми правилами корреляции, индикаторами компрометации и плейбуками.

Быстро развивается и становится проще

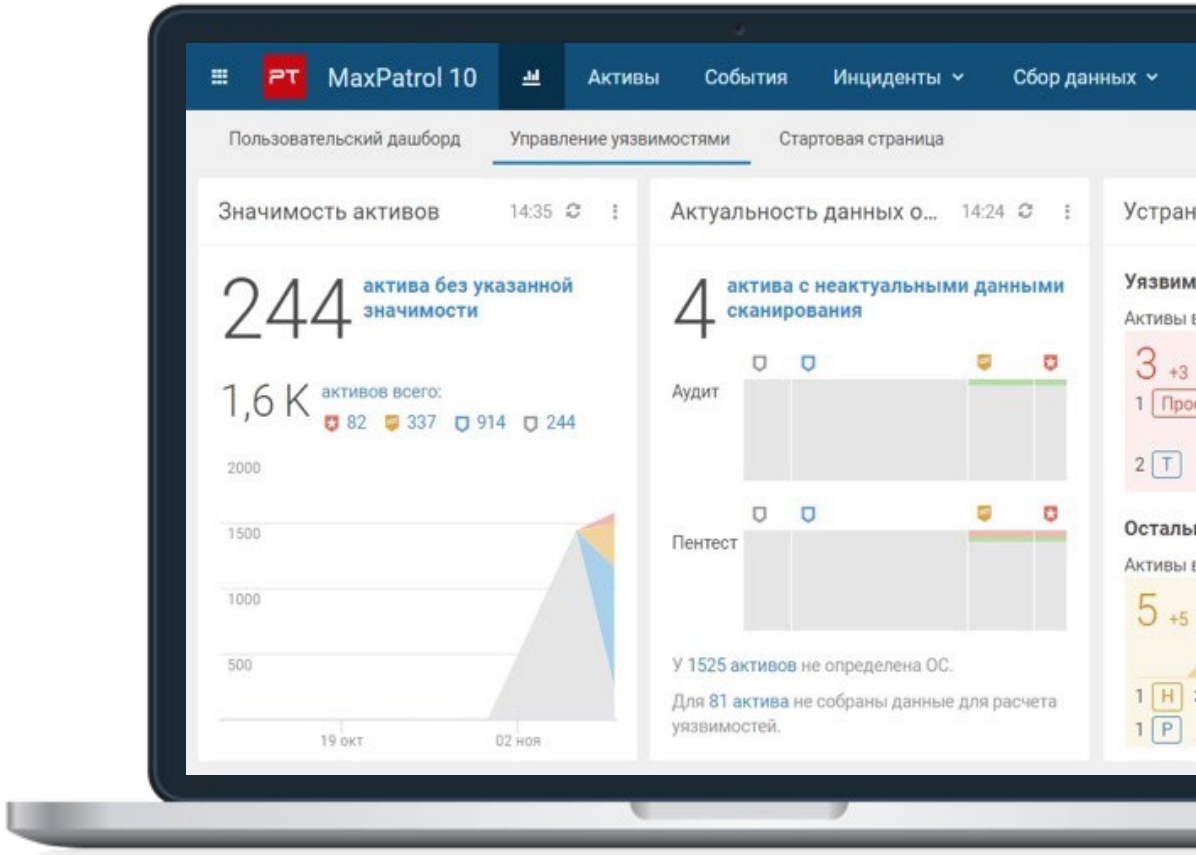
Выпускаем два релиза в год, регулярно внедряем новые технологии и расширяем команду разработки продукта. Мы постоянно упрощаем продукт, чтобы развернуть MaxPatrol SIEM, работать с ним и выявлять угрозы мог даже новичок. Например, за последние два года в продукте появились регулярная поставка пакетов экспертизы, чек-лист настройки системы, конструктор правил корреляции и возможность быстрого снижения количества ложных срабатываний.

MaxPatrol VM

MaxPatrol VM

Система управления уязвимостями нового поколения

- Помогает выстроить полноценный процесс управления уязвимостями, в который вовлечены как ИБ, так и IT-специалисты.
- Контролирует защищенность IT-инфраструктуры в каждый момент времени и помогает правильно приоритизировать работу над уязвимостями.



MaxPatrol VM

Сокращает время работы с уязвимостями

MaxPatrol VM не только проводит глубокую проверку систем, но и помогает автоматизировать управление уязвимостями с учетом значимости компонентов сети для бизнес-процессов.

Позволяет быстрее реагировать на новые опасные уязвимости

MaxPatrol VM может выявить наличие уязвимости на основе ранее собранной информации об инфраструктуре. Это позволяет сразу же переходить к этапу устранения уязвимости или применения компенсирующих мер.

Делает процессы более прозрачными

В MaxPatrol VM можно задать регламенты для сканирования и устранения уязвимостей. Дашборды системы наглядно демонстрируют работу IT и ИБ отделов, позволяя контролировать уровень защищенности инфраструктуры и сроки устранение уязвимостей.

Делает систему максимально сложной для проникновения

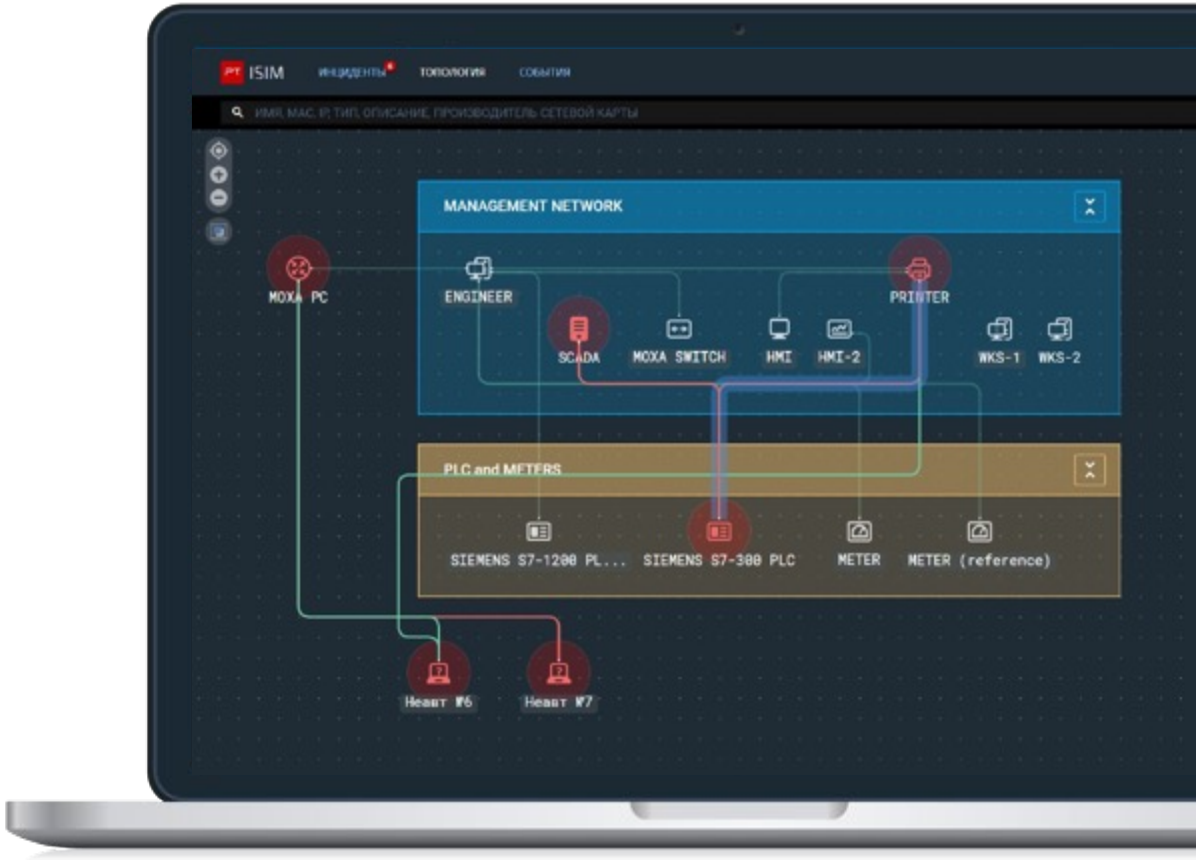
Специалисты Positive Technologies сообщат о трендовых уязвимостях, которые необходимо закрыть в первую очередь. Они наиболее опасные и используются злоумышленниками в атаках прямо сейчас.

PT ISIM

PT ISIM

Система глубокого анализа технологического трафика (Industrial NTA/NDR) для выявления сложных атак внутри сетей АСУ ТП

- Помогает на ранней стадии выявлять кибератаки и неавторизованные действия персонала.
- Позволяет контролировать векторы атак и соблюдение политик ИБ, специфических для конкретного промышленного объекта.
- Позволяет проводить превентивный поиск сложных угроз внутри технологической сети и обеспечивает доказательную базу в ходе расследования инцидентов.



PT ISIM

Непрерывно инвентаризирует и профилирует сеть

Не оказывает влияния на технологический процесс, PT ISIM непрерывно инвентаризирует элементы сети АСУ ТП, контролирует ее целостность и оповещает о критических изменениях, которые могут являться признаком нарушения ИБ и требовать немедленного реагирования.

С высокой точностью детектирует угрозы и аномалии

PT ISIM использует собственную базу данных индикаторов промышленных угроз (PT ISTI) и благодаря комбинации сигнатурных методов обнаружения атак и механизма поведенческого анализа позволяет эффективно выявлять кибератаки на ранней стадии. В постоянно пополняемой базе PT ISTI насчитывается более 4000 различных индикаторов и правил обнаружения угроз в АСУ ТП.

Обеспечивает поиск угроз в сетях АСУ ТП и расследование инцидентов ИБ

Продукт анализирует и хранит весь спектр трафика технологической сети: от ИТ-протоколов до специализированных промышленных. Благодаря встроенным инструментам работы с метаданными продукт предоставляет широкие возможности для специализированного поиска угроз (threat hunting) и расследования инцидентов информационной безопасности в сетях АСУ ТП.

Позволяет соответствовать требованиям

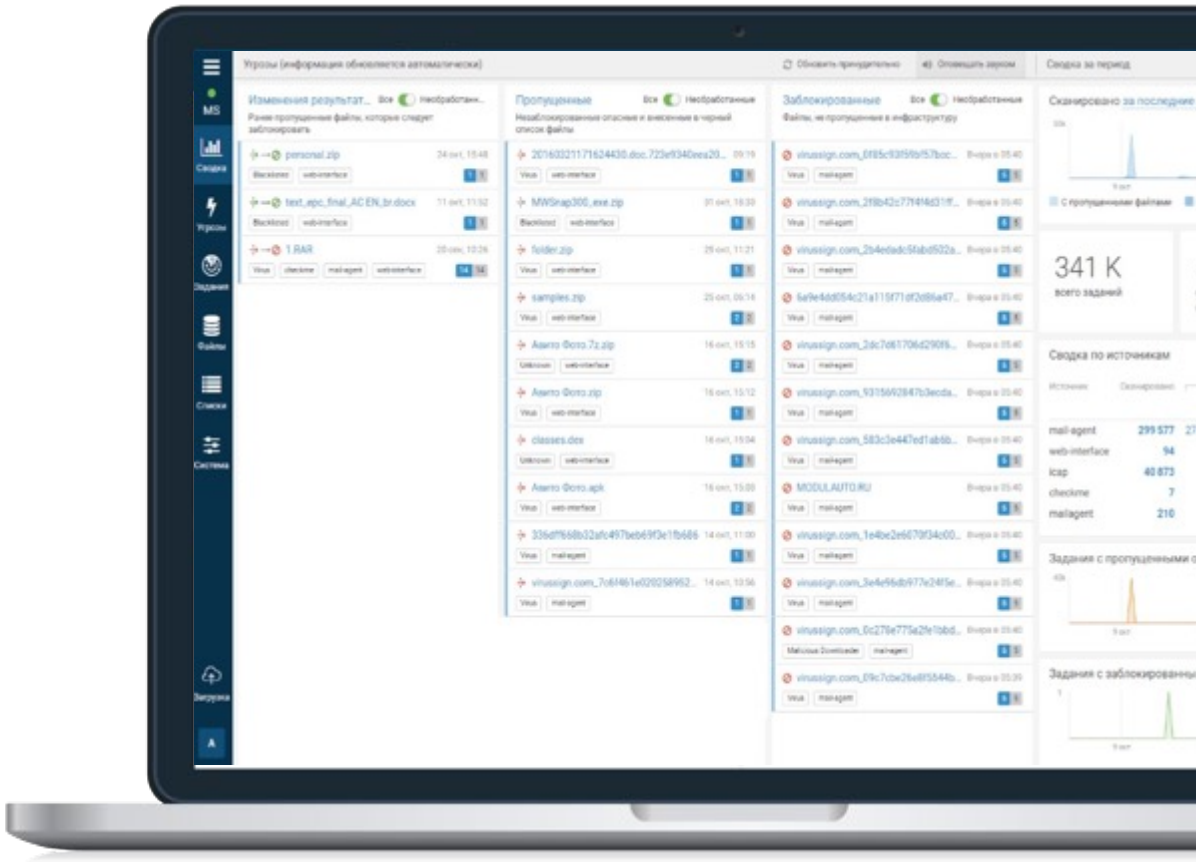
PT ISIM обеспечивает реализацию широкого перечня мер защиты АСУ ТП в соответствии с 187-ФЗ, требованиями приказов ФСТЭК № 31, 239, 196, отраслевых стандартов и является ключевым звеном для системы ГосСОПКА.

PT MultiScanner

PT MultiScanner

Многоуровневая система защиты от всех типов вредоносных программ

- Обеспечивает защиту от вирусных угроз с помощью мультивендорной антивирусной проверки.
- Позволяет быстро локализовывать и устранять угрозы благодаря подробной информации о пораженных узлах.



PT MultiScanner

Защищает от массовых атак

Продукт осуществляет проверку файлов с помощью нескольких антивирусов и правил PT Expert Security Center. Это позволяет защититься как от массовых угроз, так и от атак хакерских группировок с применением известного вредоносного ПО.

Помогает быстрее реагировать и расследовать инциденты

PT MultiScanner дает точную информацию обо всех пораженных узлах сети и позволяет локализовать угрозу: найти ее источник, отследить участников и этапы распространения, а следовательно – оперативно принять необходимые меры.

Выявляет скрытое присутствие вредоносного ПО

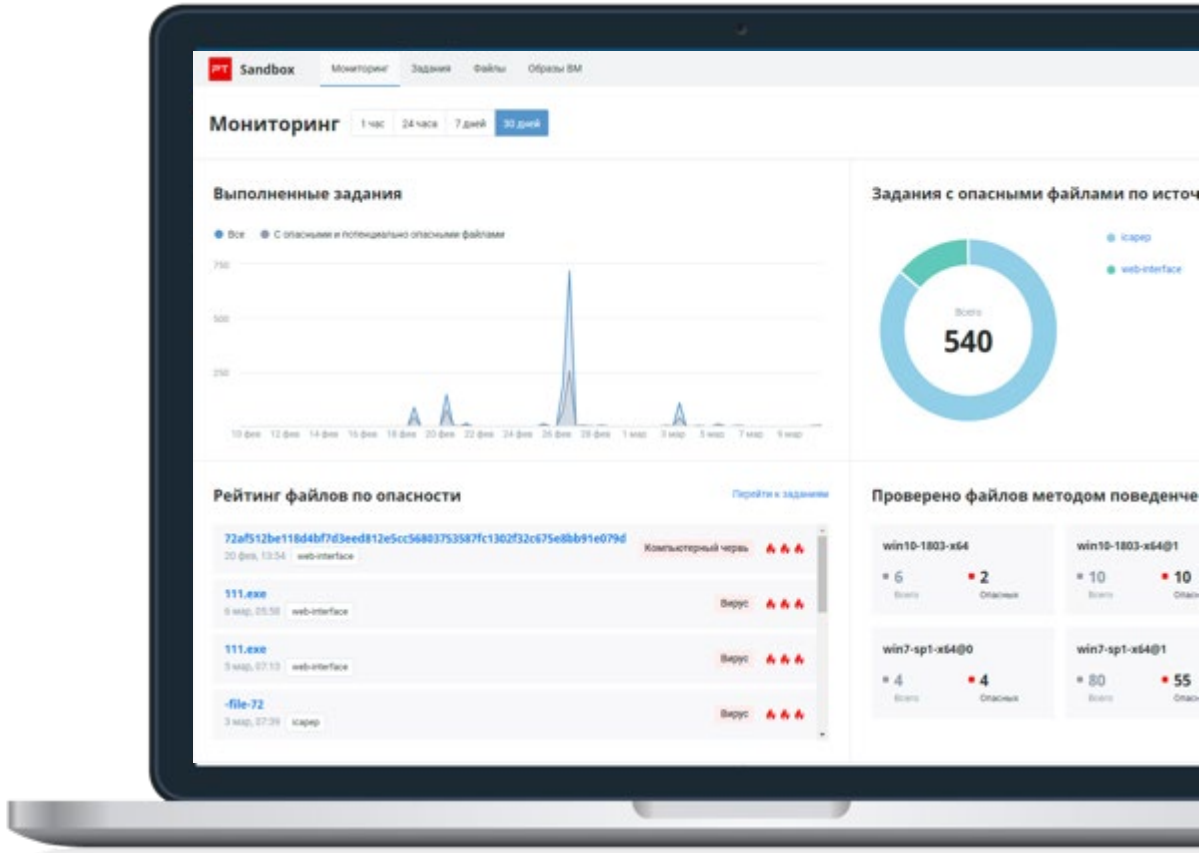
Благодаря автоматическому ретроспективному анализу PT MultiScanner находит вредоносное ПО, которое не было обнаружено ранее. Повторная проверка файлов запускается после обновлений баз данных продукта.

PT Sandbox

PT Sandbox

Передовая песочница с возможностью гибкой кастомизации виртуальных сред

- Защищает от целевых и массовых атак с применением неизвестного вредоносного ПО и угроз нулевого дня.
- Выявляет и блокирует угрозы в корпоративной почте, пользовательском веб-трафике, файловых хранилищах.



PT Sandbox

Использует самые актуальные знания для выявления угроз

Все файлы проходят комплексную проверку, включающую статический и динамический анализ с помощью уникальных правил PT Expert Security Center и проверку с помощью нескольких антивирусов. Правила PT ESC создаются экспертами в ходе исследования деятельности хакерских группировок и расследований инцидентов и еженедельно выгружаются в продукт.

Защищает именно вашу инфраструктуру

В PT Sandbox можно гибко настроить виртуальные среды в соответствии с реальными рабочими станциями и загрузить в них специфическое ПО, которым пользуются сотрудники. Это позволяет выявлять целевые и массовые атаки на конкретный софт или его версии и защищаться от угроз нулевого дня.

Обнаруживает угрозы не только в файлах, но и в трафике

PT Sandbox проверяет весь сетевой трафик, который генерируется в процессе анализа файла, включая скрытый за TLS. Это позволяет выявлять опасную сетевую активность, внешне не связанную с файлом.

Выявляет атаки, не обнаруженные ранее

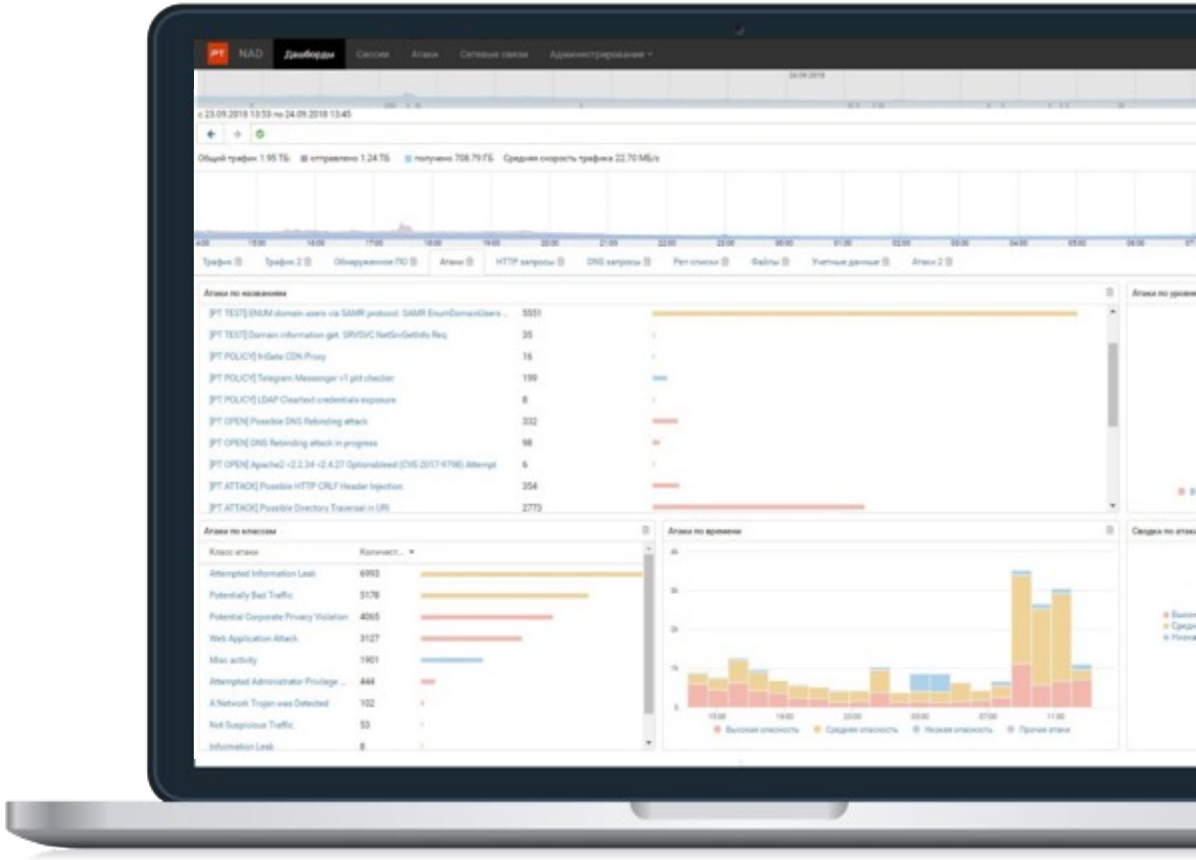
Продукт проводит автоматический ретроспективный анализ файлов после обновления баз знаний, выявляя скрытые в инфраструктуре и самые новые угрозы.

PT Network Attack Discovery

PT NAD

Система глубокого анализа сетевого трафика (NTA/NDR) для выявления атак на периметре и внутри сети

- Обнаруживает скрытые угрозы в сети по большому количеству признаков.
- Дает понимание, что происходит в сети, и позволяет проконтролировать соблюдение регламентов ИБ.
- Повышает эффективность работы SOC, помогает восстановить цепочку атаки и собрать доказательную базу.



PT Network Attack Discovery

Видит активность злоумышленников как на периметре, так и внутри сети

PT NAD анализирует не только внешний, но и внутренний трафик, поэтому он детектирует горизонтальные перемещения злоумышленников, попытки эксплуатации уязвимостей, атаки на конечных пользователей в домене и на внутренние сервисы.

Использует передовые технологии выявления угроз

Для выявления атак на ранних стадиях продукт использует технологии поведенческого анализа, глубокую аналитику, собственные правила детектирования угроз, индикаторы компрометации и ретроспективный анализ. PT NAD видит вредоносную активность даже в зашифрованном трафике.

Является основой для построения SOC и threat hunting

Продукт хранит 1200 параметров сессий и записи сырого трафика. Такие данные становятся полезными источниками знаний при раскрутке цепочки атаки и ее локализации, а также при проверке гипотез в рамках threat hunting.

PT Application Firewall

PT AF

Межсетевой экран уровня веб-приложений (Web Application Firewall)

- Защищает веб-приложения от целевых и массовых атак.
- Быстро встраивается в инфраструктуру.
- Поддерживает непрерывность бизнес-процессов.

PT Application Firewall

Быстрый старт и интеграция

PT Application Firewall работает «из коробки», имеет различные опции внедрения: сетевой мост L2, прозрачный прокси-сервер, обратный прокси-сервер, режим мониторинга или расследования, интегрируется со сторонними СЗИ, в том числе: антивирусные системы, SIEM, Anti-DDoS, DLP.

Простота в использовании

PT Application Firewall снижает трудозатраты оператора ИБ за счет встроенных политик защиты, механизмов корреляции и приоритизации найденных угроз.

Адаптация к изменениям

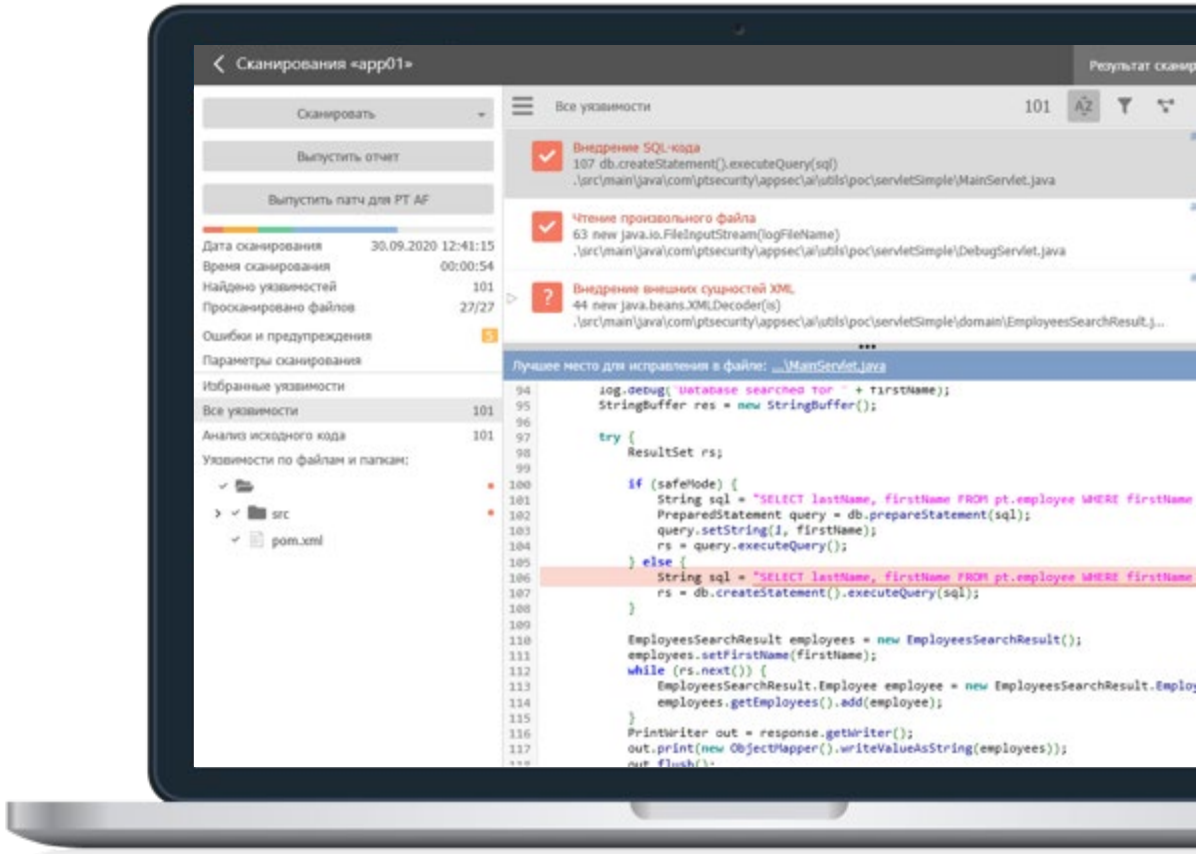
PT Application Firewall гибко масштабируется под увеличивающиеся нагрузки на веб-приложения, автоматически адаптируется к изменениям в их бизнес-логике за счет алгоритмов машинного обучения и виртуального патчинга уязвимостей.

PT Application Inspector

PT AI

Универсальный инструмент для поиска уязвимостей в приложениях

- Точно находит и приоритизирует уязвимости.
- Проверяет исходный код и готовое приложение.
- Интегрируется в действующие процессы разработки.



PT Application Inspector

Максимальная точность

За счет комбинации статических, динамических и интерактивных методов проверки кода (SAST, DAST и IAST), а также анализа сторонних библиотек (SCA) и конфигурационных файлов, PT Application Inspector находит только реальные уязвимости. Это помогает разработчикам сконцентрироваться на важных проблемах и снижает затраты экспертов на ручную проверку результатов.

Простота и безопасность тестирования

PT Application Inspector не требует установки и настройки приложения или доступа к тестовой среде. Просто укажите папку, содержащую готовый код приложения (или его часть) или ссылку на сайт, чтобы начать анализ.

Быстрое встраивание в процессы разработки

PT Application Inspector гибко встраивается в существующие процессы за счет готовых плагинов для подключения к системам сборки и доставки приложений, позволяет выстроить процесс безопасной разработки кода.

XSpider

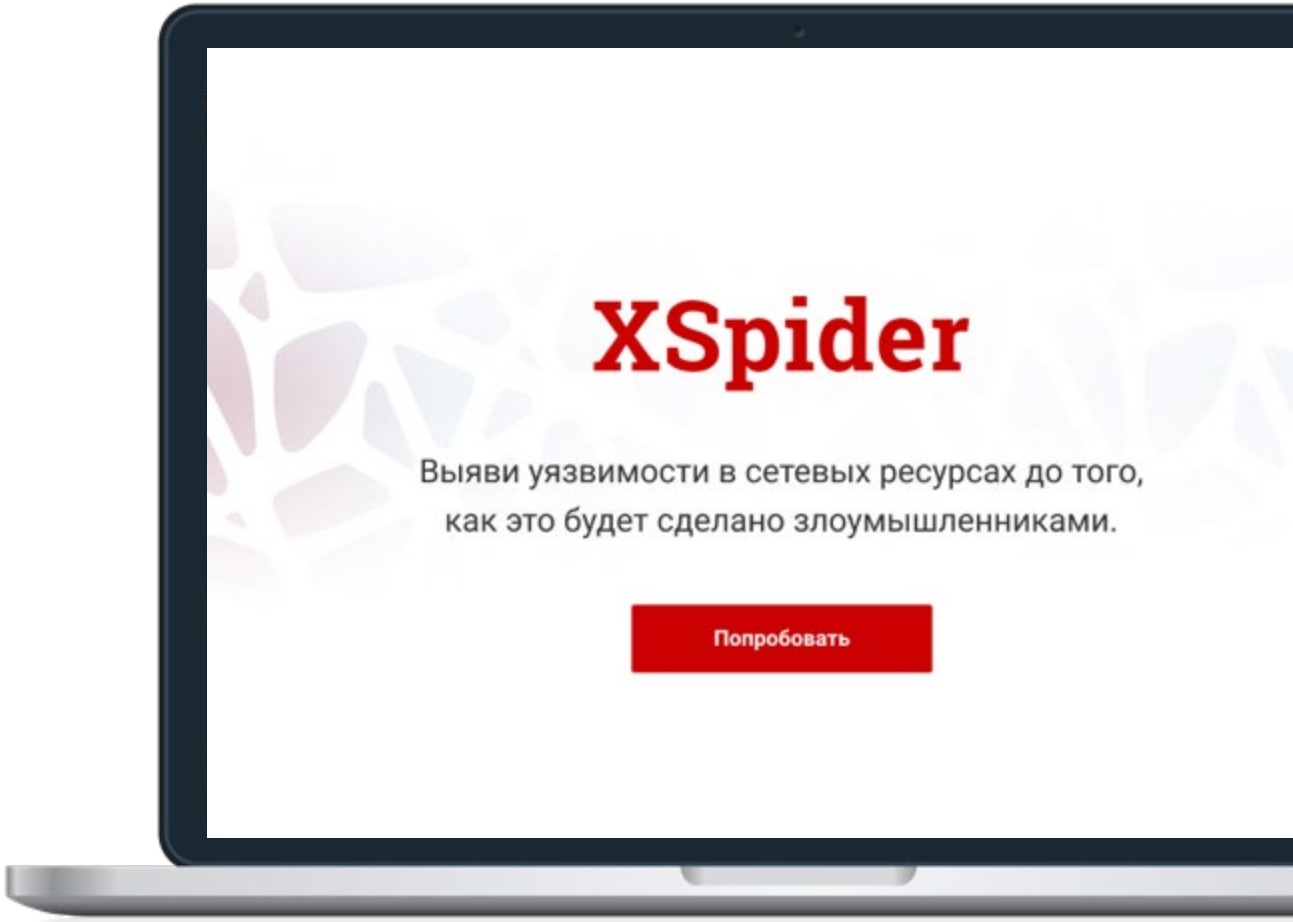
XSpider

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



XSpider

Обнаружит уязвимости в сетевых ресурсах

Продукт проверяет сеть на уязвимости методом черного ящика. Выявляет уязвимости на рабочих станциях, серверах, сетевом оборудовании, проводит анализ веб-ресурсов. Проверяет стойкость паролей для сервисов, требующих аутентификации. База актуальных уязвимостей XSpider регулярно пополняется экспертами Positive Technologies.

Автоматизирует процесс поиска уязвимостей

XSpider избавляет от необходимости ручной проверки каждого отдельного компонента информационной системы. Решение быстро настраивается и не требует от специалистов навыков тестирования на проникновение.

Анализирует результаты проверки сети

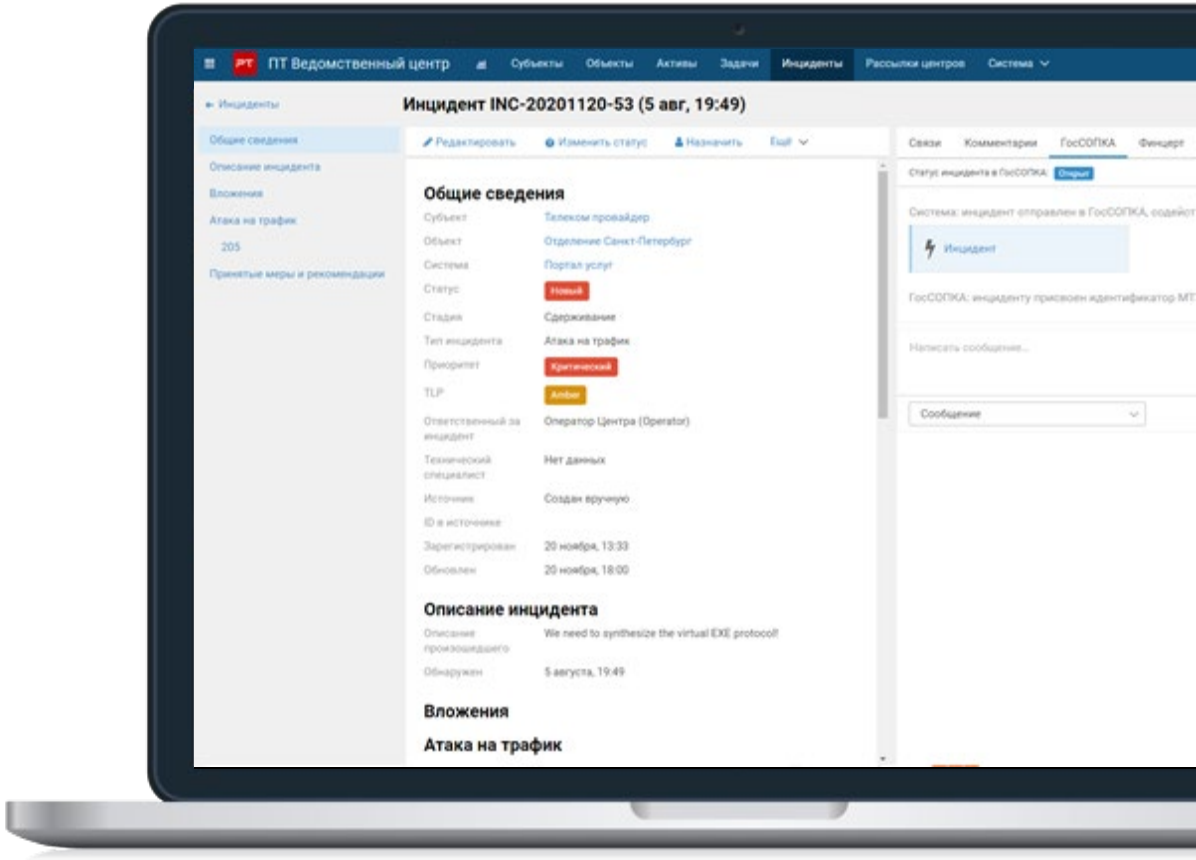
XSpider выдает в удобном и структурированном виде данные о результатах сканирования для детального анализа текущего состояния системы. По всем обнаруженным уязвимостям можно получить подробную информацию и четкие рекомендации по их устранению.

ПТ Ведомственный центр

ПТ ВЦ

Система управления инцидентами и взаимодействия с ГосСОПКА и ФинЦЕРТ

- Позволяет соответствовать требованиям законодательства о необходимости регистрации инцидентов, управления ими и информирования НКЦКИ и ФинЦЕРТ.
- Помогает автоматизировать и контролировать процесс реагирования на инциденты: назначать ответственных, выставлять приоритеты, отслеживать статусы и сроки обработки.



ПТ Ведомственный центр

Взаимодействие с ГосСОПКА и ФинЦЕРТ

Обмен информацией об инцидентах и актуальных угрозах с НКЦКИ и ФинЦЕРТ происходит в двухстороннем формате. Сведения о регистрации инцидента, ходе реагирования и завершении работ отправляются в онлайн-чате.

Экономит время специалистов по ИБ

Автоматическое создание карточек инцидентов и применение шаблонов реагирования снижают временные затраты специалистов. Наглядные дашборды помогают оператору ИБ контролировать процесс и обработать инцидент в срок.

Кастомизация под процессы компании

Гибкая конфигурация системы позволяет выстроить управление инцидентами в соответствии с задачами компании: добавить дополнительные поля и фильтры, а также создать автоматические сценарии для обработки инцидентов.

PT Platform 187

PT Platform 187

программно-аппаратный комплекс для выполнения основных требования 187-ФЗ

- Платформа помогает реализовать меры защиты объектов КИИ в соответствии с требованиями ФСТЭК России и построить ведомственные центры ГосСОПКА в соответствии с требованиями ФСБ России.
- Продукты платформы регулярно получают обновления для выполнения новых требований регуляторов.

PT Platform 187

Подходит для небольших инфраструктур

Подходит организациям с инфраструктурой до 250 сетевых узлов и территориальным подразделениям крупных организаций как часть сегмента ГосСОПКА. Удобно использовать для постепенного масштабирования. Дает возможность поэтапно перейти на на enterprise-версии продуктов для мониторинга инфраструктуры.

Пять продуктов в одном

На сервере развернуты MaxPatrol SIEM, MaxPatrol 8, PT Network Attack Discovery, «ПТ Ведомственный центр», PT MultiScanner. Все продукты платформы уже интегрированы и обеспечивают максимальную совместимость компонентов.

Собственный мини-SOC из коробки

Платформа включает базовые технические средства, необходимые для SOC, и помогает выстроить процессы информационной безопасности, расширить внутреннюю экспертизу и повысить эффективность ИБ.

Решения
Positive Technologies

ptsecurity.com

Решения

Для раннего выявления сложных угроз

Для обеспечения безопасности объектов КИИ

Для построения центра ГосСОПКА

Комплексное решение

для раннего выявления сложных угроз – PT Anti-APT

Позволяет эффективно выявлять и предотвращать целевые атаки (APT). Помогает максимально быстро обнаружить скрытое присутствие злоумышленника в инфраструктуре и воссоздать полную картину атаки для эффективного расследования

Включает в себя:

PT Network Attack Discovery, PT Sandbox и услуги экспертного центра PT ESC

Подходит для:

Крупных холдингов, и корпораций с сетью филиалов

Преимущества

- Выявляет присутствие атакующего на периметре и в инфраструктуре
- Автоматически обнаруживает не выявленные ранее факты взлома инфраструктуры
- Использует уникальные технологии обнаружения атак в трафике
- Применяет передовой динамический анализ для выявления опасных файлов

Решения

Для раннего выявления сложных угроз

Для обеспечения безопасности объектов КИИ

Для построения центра ГосСОПКА

Комплексное решение
для обеспечения безопасности объектов КИИ

Позволяет построить системы безопасности объектов КИИ в соответствии с требованиями закона № 187-ФЗ. Обеспечивает выполнение требований и автоматизирует взаимодействие с ГосСОПКА. Может быть использовано в том числе для распределенных инфраструктур

Включает в себя:

MP SIEM, MP 8, PT NAD, PT MS, PT Sandbox, PT ISIM, PT AF, PT AI, ПТ ВЦ и услуги экспертного центра PT ESC

Подходит для:

Субъектов КИИ

Преимущества

- Позволяет выявлять атаки на ранней стадии и в ретроспективе
- Позволяет эффективно расследовать возникающие инциденты ИБ
- Позволяет непрерывно взаимодействовать с ГосСОПКА
- Позволяет соответствовать требованиям регулирующих органов

Решения

Для раннего выявления сложных угроз

Для обеспечения безопасности объектов КИИ

Для построения центра ГосСОПКА

Комплексное решение
для построения центра ГосСОПКА и взаимодействия с НКЦКИ

Позволяет поэтапно построить центр ГосСОПКА внутри субъекта КИИ. Помогает постепенно развивать внутреннюю экспертизу ИБ, выстраивать процессы в подразделении ИБ и успешно отражать как типовые атаки, так и новые их виды

Включает в себя:

MP SIEM, MP 8, PT NAD, PT MS, PT Sandbox, PT ISIM, PT AF, PT AI, ПТ ВЦ и услуги экспертного центра PT ESC

Подходит для:

Организаций, планирующих создание центра ГосСОПКА

Преимущества

- Наши продукты защищают критическую инфраструктуру крупнейших компаний
- Продукты имеют сертификаты соответствия ФСТЭК России*
- Все продукты входят в единую экосистему Positive Technologies
- Все продукты включены в единый реестр российского программного обеспечения

* PT ISIM и PT MS на сертификации

Услуги
Positive Technologies

ptsecurity.com

Сервисы 2.0:

услуги для непрерывного повышения защищенности бизнеса от киберугроз

Набор уникальных услуг по повышению защищенности бизнеса от киберугроз поможет непрерывно оценивать уязвимость компании перед действиями реальных злоумышленников и оперативно принимать меры по защите от кибератак и устранению последствий.

Сочетание сервисов моделирования сложных атак и услуг по выявлению угроз позволяет эффективно выстроить процессы обеспечения защиты ваших бизнес-процессов и свести к минимуму возможный финансовый и репутационный ущерб от кибератак.

Эмуляция APT-атаки

Поможет оценить и повысить устойчивость вашего бизнеса перед реальной кибератакой

Pentest 365

Обеспечит непрерывное выявление актуальных векторов кибератак на вашу компанию

Red team vs Blue team

Поможет в обнаружении угроз и совершенствовании стратегии реагирования на них

Услуги
мониторинга и реагирования на инциденты ИБ

Positive Technologies Expert Security Center — экспертное подразделение, оказывающее услуги по реагированию, расследованию инцидентов и мониторингу защищенности корпоративных систем на базе продуктов PT.

В основе наших услуг более 15 лет опыта в анализе защищенности, расследовании инцидентов и деятельности крупнейших APT-группировок, а также мониторинга безопасности крупных компаний.

Мониторинг периметра

Поможет непрерывно выявлять проблемы, возникающие на сетевом периметре компании

Поиск следов компрометации

Выявит следы подготовки к хакерской атаке и признаки компрометации инфраструктуры

Реагирование и расследование

Поможет оперативно локализовать угрозу и быстро восстановить работу бизнеса

Услуги
по глубокому анализу защищенности

Тестирование на проникновение
Поможет оценить риск и возможности проникновения злоумышленника в сеть компании

Анализ защищенности беспроводных сетей
Поможет повысить безопасность корпоративной Wi-Fi инфраструктуры

Анализ конфигураций сетевого оборудования
Поможет оценить и повысить безопасность настроек устройств сети

Оценка осведомленности пользователей
Поможет повысить готовность персонала к кибератакам

Анализ защищенности веб-приложений
Поможет существенно снизить риск успешной кибератаки как на внешний, так и внутренний периметр компании

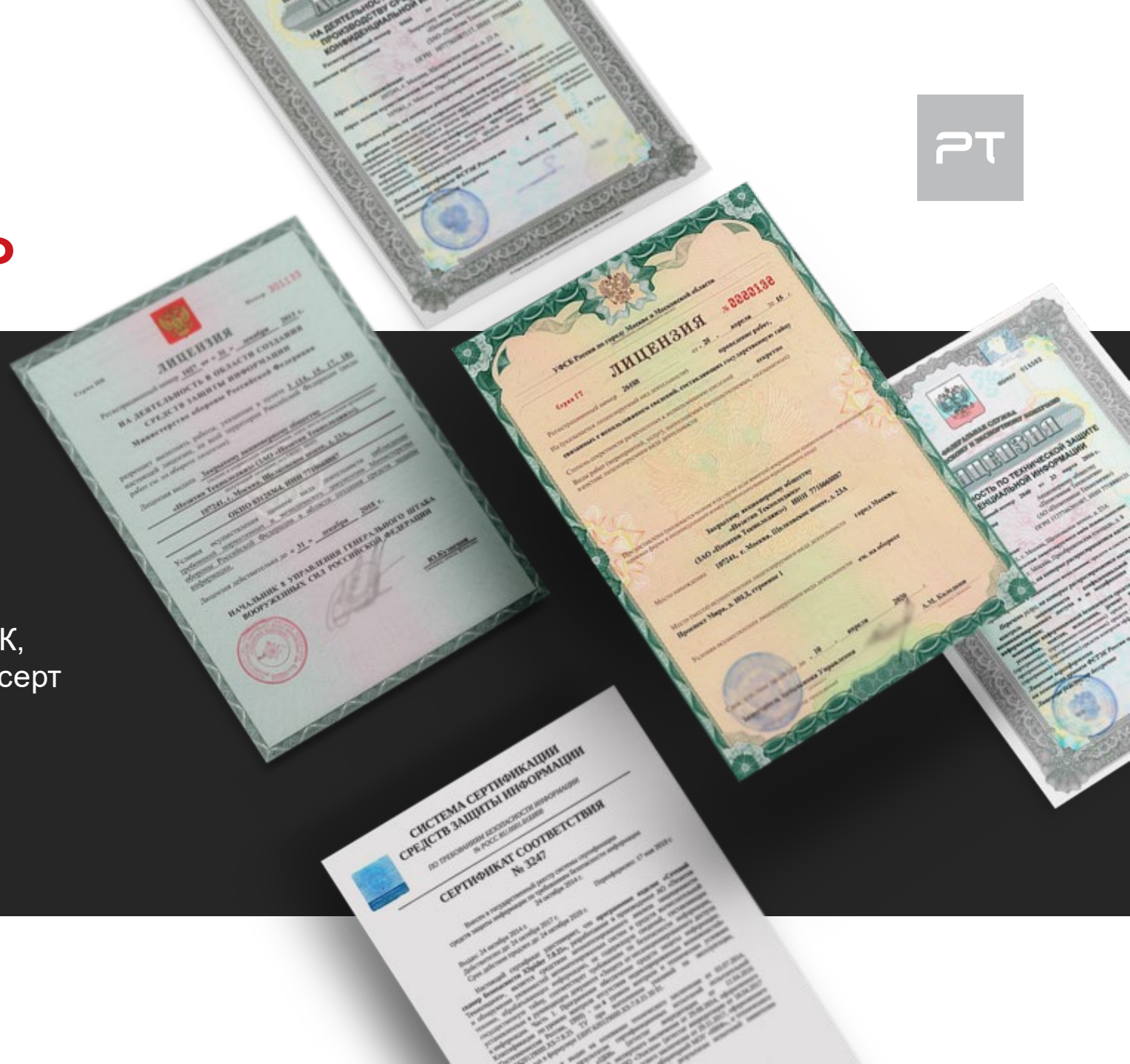
Анализ защищенности ERP-систем
Поможет оценить риски ИБ, связанные с критическими системами управления бизнесом

Анализ защищенности мобильных приложений
Поможет повысить защищенность данных ваших клиентов и предотвратить мошенничество

Лицензии и сертификаты

ptsecurity.com

Лицензии
на деятельность



- **Positive Technologies** — лицензиат ФСТЭК, ФСБ Министерства обороны РФ
- **Продукты сертифицированы** ФСТЭК, Министерством обороны РФ, Газпромсерт
- **Продукты компании** в Едином реестре российского ПО

Сертификаты

Сертификаты Министерства обороны

- **MaxPatrol 8** (№ 3750, действителен до 24 октября 2020 г.)
- **MaxPatrol SIEM** (№ 3044, действителен до 19 декабря 2023 г.)
- **PT Application Firewall** (№ 2619, действителен до 24 октября 2022 г.)

Сертификаты ФСТЭК

- **MaxPatrol 8** (№ 2922, действителен до 8 июля 2024 г.)
- **MaxPatrol SIEM** (№ 3734, действителен до 12 апреля 2025 г.)
- **PT Network Attack Discovery** (№ 4042, действителен до 30 ноября 2023 г.)
- **PT Application Firewall** (№ 3455, действителен до 27 октября 2021 г.)
- **PT Application Inspector** (№ 4000, действителен до 3 сентября 2023 г.)
- **PT ISIM** (№ 4182, действителен до 9 декабря 2024 г.)

Реестр российского ПО

- **MaxPatrol 8:** № 785
- **MaxPatrol SIEM:** № 1143
- **PT ISIM:** № 3424
- **PT MultiScanner:** № 1883
- **PT Application Firewall:** № 1141
- **PT Application Inspector:** № 1253
- **PT NAD:** № 4710

Зарубежные сертификаты

- **MaxPatrol 8** (№ BSI-DSZ-CC-0931-2015, Common Criteria)
- **MaxPatrol 8** (№ 1452619, соответствие требованиям СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006. ОУД 4, Республика Казахстан; действителен до 1 октября 2021 г.)
- **MaxPatrol SIEM** (№ 485, соответствие требованиям ТР 2013/027/BY, Республика Беларусь; действителен до 29 мая 2023 г.)
- **MaxPatrol SIEM** (№ 1452620, соответствие требованиям СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006. ОУД 4, Республика Казахстан; действителен до 1 октября 2021 г.)
- **PT ISIM** (№ 1452622, соответствие требованиям СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006. ОУД 4, Республика Казахстан; действителен до 1 октября 2021 г.)
- **PT Application Firewall** (№ 1452618, соответствие требованиям СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006. ОУД 4, Республика Казахстан; действителен до 1 октября 2021 г.)
- **PT Application Firewall** (№ 181005R00, ICSA Labs от 23 февраля 2018 г.)
- **PT Application Inspector** (№ 1452621, соответствие требованиям СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006. ОУД 4, Республика Казахстан; действителен до 1 октября 2021 г.)
- **PT MultiScanner** (№ 1452623, соответствие требованиям СТ РК ГОСТ Р ИСО/МЭК 15408-3-2006. ОУД 4, Республика Казахстан; действителен до 1 октября 2021 г.)

Свяжитесь с нами:

+7 (495) 744-01-44
sales@ptsecurity.com

ptsecurity.com