Результативный подход к кибербезопасности

positive technologies

ТЕХНОЛОГИЧНО ПРЕДОТВРАЩАЕМ НЕДОПУСТИМОЕ ДЛЯ БИЗНЕСА И ГОСУДАРСТВА

ptsecurity.com

Узнайте, как защитить ваш бизнес
от современных киберугроз

ПРОДУКТЫ

ptsecurity.com

Официальный канал в Телеграм

Официальный канал в VK

Официальный канал на Хабр

It's positive investing

Positive Technologies — лидер рынка результативной кибербезопасности.

Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 180 тысяч акционеров.

Более чем за 20 лет работы компания выработала визионерский подход к созданию своих решений. Метапродукты Positive Technologies меняют индустрию и радикально повышают защищенность компаний, а через них — отраслей и государств. Так результативная кибербезопасность становится доступна любой организации в мире.

При разработке решений Positive Technologies опирается на многолетнюю практику и уникальные знания сотрудников исследовательского центра — одного из крупнейших в мире. В нем работают белые хакеры (white hats), исследующие защищенность различных систем, и эксперты по кибербезопасности, которые расследуют реальные инциденты и знают, как атакуют злоумышленники. Продукты компании соответствуют российским и международным стандартам безопасности, в том числе PCI DSS и ЦБ РС БР ИББС-2.6-2014, приказам ФСТЭК № 17 и 21.

Данный каталог содержит полный перечень наших продуктов, решений и экспертных сервисов, которые помогут выстроить надежную защиту вашей компании от кибератак..

Заказать бесплатный пилот продукта или решения, а также запросить консультацию по услугам вы можете, отправив заявку на sales@ptsecurity.com.

MAXPATROL O2

Автопилот для результативной кибербезопасности

1. **Обнаруживает злоумышленника и определяет, до каких ресурсов ему удалось добраться.**
2. **Прогнозирует сценарий развития атаки с учетом недопустимых для компании событий.**
3. **Останавливает атаку до того, как компании будет нанесен непоправимый ущерб.**

ОСНОВНАЯ ЗАДАЧА

Сделать невозможной реализацию недопустимых для бизнеса событий.

Снижает порог вхождения в мир результативной кибербезопасности

Позволяет компаниям решать задачи результативной кибербезопасности без расширения штата экспертов и траты ресурсов на автоматизацию процессов в SOC.

Автоматизирует работу SOC

Снижает влияние человеческого фактора в процессах обнаружения, расследования и реагирования на инциденты, автоматизирует рутинные действия аналитиков.

Знает, как действует злоумышленник

Использует уникальный опыт Positive Technologies и экспертизу команд PT SWARM и PT ESC, накапливаемые в регулярных киберучениях, Bug Bounty Positive Dream Hunting* и Standoff.

Экосистема Positive Technologies

Объединяет продукты Positive Technologies, которые работают как сенсоры, обмениваются знаниями и обеспечивают комплексную защиту IT-систем компании с минимальным вовлечением человека в процесс.

*Уникальная BugBounty-программа Positive Technologies, ориентированная не на поиск сугубо технических уязвимостей во внешних сервисах компании, а на реализацию недопустимых событий для бизнеса.

MAXPATROL SIEM

MaxPatrol SIEM гарантированно выявляет инциденты ИБ, ведущие к реализации недопустимых событий, и попытки нарушения киберустойчивости компании

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Показывает быстрый результат без дополнительных вложений в настройку и доработку системы.
- Дает полную видимость IT-инфраструктуры.
- Обеспечивает производительность, стабильность и масштабируемость enterprise-уровня.

Лидирующее отечественное SIEM-решение

Зрелый продукт масштаба страны — внедрен более чем в 600 промышленных, транспортных, финансовых частных и государственных компаниях.

Регулярно получает экспертизу для обнаружения угроз

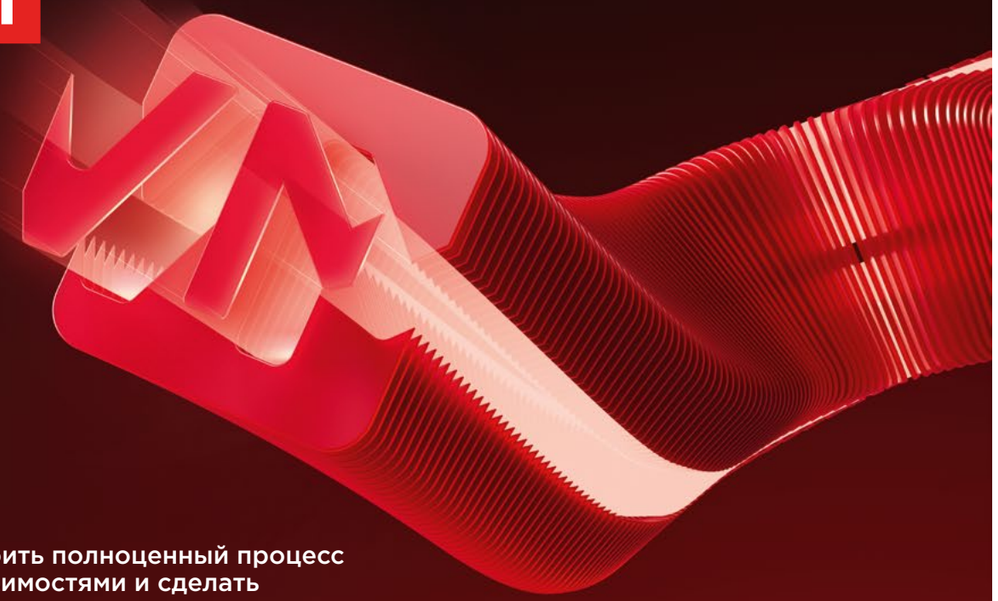
MaxPatrol SIEM пополняется пакетами экспертизы с новыми правилами корреляции каждый месяц.

Быстро развивается и становится проще

Выпускаем два релиза в год, регулярно внедряем новые технологии и расширяем команду разработки. Постоянно упрощаем продукт, чтобы развернуть MaxPatrol SIEM и выявлять угрозы мог даже специалист без опыта работы с системой.

MAXPATROL VM

Система управления уязвимостями



ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- **Поможет выстроить полноценный процесс управления уязвимостями и сделать проникновение в сеть сложным и дорогим для злоумышленника.**
- **Вовремя покажет, какие уязвимости используют атакующие, благодаря гарантированной доставки трендов за 12 часов.**

Сокращает время работы с уязвимостями

Проводит глубокую проверку систем и помогает автоматизировать управление уязвимостями с учетом значимости компонентов сети для бизнес-процессов.

Позволяет быстрее реагировать на новые опасные уязвимости

Выявляет наличие уязвимости на основе ранее собранной информации об активах инфраструктуры, что позволяет перейти к этапу ее устранения или применения компенсирующих мер без повторного сканирования.

Делает процессы более прозрачными

Позволяет создавать регламенты для сканирования и устранения уязвимостей. Дашборды системы наглядно демонстрируют работу отделов ИТ и ИБ, позволяя контролировать уровень защищенности инфраструктуры и сроки устранение уязвимостей.

Делает систему максимально сложной для проникновения

Эксперты Positive Technologies оперативно сообщат об уязвимостях, которые необходимо закрыть в первую очередь. Информация о трендовых уязвимостях доставляется в продукт за 12 часов.

MAXPATROL HCC

Модуль контроля соответствия стандартам

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Проверяет конфигурации систем в IT-инфраструктуре на соответствие российским и международным стандартам ИБ, а также внутренним политикам компании.
- Помогает выстроить процесс комплаенс-контроля и приоритизировать обнаруженные риски в зависимости от важности активов и применяемых к ним требований.

Фокусирует внимание на самых важных требованиях

Включает критически важные стандарты PT Essentials, которые содержат оптимальный набор проверок для повышения защищенности инфраструктуры.

Позволяет быстро реагировать на изменения требований

Автоматически оценивает соответствие узлов сети новым требованиям, не требуя повторного сканирование активов.

Помогает выстроить процесс

Позволяет настроить политику устранения несоответствий и легко контролировать соблюдение регламентированных сроков на главном дашборде.

MAXPATROL EDR

Продукт для защиты устройств компании и сотрудников от сложных и целевых атак

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Своевременно выявлять угрозы на узлах и реагировать на них.
- Автоматизировать рутинные задачи специалистов SOC по противодействию киберугрозам.

Обнаруживает угрозы в динамике

Обнаруживает атаки с использованием легитимных инструментов, которые могут пропустить традиционные средства защиты, основанные на сигнатурном анализе.

Своевременно и непрерывно обнаруживает ВПО

Проводит статический и динамический анализ на устройствах. Способен выявлять угрозы и популярные тактики и техники злоумышленников из матрицы MITRE ATT&CK (топ-50 для Windows и топ-20 для Linux).

Молниеносно реагирует на узлах

Предоставляет богатый выбор действий для автоматического или ручного реагирования.

Поддерживает широчайший набор ОС

Автономный агент позволяет защищать Windows, Linux и macOS устройства, включая отечественные ОС.

PT SANDBOX

Экспертная песочница для защиты от новейших и актуальных угроз

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- **Обнаруживает сложное вредоносное ПО, которое могут пропустить классические средства защиты.**
- **Работает в режиме блокировки на всех источниках, где это применимо, снижая риск реализации атаки с помощью ВПО до нуля.**

Гарантирует защиту от неизвестного ВПО индивидуально для каждой отрасли за счет кастомизированных виртуальных сред, в которые можно добавлять специфический софт и его версии. Также в продукте используются «обманки»: фейковые файлы, процессы и данные, которые провоцируют вредоносное ПО совершить активные действия и выдать себя.

Использует множество источников для обнаружения попытки злоумышленников закрепиться в любом сегменте инфраструктуры и причинить ущерб бизнесу.

Получает информацию от PT ESC за 2,5 часа, обеспечивая высочайшую актуальность защиты от нового и ранее не известного вредоносного ПО.

Защищает инфраструктуру от целевых и массовых атак за счет комбинации методов обнаружения ВПО: поведенческого анализа с настраиваемым машинным обучением, статического анализа несколькими антивирусами и проверки правилами PT ESC.

PT NEXT-GENERATION FIREWALL

Межсетевой экран нового поколения с высоким уровнем производительности и надежности

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Обработка больших объемов трафика, расшифровка и инспектирование протоколов SSL и TLS в режиме реального времени без замедления работы сети.
- Централизованное управление: хранение и редактирование политик безопасности для 10 000 устройств.
- Высокая стабильность работы и масштабируемость.
- Линейка устройств для защиты периметра — от 100 Мбит/с до 10 Гбит/с.
- Линейка устройств для ЦОД — до 100 Гбит/с.

Быстрый стек TCP/IP

Инженеры Positive Technologies самостоятельно реализовали стек протоколов по модели TCP/IP и нулевое копирование для пакетной обработки. Это позволит PT NGFW достигать высокой производительности при передаче, обработке и инспекции трафика без применения специализированных аппаратных платформ.

Аппаратные платформы с архитектурой x86

PT NGFW разрабатывается для работы на универсальных аппаратных платформах с архитектурой процессора x86. Это позволит использовать межсетевой экран на оборудовании различных производителей, включая отечественные решения из реестров ТОРП и РЭП.

Иерархия объектов и правил

Логическое разделение системы управления позволит максимально оптимизировать политики безопасности в соответствии с бизнес-процессами компании, при этом увеличение количества устройств не потребует значительного роста трудозатрат на их администрирование и настройку.

Интеграция с экосистемой Positive Technologies

Тесное взаимодействие PT NGFW с системами MaxPatrol SIEM, PT Sandbox, PT Network Attack Discovery и другими позволит оперативно реагировать на инциденты и минимизировать их влияние на сеть и бизнес.

PT NETWORK ATTACK DISCOVERY

PT NAD — система поведенческого анализа сетевого трафика (NTA), вовремя замечает атакующего внутри сети и цепочку его перемещений, которые могут привести к реализации недопустимых событий

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Легко внедряется и делает сеть прозрачной для специалистов по ИБ и ИТ.
- Обнаруживает попытки злоумышленника проникнуть в сеть или расширить свое присутствие в инфраструктуре.
- Является обязательным инструментом аналитиков SOC для проактивного поиска угроз и расследований.

Собственная технология DPI

Детально разбирает корпоративный сетевой трафик на любых скоростях и помогает точно обнаружить присутствие злоумышленника внутри сети.

Передовые технологии выявления угроз

Поведенческие и статистические модули PT ESC за несколько минут обнаруживают сложные угрозы, которые невозможно увидеть классическими методами. PT NAD видит вредоносную активность даже в зашифрованном трафике.

Является основой для современного SOC и threat hunting

Помогает восстановить хронологию атак, понять источник и масштабы угрозы за счет удобной работы с исходным трафиком и обработанными данными. Позволяет проверять гипотезы и проактивно искать угрозы в трафике.

PT ISIM

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

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Помогает на ранней стадии выявлять кибератаки и неавторизованные действия сотрудников.
- 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.

Непрерывно инвентаризирует и профилирует сеть

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

Обнаруживает угрозы и аномалии с высокой точностью

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

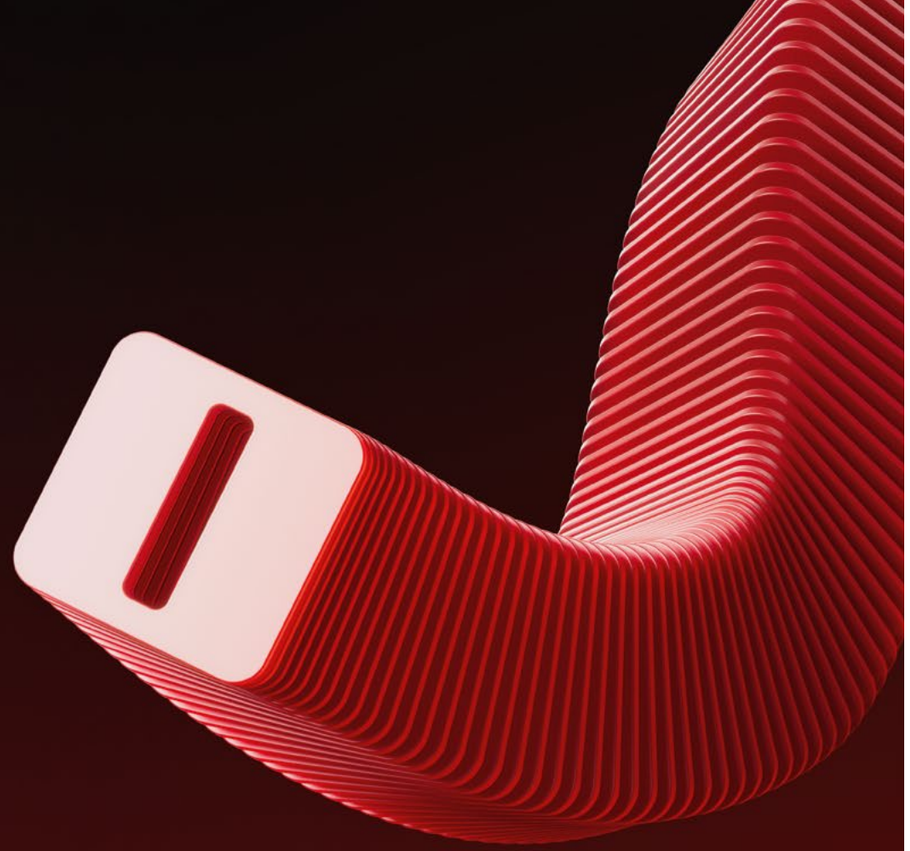
Анализирует и хранит весь спектр трафика технологической сети: от IT- до промышленных протоколов. Благодаря встроенным инструментам работы с метаданными продукт предоставляет широкие возможности для специализированного поиска угроз (threat hunting) и расследования инцидентов информационной безопасности 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 APPLICATION FIREWALL

Межсетевой экран уровня веб-приложений (web application firewall)



ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

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

Быстрый старт и интеграция

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 с антивирусными системами, SIEM, Anti-DDoS, DLP.

Простота использования

Снижает трудозатраты оператора ИБ за счет встроенных политик защиты, механизмов корреляции и приоритизации найденных угроз.

Адаптация к изменениям

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

Инструмент для выявления уязвимостей и ошибок в приложениях, поддерживающий процесс DevSecOps

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

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

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 использования

Не требует установки и настройки приложения или доступа к тестовой среде. Просто укажите папку, содержащую готовый код приложения (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.

PT BLACKBOX

Доступный и простой в использовании инструмент динамического анализа защищенности приложений, который позволяет найти и устранить уязвимости на этапе тестирования и доставки программного обеспечения

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Выявляет уязвимости в веб-приложениях на ранней стадии разработки программного обеспечения.
- Составляет отчет с рекомендациями по устранению уязвимостей.
- Позволяет предотвращать такие атаки, как внедрение SQL-кода, XSS, RCE и другие.

Экономит ресурсы

Определяет повторяющиеся шаблонные страницы и не тратит время пользователя на сканирование каждой из них по отдельности.

Обнаруживает скрытые веб-страницы

Комбинация сигнатурного и эвристического анализа позволяет находить тестовые или административные разделы.

Интегрируется в жизненный цикл программного обеспечения

Позволяет эффективно обнаруживать и исправлять уязвимости на ранней стадии разработки программного обеспечения.

Настраивается индивидуально под требования заказчика

Дает возможность самостоятельно задавать параметры сканирования.

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
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.

PT XDR

Решение класса eXtended Detection and Response для точного обнаружения и реагирования на сложные угрозы и целевые атаки

В состав решения входят продукты:

MaxPatrol EDR | MaxPatrol VM | MaxPatrol SIEM | PT Sandbox

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Обеспечивает своевременное обнаружение и реагирование в случае атак на конечные точки.
- Осуществляет надежный сбор данных со всех источников в инфраструктуре.
- Комбинирует инструменты обнаружения угроз для выявления самых сложных векторов атак.
- Автоматизирует реагирование на типовые угрозы, позволяя специалистам SOC сосредоточиться на решении больших задач.

Полный контекст

Собирает события и контекст из множества систем информационной безопасности, расширяя зону мониторинга от конечного устройства до всей сети.

Комплексный анализ

Объединяет экспертизу нескольких продуктов, обеспечивающих всестороннюю защиту конечных точек: выявление инцидентов, уязвимостей и вредоносного ПО.

Уверенное реагирование на узлах

Позволяет принимать обоснованные решения, базирующиеся на результатах всестороннего анализа и обработки событий с помощью продуктов, входящих в состав.

Для защиты промышленных предприятий — PT Industrial Cybersecurity Suite

Платформа для защиты промышленности от киберугроз.
Позволяет обнаруживать действия злоумышленника на всех этапах развития атаки в промышленных средах и своевременно реагировать на них.

PT ICS обеспечивает комплексную безопасность в индустриальном сегменте компании: от сетевых узлов до технологических устройств.

Включает в себя:

PT ISIM и промышленные версии продуктов PT Sandbox, PT XDR, MaxPatrol VM, MaxPatrol SIEM.

Подходит для:

Любых промышленных компаний.

Преимущества

- Подходит для любых отраслей промышленности: энергетики, транспорта, металлургии, машиностроения, медицины, ЖКХ и т. д.
- Легко масштабируется от одной производственной площадки до размеров промышленного холдинга или целой отрасли.
- Отечественное решение: все продукты в составе платформы — полностью российского производства и входят в реестр отечественного ПО.

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. Платформа PT ICS может быть использована для распределенных инфраструктур.

Включает в себя:

MaxPatrol SIEM, MaxPatrol 8, PT NAD, PT MS, PT Sandbox, PT ISIM, PT AF, PT AI, ПТ Ведомственный центр и услуги 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.

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 по ИБ и успешно отражать как типовые атаки, так и новые их виды.

Включает в себя:

MaxPatrol SIEM, MaxPatrol 8, PT NAD, PT MS, PT Sandbox, PT ISIM, PT AF, PT AI, ПТ Ведомственный центр и услуги PT ESC.

Подходит для:

Организаций, планирующих создание центра ГосСОПКА.

Преимущества

- 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 отечественного ПО.

СЕРВИСЫ

ptsecurity.com

Услуги для повышения защищенности от киберугроз

Услуги для повышения защищенности от киберугроз помогут оценить готовность компании к противостоянию злоумышленникам, оперативно принимать меры для защиты от кибератак и устранения их последствий. Сочетание услуг по выявлению угроз и сервисов моделирования сложных атак позволит выстроить эффективную защиту бизнес-процессов, минимизировать возможный финансовый и репутационный ущерб от взлома.

Анализ защищенности веб-приложений

Поможет выявить существующие уязвимые места веб-приложения и получить объективную независимую оценку уровня его защищенности.

Анализ защищенности мобильных приложений

Поможет выявить существующие уязвимые места мобильного приложения и определить уязвимости и риски, которые с этим связаны.

Анализ защищенности систем дистанционного банковского обслуживания

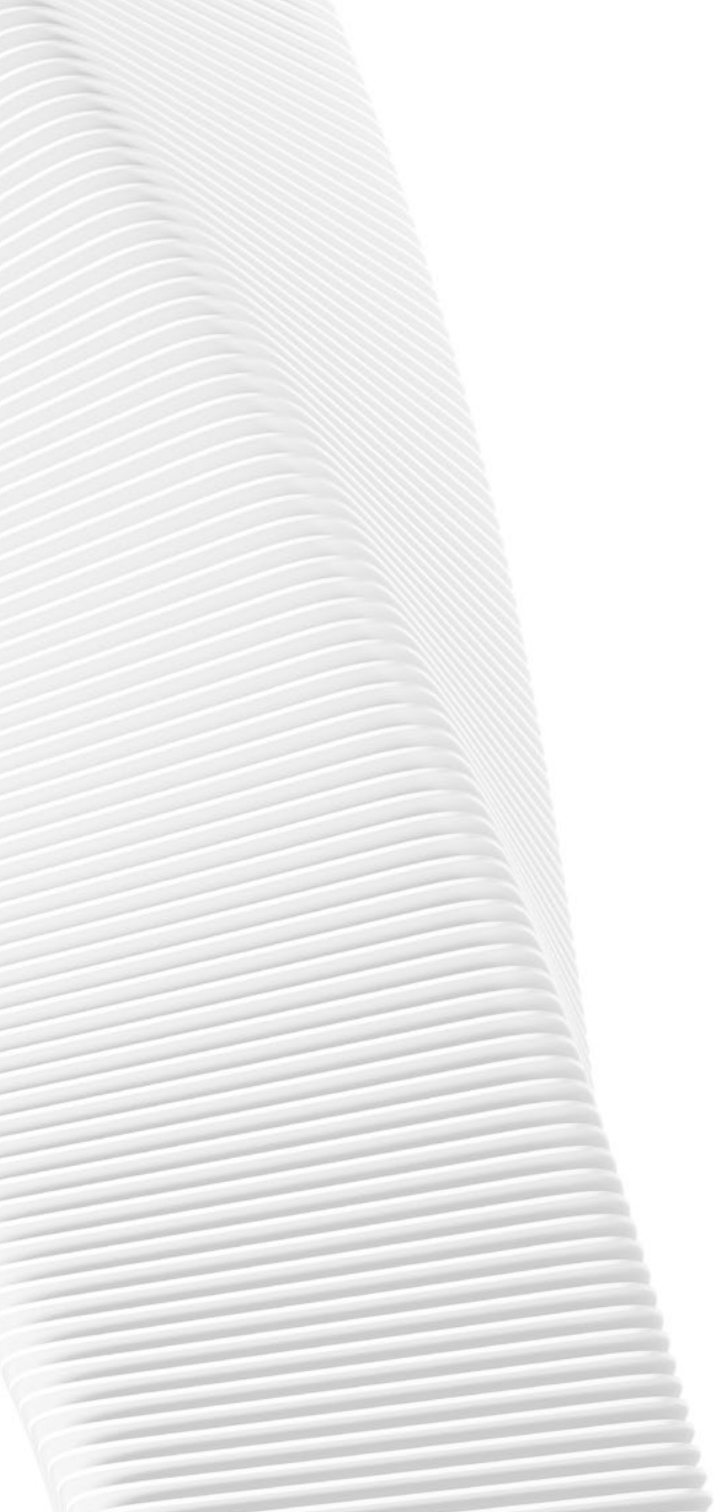
Поможет получить объективную оценку текущего уровня защищенности системы ДБО и своевременно выявить основные проблемы защиты и оперативно разработать механизмы их решения.

Реагирование и расследование инцидентов

Помогает оперативно установить все обстоятельства инцидента и устранить его последствия.

Ретроспективный анализ инфраструктуры и выявление следов компрометации

Позволяет выявить факторы компрометации объектов инфраструктуры организации, ранее не зафиксированных штатными системами защиты.



ptsecurity.com