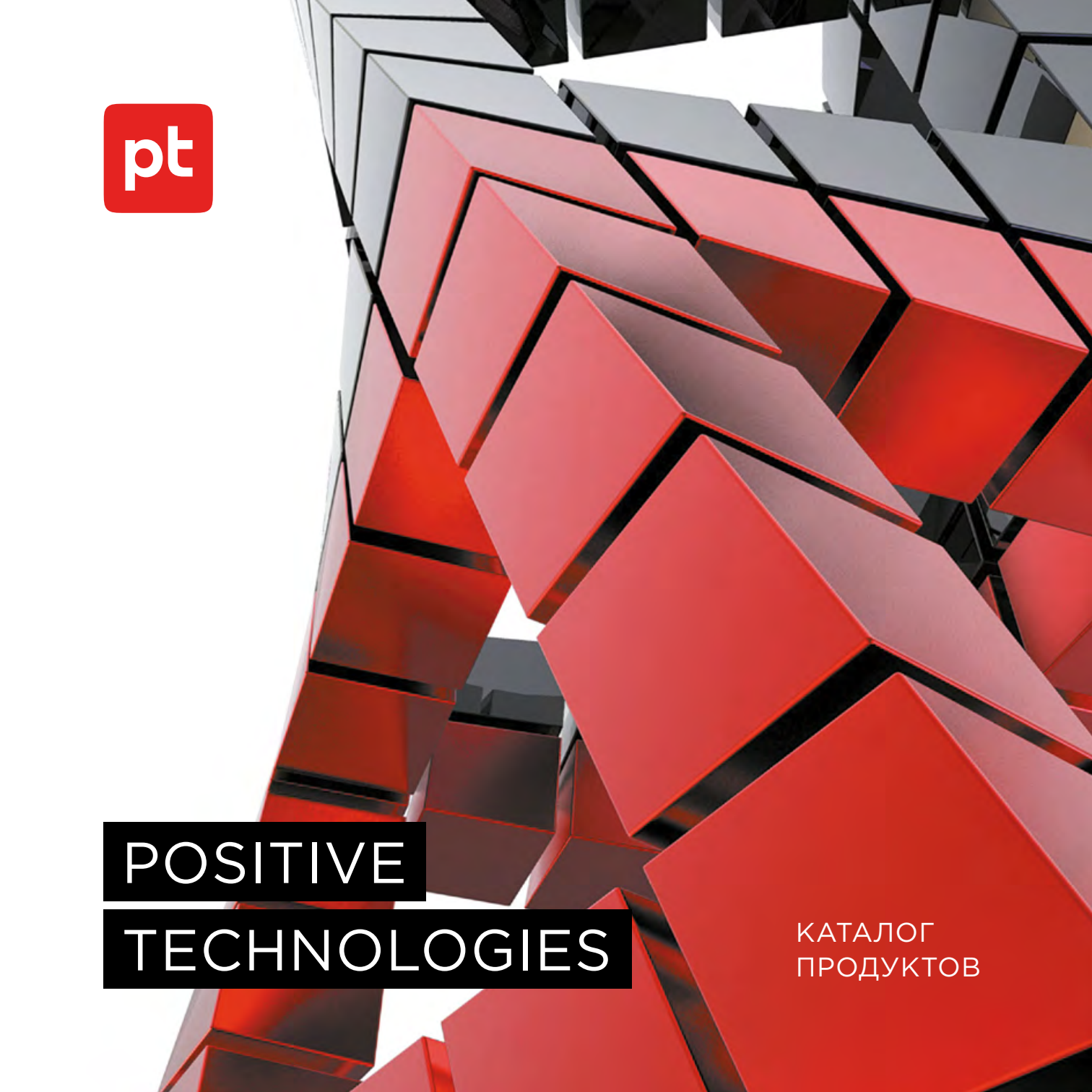


POSITIVE TECHNOLOGIES

КАТАЛОГ ПРОДУКТОВ

ПОЗИТИВНЫЙ ПОДХОД К КИБЕРБЕЗОПАСНОСТИ

Узнайте, как защитить ваш бизнес
от современных киберугроз

ptsecurity.com

ПРОДУКТЫ

ptsecurity.com

На странице каждого продукта вы можете узнать о сложности его внедрения и использования.

СЛОЖНОСТЬ ВНЕДРЕНИЯ

НИЗКАЯ
Можно внедрить самостоятельно

СРЕДНЯЯ
Может внедрить партнер

ВЫСОКАЯ
Может внедрить Positive Technologies

СЛОЖНОСТЬ ИСПОЛЬЗОВАНИЯ

НАЧАЛЬНЫЙ УРОВЕНЬ

СРЕДНИЙ УРОВЕНЬ

ЭКСПЕРТНЫЙ УРОВЕНЬ

Positive Technologies уже 19 лет создает инновационные решения в сфере информационной безопасности.

Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяет более 2000 компаний в 30 странах мира. В числе наших клиентов 80% участников рейтинга «Эксперт 400» в России и более двухсот зарубежных компаний.

Данный каталог содержит полный перечень наших продуктов, комплексных 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 SIEM

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

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Выявление сложных угроз и атак, составление комплексной картины происходящего в IT-инфраструктуре
- Снижение трудозатрат экспертов ИБ на мониторинг состояния инфраструктуры и написание правил

Выявляет даже самые новые угрозы

Знания экспертов PT регулярно передаются в базу PT Knowledge Base в виде пакетов экспертизы. Пользователи MaxPatrol SIEM получают пакеты из PT KB, что помогает детектировать актуальные техники и тактики атак до наступления последствий и снижает потребность в специалистах ИБ.

Дает детальную информацию об инфраструктуре

Уникальная технология детальной инвентаризации дает MaxPatrol SIEM подробную информацию о каждом активе и уязвимых местах, показывая оператору ИБ, что происходит в инфраструктуре. Из коробки доступна поддержка 300+ различных систем, включая большой спектр российского ПО.

Работает в сетях любого масштаба

Среди 250+ внедрений MaxPatrol SIEM присутствуют: серверы с нагрузкой до 60 000 событий в секунду; иерархические инсталляции по всей территории РФ (до 15 подчиненных серверов); геораспределенные кластеры; сложные системы отчетности и мониторинга источников событий.

MAXPATROL VM

Система нового поколения
для управления уязвимостями

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Выстроить полноценный процесс управления уязвимостями, результаты которого видны
- Контролировать защищенность IT-инфраструктуры в каждый момент времени и правильно приоритизировать работу над уязвимостями

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 быстро 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.

Повышает защищенность компании от реальных угроз

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

PT SANDBOX

Песочница для риск-ориентированной защиты от целевых атак

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Обеспечение защиты от целевых атак с применением неизвестного вредоносного ПО и угроз нулевого дня
- Централизованное выявление угроз в почте, файловых хранилищах, веб-трафике, корпоративных системах и на веб-порталах
- Персонализация защиты в зависимости от ключевых бизнес-рисков компании

Воспроизводит реальную инфраструктуру

Продукт позволяет точно имитировать реальные рабочие станции компании: дает возможность добавить в виртуальную среду специфическое ПО, которые используют сотрудники, содержит «приманки», провоцирующие атакующих выдать себя.

Проводит глубокий анализ файлов

Каждый файл проходит комплексную проверку, включающую статический и динамический анализ с помощью уникальных правил PT Expert Security Center, а также проверку антивирусами.

Обнаруживает угрозы не только в файлах, но и в трафике

PT Sandbox проверяет на наличие угроз весь трафик, который генерируется в процессе анализа подозрительного файла, а также расшифровывает TLS-трафик, выявляя в нем вредоносную активность.

PT NETWORK ATTACK DISCOVERY

Система анализа сетевого трафика (NTA) для выявления атак и их расследования

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Обеспечение прозрачности сети и получение подробной картины активности в инфраструктуре
- Повышение эффективности работы SOC, упрощение реагирования на инциденты и расследования атак
- Выявление сложных атак в трафике по большому количеству признаков

Видит опасную активность во внешнем и внутреннем трафике

PT NAD определяет 85 протоколов, разбирает до уровня L7 включительно 30 наиболее распространенных из них и позволяет получить полную картину активности как на периметре, так и внутри инфраструктуры.

Использует передовые технологии выявления угроз

Для выявления атак на ранних стадиях продукт использует технологии машинного обучения, глубокую аналитику, собственные правила детектирования угроз, индикаторы компрометации и ретроспективный анализ.

Выявляет присутствие угроз по множеству признаков

Продукт обнаруживает вредоносное ПО в зашифрованном трафике, горизонтальное перемещение злоумышленника, скрытые каналы (туннелирование), коммуникацию с автоматически сгенерированными доменами, эксплуатацию уязвимостей и хакерский инструментарий.

PT APPLICATION FIREWALL

Межсетевой экран
уровня веб-приложений
(Web Application Firewall, WAF)

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Обеспечение непрерывности бизнес-процессов и соответствия стандартам
- Обеспечение всесторонней и непрерывной защиты веб-приложений, в том числе постоянно обновляемых, а также защиты пользователей и инфраструктуры

Блокирует массовые и целевые атаки

Благодаря комбинации защитных механизмов и экспертизе Positive Technologies, PT Application Firewall обеспечивает комплексную защиту от известных угроз и атак нулевого дня.

Быстро встраивается в инфраструктуру

PT Application Firewall имеет встроенный мастер настройки и предустановленные шаблоны политик безопасности, благодаря которым его легко установить и использовать.

Адаптируется под защищаемые приложения

PT Application Firewall сочетает в себе «коробочность» и возможности тонкой настройки, что позволяет ему работать одновременно с большим числом приложений разной степени сложности и значимости.

PT APPLICATION INSPECTOR

Инструмент для тестирования безопасности приложений (Application Security Testing, AST)

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Выявление уязвимостей в исходном коде приложения
- Построение процесса безопасной разработки (Secure SDL, DevSecOps)

Точно находит и приоритизирует уязвимости

PT Application Inspector обнаруживает не только сами уязвимости, но и условия их эксплуатации благодаря комбинации механизмов выявления и экспертизе Positive Technologies.

Прост в использовании

Чтобы начать анализ, не нужно настраивать приложение и получать доступ к среде. Просто укажите папку с исходным кодом.

Интегрируется в действующие 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 ISIM

Программно-аппаратный комплекс, обеспечивающий непрерывный мониторинг защищенности сети АСУ ТП

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Обеспечение контроля над векторами атак и соблюдением политик ИБ, специфических для конкретного промышленного объекта
- Выявление кибератак и неавторизованных действий персонала на ранних стадиях
- Эффективное расследование кибератак и инцидентов за счет полного анализа технологического трафика

Непрерывно инвентаризирует и профилирует сеть

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

С высокой точностью детектирует угрозы и аномалии

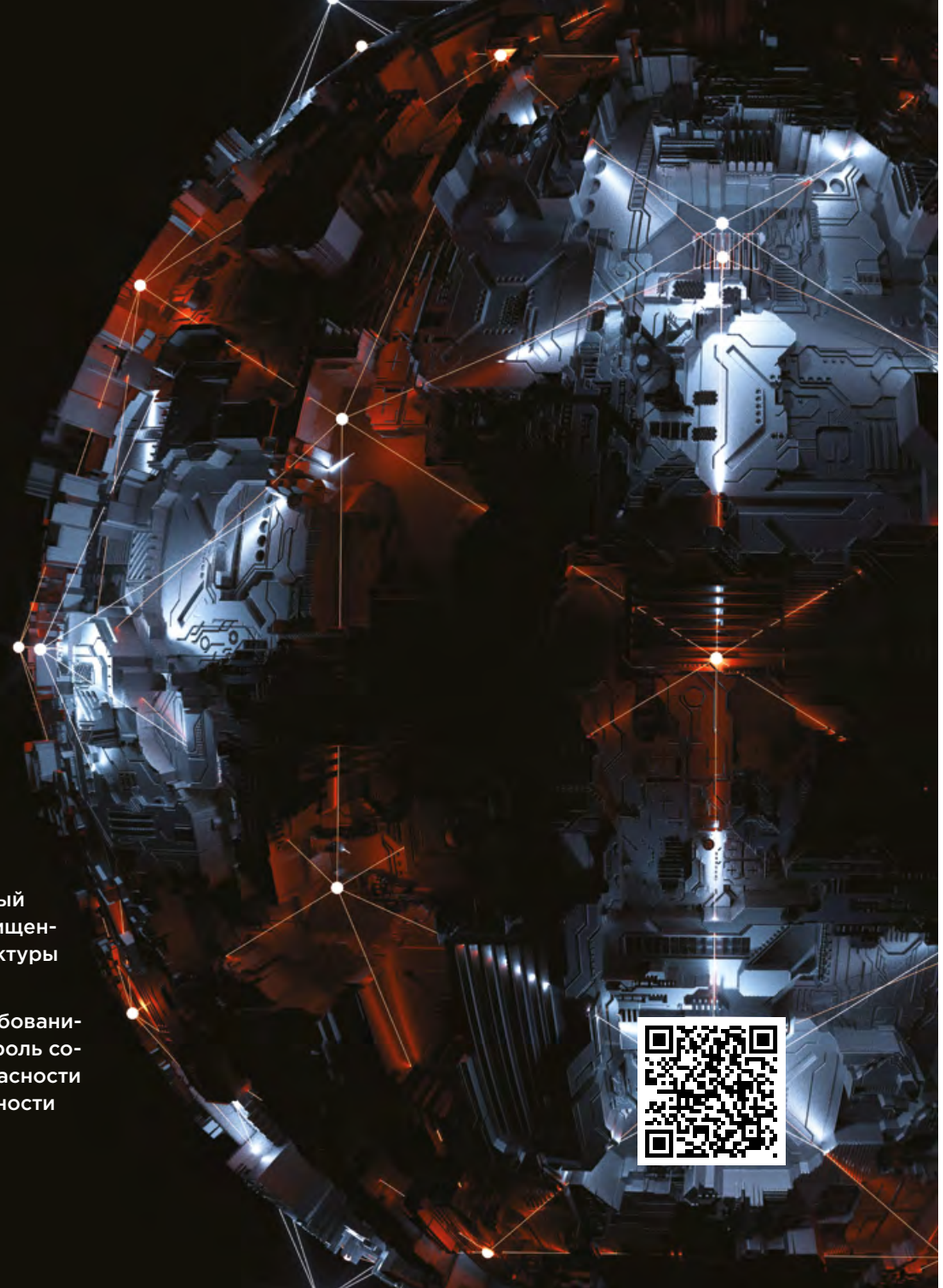
PT ISIM использует собственную базу данных индикаторов промышленных угроз (PT ISTI) и благодаря комбинации сигнатурных методов обнаружения атак и механизма поведенческого анализа позволяет эффективно выявлять кибератаки на ранней стадии.

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.

MAXPATROL 8

Универсальное средство автоматизированного анализа защищенности и контроля соответствия стандартам



ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Регулярный и комплексный контроль состояния защищенности всей IT-инфраструктуры
- Оценка соответствия требованиям стандартов ИБ и контроль соблюдения политик безопасности различной степени сложности

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 информационных систем, проверяет соответствие настроек информационных систем требованиям ИБ. Использует методы черного и белого ящика 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). Поддерживает проверку на соответствие 180+ техническим стандартам безопасности. Также позволяет настроить специальные политики для контроля выполнения собственных корпоративных правил безопасности.

PT MULTISCANNER

Многоуровневая система защиты от вирусных угроз

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Обеспечение мультивендорной антивирусной защиты IT-инфраструктуры
- Обеспечение эффективного реагирования благодаря быстрой локализации вирусных угроз

Защищает от массовых угроз

Продукт проверяет каждый файл с помощью нескольких антивирусов и набора индикаторов компрометации, регулярно пополняемого экспертами PT ESC в ходе расследований инцидентов в крупных компаниях.

Следит за всеми потоками данных

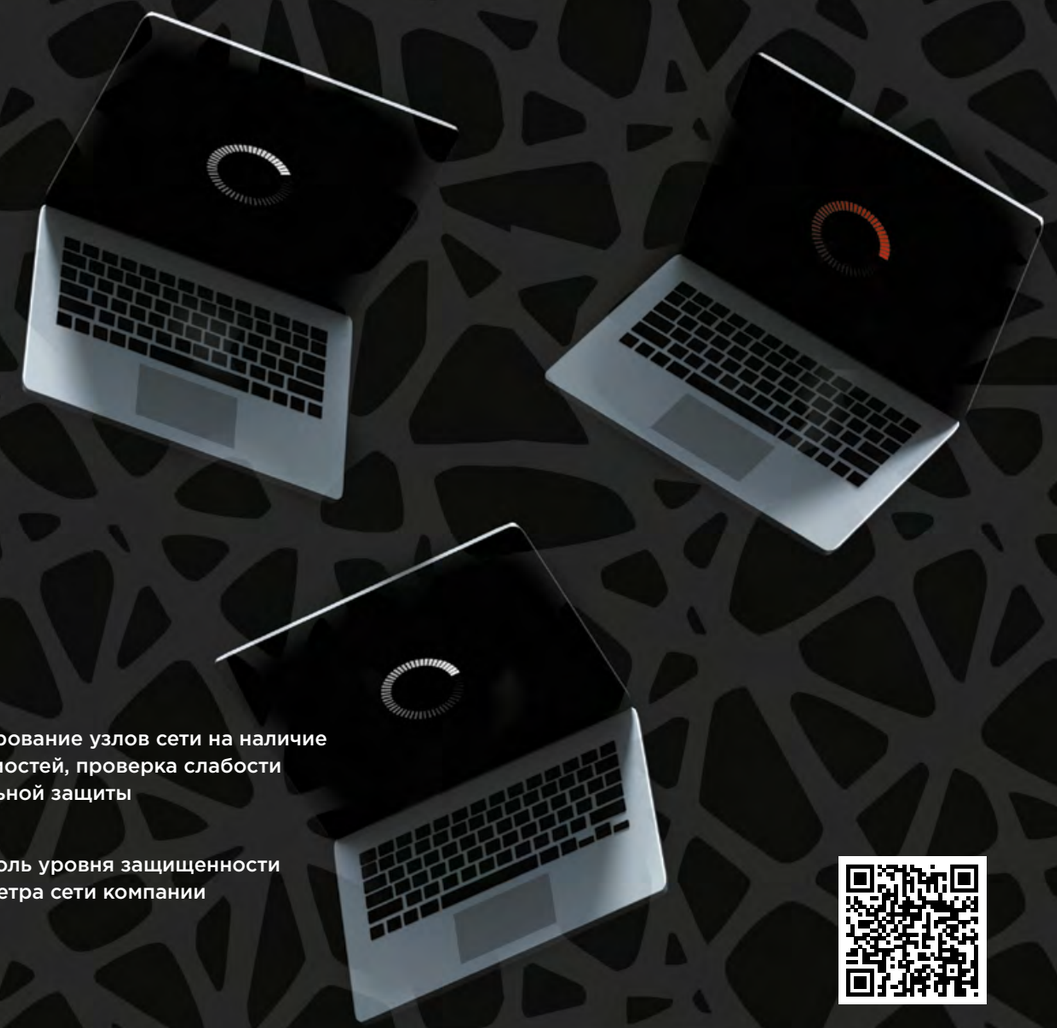
Продукт анализирует на наличие угроз файлы, которые попадают в корпоративную сеть в сетевом и почтовом трафике, загружаются в веб-приложения и файловые хранилища компании.

Выявляет атаки, не замеченные в прошлом

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

XSPIDER

Профессиональный
сканер уязвимостей



ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Сканирование узлов сети на наличие уязвимостей, проверка слабости парольной защиты
- Контроль уровня защищенности периметра сети компании

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.

PT PLATFORM 187

Решения по кибербезопасности
для небольших инфраструктур

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Построение основных процессов информационной безопасности и значительное повышение их эффективности
- Реализация функций безопасности значимых объектов КИИ и построение взаимодействия с главным центром ГосСОПКА

Подходит для небольших инфраструктур

Подходит организациям с инфраструктурой до 500 сетевых узлов. Удобно использовать для постепенного масштабирования. Дает возможность поэтапно перейти на enterprise-версии продуктов для мониторинга инфраструктуры.

Пять конфигураций решения

Каждая конфигурация включает в себя набор технических средств для реализации основных функций безопасности компании. Все продукты уже интегрированы и обеспечивают максимальную совместимость компонентов. Состав комплекса подбирается с учетом требований заказчика и особенностей его инфраструктуры.

Позволяет соответствовать требованиям

Платформа помогает реализовать меры защиты объектов КИИ в соответствии с требованиями ФСТЭК России и построить ведомственные центры ГосСОПКА в соответствии с требованиями ФСБ России.

ПТ ВЕДОМСТВЕННЫЙ ЦЕНТР

Система управления инцидентами

ЗАДАЧИ, КОТОРЫЕ ВЫ МОЖЕТЕ РЕШИТЬ

- Автоматизация и контроль процесса реагирования на инциденты
- Обмен информацией об инцидентах и актуальных угрозах с НКЦКИ и другими отраслевыми CERT

Экономит время специалистов по ИБ

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

Адаптируется к задачам заказчика

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.

Позволяет соответствовать требованиям

Система помогает организациям соответствовать требованиям закона №187-ФЗ и его подзаконных актов, а также приказу ФСБ России от 19.06.2019 №282 о необходимости регистрации инцидентов, управления ими и информирования регуляторов.

КОМПЛЕКСНЫЕ РЕШЕНИЯ

ptsecurity.com

Раннее выявление целевых атак

Решение для крупных компаний, холдингов и корпораций с сетью филиалов, выстраивающих защиту от целевых атак (APT)

Помогает максимально быстро обнаружить скрытое присутствие злоумышленника в инфраструктуре и воссоздать полную картину атаки для эффективного расследования.

Состав решения

- PT Network Attack Discovery
- PT Sandbox
- Услуги экспертного центра PT ESC

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.

Обеспечение безопасности объектов КИИ

Решение для субъектов КИИ, планирующих построить систему безопасности объекта 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.

Состав решения

- MaxPatrol SIEM
- PT Network Attack Discovery
- MaxPatrol 8
- PT MultiScanner
- PT ISIM
- PT Application Inspector
- PT Application Firewall
- Услуги экспертного центра PT ESC
- ПТ Ведомственный центр

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.

Создание центра ГосСОПКА и взаимодействие с НКЦКИ

Решение для организаций, планирующих поэтапное создание центра ГосСОПКА

Помогает постепенно развивать внутреннюю экспертизу ИБ, выстраивать процессы в подразделении ИБ и успешно отражать как типовые атаки, так и новые их виды.

Состав решения

- MaxPatrol SIEM
- PT Network Attack Discovery
- MaxPatrol 8
- PT MultiScanner
- PT ISIM
- PT Application Inspector
- PT Application Firewall
- Услуги экспертного центра PT ESC
- ПТ Ведомственный центр

Преимущества

- Продукты имеют сертификаты соответствия ФСТЭК России.
- Все продукты входят в единую экосистему Positive Technologies.
- Все продукты включены в единый реестр российского программного обеспечения.

СЕРВИСЫ

ptsecurity.com

Услуги по анализу защищенности

Услуги по оценке уровня защищенности направлены на глубокий анализ различных аспектов корпоративной информационной безопасности или всей системы управления ИБ в компании в целом. Они позволяют своевременно выявить слабые места в защите и принять необходимые меры для их устранения.

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 критически значимыми системами управления бизнесом.

Анализ защищенности мобильных приложений

Поможет повысить защищенность данных ваших клиентов и предотвратить мошенничество.

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 Positive Technologies. В основе услуг PT ESC — более 16 лет опыта в анализе защищенности, расследовании инцидентов и деятельности крупнейших APT-группировок, а также мониторинга безопасности крупных компаний.

Мониторинг периметра

Помогает непрерывно выявлять проблемы, возникающие на сетевом периметре компании.

Поиск следов компрометации

Позволяет выявить следы подготовки к хакерской атаке и признаки компрометации инфраструктуры.

Реагирование и расследование

Поможет существенно снизить риск успешной кибератаки как на внешний, так и внутренний периметр компании.

Managed protection

Эксперты PT ESC помогут добиться максимальной пользы от внедрения продуктов PT MaxPatrol SIEM, PT NAD, PT SandBox и PT ISIM за счет периодического контроля выявленных инцидентов.

Услуги для непрерывного повышения защищенности бизнеса от киберугроз

Набор уникальных услуг по повышению защищенности бизнеса от киберугроз поможет вам 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 атакой.

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.

ДЛЯ ЗАМЕТОК

PT-Product-Catalog_2021_PB.RUS.0010.09.SEP.30.2021

ptsecurity.com