POSITIVE TECHNOLOGIES

ptsecurity.com

О КОМПАНИИ

Positive Technologies — один из мировых лидеров в области комплексной защиты крупных информационных систем от современных киберугроз. Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России. В основе наших продуктов и услуг лежит 16-летний исследовательский опыт по следующим направлениям:

- безопасность информационных систем,
- анализ уязвимостей программного обеспечения,
- безопасность операционных технологий и технологических систем,
- расследование инцидентов безопасности.

Positive Technologies активно привлекает лучших экспертов и инженеров в области ИБ: в компании работают более 700 человек, и она имеет представительства и R&D-центры не только в России, но и в Англии, Италии, США, Тунисе, Чехии и Южной Корее.

Специалисты исследовательского центра Positive Research помогли обнаружить более 250 неизвестных ранее уязвимостей в продуктах Cisco, Google, Honeywell, Huawei, Microsoft, Oracle, SAP, Schneider Electric, Siemens, заслужив репутацию экспертов мирового уровня в вопросах защиты самых разнообразных устройств и инфраструктур.

УСЛУГИ

- Тестирование на проникновение: внешнее, внутреннее, социальная инженерия, беспроводные сети
- Мониторинг защищенности внешнего периметра (Advanced Border Control)
- Комплексный анализ уязвимостей веб-приложений
- Комплексный анализ уязвимостей мобильных приложений
- Анализ защищенности промышленных систем (АСУ ТП)
- Анализ защищенности сетей операторов связи (SS7, Diameter, RAN)
- Анализ защищенности банковских систем (ДБО, АБС, банкоматы)
- Выявление и расследование инцидентов ИБ
- Ретроспективный анализ: поиск следов успешных атак, не зафиксированных системами защиты информации

ПРОДУКТЫ

PT Telecom Attack Discovery

Защита сигнальных сетей SS7 и Diameter

Обеспечивает защиту сигнальных сетей SS7 и Diameter операторов мобильной связи. Благодаря умному механизму выявления любых видов угроз и мгновенному реагированию на инциденты PT TAD позволяет предотвратить утечки персональных данных, перехват звонков и СМС, отслеживание местоположения абонентов, мошенничество и атаки, приводящие к отказу в обслуживании.

MaxPatrol

Тотальный контроль защищенности

Механизмы тестирования на проникновение (Pentest), проверки безопасности системных конфигураций (Audit) и контроля соответствия стандартам (Compliance) обеспечивают непрерывный мониторинг безопасности на всех уровнях информационной системы. Постоянно пополняемая база знаний уязвимостей — одна из крупнейших в мире.

MaxPatrol SIEM

Выявление инцидентов ИБ в реальном времени

Обрабатывает события ИБ, собирает данные об активах и автоматически выявляет известные и новые виды угроз. Служба ИБ моментально получает уведомления об инцидентах, что помогает оперативно отреагировать на атаку и предотвратить репутационный и финансовый ущерб.

PT MultiScanner

Защита от вредоносных программ

Многоуровневая система защиты от вредоносного ПО. Анализирует файлы, которые попадают в корпоративную сеть в сетевом и почтовом трафике, загружаются в веб-приложения и файловые хранилища компании. Файлы проверяются с помощью нескольких антивирусов и набора индикаторов компрометации, а также проходят динамический анализ в песочнице. Благодаря ретроспективному анализу продукт обнаруживает угрозы, которые не были выявлены ранее.

PT Network Attack Discovery

Поиск следов компрометации в сетевом трафике

Решение для поиска следов компрометации и расследования атак в сетевом трафике. PT NAD глубоко анализирует сетевой трафик, выявляет сетевые атаки и аномалии до того, как они нанесли серьезный ущерб, и помогает проводить детальные расследования.

PT Platform 187

Реализация основных требований 187-ФЗ

Программно-аппаратный комплекс для реализации основных функций безопасности значимых объектов КИИ и взаимодействия с ГосСОПКА. Платформа включает в себя набор технических средств, который помогает выполнить основные требования законодательства, автоматизирует процессы ИБ и значительно повышает их эффективность.

ПТ Ведомственный центр

Управление инцидентами и взаимодействие с ГосСОПКА

Система управления инцидентами, которая автоматизирует процесс реагирования и информирует о них Национальный координационный центр по компьютерным инцидентам (НКЦКИ). Система помогает организациям соответствовать требованиям 187-ФЗ и его подзаконных актов о необходимости регистрации инцидентов, управления ими и взаимодействия с НКЦКИ.

XSpider

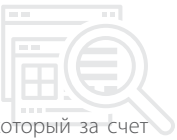
Поиск брешей в информационных системах

Благодаря рекордно низкому уровню ложных срабатываний, простоте использования и невысокой цене сканер безопасности XSpider заслуженно считается самым популярным решением данного класса на российском рынке. Продукт предлагает максимальное покрытие программной и аппаратной части крупных информационных систем — от рабочих станций до сетевых устройств.

ПРОДУКТЫ

PT Application Inspector

Анализ защищенности приложений



Анализатор защищенности приложений, который за счет комбинации статического, динамического и интерактивного методов анализа обеспечивает высокоточные результаты. Портфолио PT Application Inspector включает решения как для экспертов ИБ, так и для команды разработки и менеджмента, что позволяет выстроить процесс безопасной разработки и эффективно решать задачи безопасности приложений.

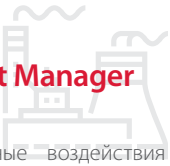
PT Application Firewall

Блокирование атак на приложения

Самообучающийся защитный экран уровня приложений, предназначенный для выявления и блокирования современных атак на веб-порталы, ERP-системы и мобильные приложения. Благодаря встроенному сканеру уязвимостей и механизму корреляции PT Application Firewall отсеивает неактуальные попытки взлома и выявляет цепочки развития реальных атак.

PT Industrial Security Incident Manager

Киберзащита промышленных систем



Помогает обнаруживать злоумышленные воздействия на промышленные системы и обеспечивает эффективное расследование инцидентов ИБ на объектах критической информационной инфраструктуры. PT ISIM инвентаризирует промышленную сеть без вмешательства в технологический процесс, анализирует работу АСУ ТП, выявляет случаи неавторизованного управления контроллерами (ПЛК) и кибератаки на элементы АСУ ТП.

Для получения дополнительной информации
обращайтесь по адресу pt@ptsecurity.com

ПРОДУКТЫ

PT Application Inspector — универсальный инструмент анализа защищенности приложений любого масштаба и поддержки цикла безопасной разработки.

PT Application Firewall — система обнаружения атак на приложения с уникальным набором защитных технологий.

PT Industrial Security Incident Manager — система мониторинга защищенности и управления инцидентами информационной безопасности промышленных систем.

PT Telecom Attack Discovery — система обнаружения вторжений и защиты сигнальных сетей операторов мобильной связи.

MaxPatrol — лидер среди систем контроля защищенности и соответствия стандартам в России.

MaxPatrol SIEM — система мониторинга событий ИБ и выявления инцидентов в реальном времени.

PT MultiScanner — многоуровневая система защиты от вредоносных программ.

PT Network Attack Discovery — решение для выявления следов компрометации в сетевом трафике и расследования атак.

PT Platform 187 — программно-аппаратный комплекс для реализации основных функций безопасности значимых объектов КИИ и подключения к ГосСОПКА.

«ПТ Ведомственный центр» — система управления инцидентами и взаимодействия с ГосСОПКА.

XSpider — сканер, способный выявить максимальное количество уязвимостей в информационной системе.

ПРЕДСТАВИТЕЛЬСТВА В РОССИИ

Москва — центральный офис
Преображенская пл., д. 8

Самара
Молодогвардейская ул., д. 204, офисы 602, 603

Нижний Новгород
Ул. Тимирязева, д. 15, корп. 2, 2 этаж

Санкт-Петербург
2-я Советская ул., д. 17

Новосибирск
Вокзальная магистраль, д. 1/1, офис 706

Томск
Ул. Нахимова, д. 8, офис 221

PT-Products_CO_A4.RUS.0006.20.APR.04.2019