Кибербез нацеленный на результат

Артём Нюхалов

Представитель Positive technologies
в странах Центральной Азии

23 года

экспертизы
в разработке
и исследованиях

20k+

внедрений

500+

партнеров

MOEX МОСКОВСКАЯ БИРЖА

Первая и единственная публичная компания в области кибербезопасности на Московской бирже (MOEX: POSI)

Входим в топ-50 компаний на Московской Бирже (основной индекс IMOEX)

pt

Positive Technologies

25+

высокотехнологичных
продуктов и решений
в портфеле

3000

крупных компаний из всех отраслей — наши клиенты

200k+

акционеров

*Согласно рейтингу ЭКОПСИ и Хабр

Red team и blue team

Фундаментальное преимущество Positive Technologies — объединение экспертизы

PT SWARM — НАСТУПАТЕЛЬНАЯ БЕЗОПАСНОСТЬ

1 менее часа
минимальное время для получения максимальных привилегий в домене

Positive Labs
помогаем новым технологиям становиться более зрелыми и защищенными: от электрокаров до экзоскелетов

в 96%+ проектов
успешно проникаем в периметр компании*

350+ уязвимостей
обнаружили за 2025 год

50% уязвимостей
в промышленности и телекомах обнаружили наши эксперты

ЗАЩИТА СИСТЕМ КЛИЕНТА — **PT ESC**

60+ минут
представим анализ инфраструктуры

30+ минут
отреагируем на инцидент

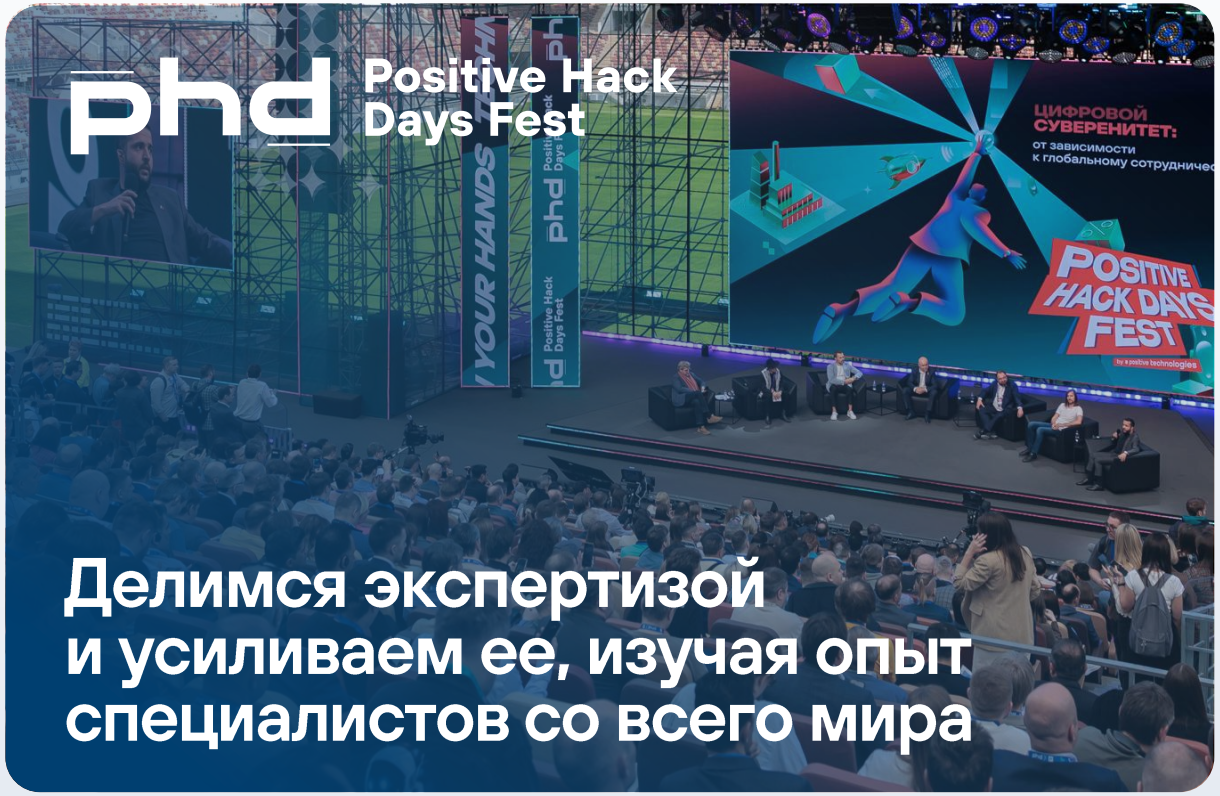
200+
обнаруженных уязвимостей нулевого дня в год

аудитов кибербезопасности ежегодно

dbugs portal
бесплатный портал от команды PT SWARM с данными более чем о 300 000 уязвимостей со всего мира

PT Fusion
портал от команды PT Threat Intelligence, объединяющий все ключевые уязвимости в одном удобном и понятном интерфейсе

*На основе проведенных исследований по итогам пентестов за 2022 и 2023 годы



Делимся экспертизой и усиливаем ее, изучая опыт специалистов со всего мира

15 лет

развиваем экспертизу и комьюнити на международном киберфестивале

40

стран-участниц киберфестиваля

PHDays — уникальное по масштабу и значимости мероприятие для кибербезопасности

В 2025 году получили

›825

заявок на выступления от 716 экспертов со всего мира

150k

человек погрузились в мир кибербеза за три дня на крупнейшем российском стадионе — Лужники

Кибербезопасность глазами бизнеса, хакера, разработчика и специалиста по ИБ

В 26 ТЕМАТИЧЕСКИХ ТРЕКАХ И 269 ДОКЛАДАХ ОТ 500+ СПИКЕРОВ

Самые масштабные кибербитвы

С 2016 года проводим кибербитвы, где сотни хакеров и десятки команд защитников проверяют защищенность компаний, отраслей и стран, используя настоящие промышленные контроллеры и АСУ ТП

Крупнейшие российские онлайн-полигоны

Запустили онлайн-полигоны для выявления и расследования APT-атак (для команд SOC) и практических тренировок по анализу защищенности и поиску уязвимостей (для белых хакеров)

30 000+

зарегистрированных экспертов из 60 стран
крупнейшее профессиональное сообщество в области практической кибербезопасности

300+ млн

выплачено исследователям на Standoff Bug Bounty с 2022 года — экспертиза превращается в реальные деньги

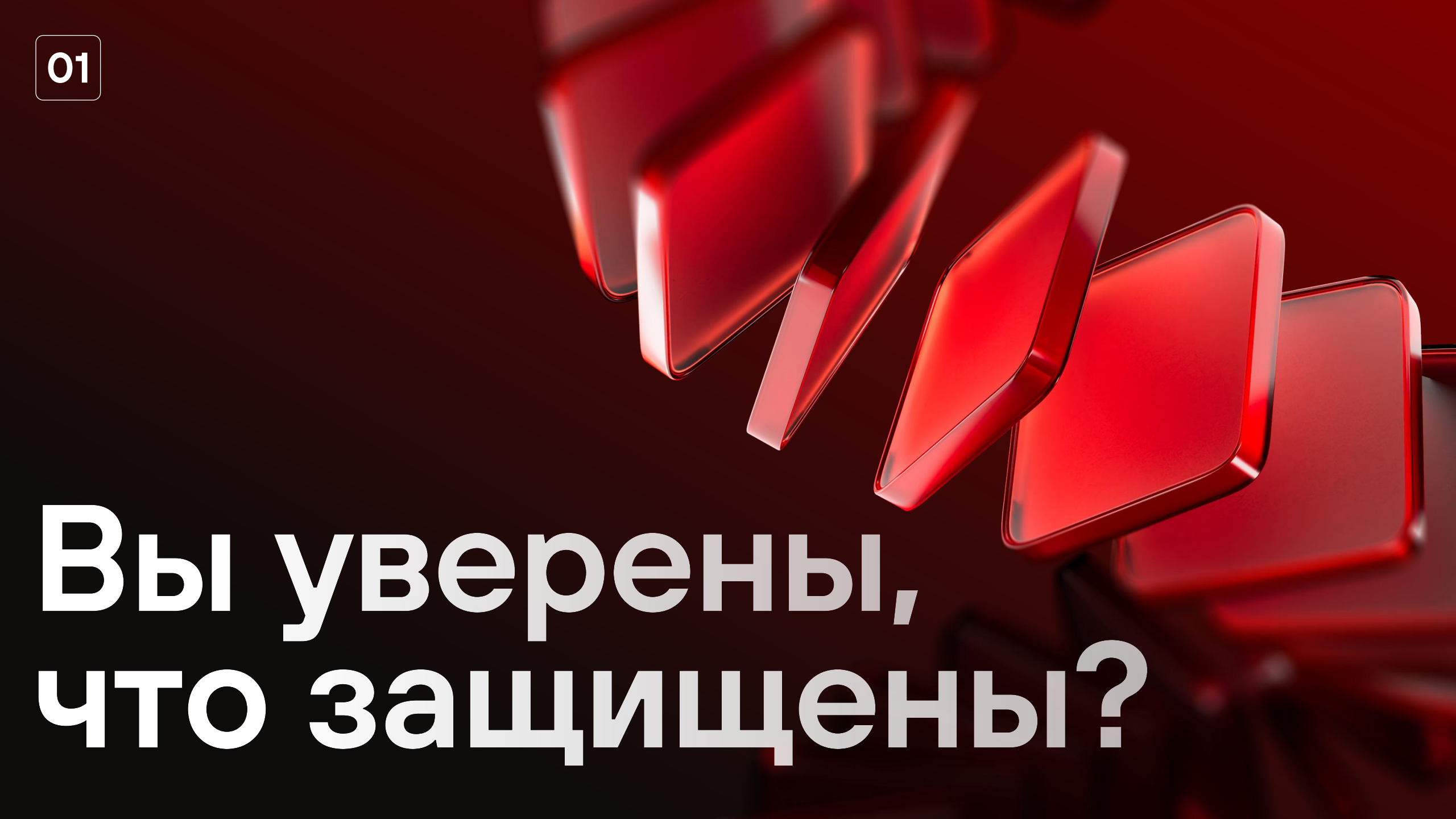
1500+

виртуальных машин обеспечивают максимальную реалистичность кибербитв

Выпустили уже 300+ публичных исследований по кибербезопасности в России и мире

Ежеквартальное исследования о ИБ-трендах Positive Research

01



Вы уверены, что защищены?

Бизнес годами инвестирует в кибербезопасность, но так и не видит реальных результатов

РАЗРЫВ МЕЖДУ СТОИМОСТЬЮ ЗАЩИТЫ И СТОИМОСТЬЮ АТАКИ БУДЕТ РАСТИ

294 млн ₽*

в среднем инвестировали в кибербезопасность в 2025 году крупные российские компании

~$ 5,4M

$ 12k**

именно за столько можно реализовать недопустимое событие в 2/3 крупных предприятий РФ

*По данным исследования Центра стратегических инициатив «Инвестиции в информационную безопасность в России»
**По данным исследования АО «Кибериспытание» «Недопустимое событие 2025»

Автоматизация кибератак делает их дешевле и разрушительнее

Автоматизация кибератак

ИИ автоматизирует кибератаки, делает их более сложными и адаптивными, позволяя злоумышленникам прогнозировать поведение систем защиты

Кибератака как сервис

Появление SaaS-платформ для организации кибератаки делает их более дешевыми и массовыми — атакуют отрасли целиком, а не отдельные компании

Хакеры зачастую проникают в крупный бизнес через подрядчиков

СРЕДНИЙ БИЗНЕС НЕ ИНВЕСТИРУЕТ В КИБЕРБЕЗОПАСНОСТЬ,
СЧИТАЯ ЧТО НЕ ИНТЕРЕСЕН ХАКЕРАМ

40%

кибератак приходится
на средний бизнес*

60%

небольших компаний,
подвергшихся кибератаке,
ее не переживают*

34 минуты

минимальное время на реализацию
недопустимого события в компании,
где не предприняты усилия
для замедления хакера**

*qualysec.com
**По данным исследования АО «Кибериспытание» «Недопустимое событие 2025»

«У нас зрелый SOC» самая опасная фраза в ИБ

Зоопарк технологий и нулевая отдача

Компании закупили дорогие средства защиты, но не умеют их правильно применять.
В результате инвестиции в безопасность не окупаются

43% — средний уровень покрытия детектирования

SOC копит гигабайты логов, которые никто не анализирует, а инциденты пропускаются

Спокойствие — обманчивый показатель

Даже если есть плейбуки под давлением команда может действовать не так, как это было задумано

Команда без развития

Без постоянных тренировок и обучения компетенции застывают на базовом уровне.
Результат — дорогие СЗИ, которыми некому пользоваться

Наш подход

РЕЗУЛЬТАТИВНАЯ КИБЕРБЕЗОПАСНОСТЬ

Результат кибербезопасности — киберустойчивость

Киберустойчивость — способность организации (отрасли, государства) стабильно функционировать в условиях кибератак, направленных на реализацию недопустимых событий

1

Определяем недопустимые для организации события

2

Усложняем путь хакера и ускоряем реагирование

3

Измеряем кибер-устойчивость на кибериспытаниях с участием реальных хакеров

Допустимое событие

Недопустимое событие

ПРИМЕРЫ ПРОМЫШЛЕННОЙ КОМПАНИИ

Приостановка оборудования, которая вызвала задержку выполнения одного из контрактов

Техногенные аварии с экологическим ущербом и угрозой жизни из-за взлома технологического процесса

Примеры недопустимых событий для вашей отрасли

Открытая методология РКБ

Наши продукты, сервисы и услуги дают подтверждаемый результат

время
АТАКИ

Защищаем ИТ-инфраструктуру, чтобы хакерам было было сложно и дорого взломать ее

время
РЕАГИРОВАНИЯ

Видим и останавливаем хакеров, которые проникли в инфраструктуру, до наступления недопустимого события

итог
КИБЕРУСТОЙЧИВОСТЬ

Проверяем надежность своих продуктов на кибериспытаниях

bugbounty.standoff365.com/programs/pt_product

РАЗВИТИЕ КОМПЕТЕНЦИЙ

Повышайте киберустойчивость

STANDOFF

ЭТАП 0 — БАЗОВЫЕ НАВЫКИ

Платформа автономного обучения

Формируйте экспертизу команды ИБ: отработка базовых навыков работы с СЗИ и расследования несложных цепочек атак

ЭТАП 1 — АУДИТ

Киберучения Standoff

Проведите аудит готовности команды ИБ на оффлайн-интенсиве по расследованию атак реальных белых хакеров

ЭТАП 2 — ПОДГОТОВКА

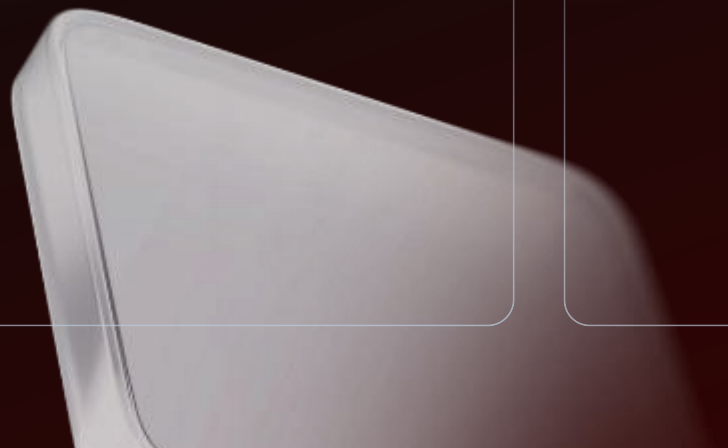
Онлайн-полигон Standoff Defend

Отработайте защиту от APT-атак на реалистичных симуляциях без риска для бизнеса

ЭТАП 3 — ПРОВЕРКА

Кибербитва Standoff

Проверьте вашу команду ИБ в условиях интенсивных атак лучших белых хакеров



Попробуйте расследовать атаку уже сегодня

Мастер-класс по расследованию атаки на онлайн-полигоне Standoff Defend

Вместе с экспертом Standoff вы разберете реальную хакерскую атаку: от первичного обнаружения следов компрометации до восстановления цепочки действий злоумышленника. Вся работа ведется в реальных СЗИ — тех же инструментах, с которыми специалисты работают в боевых условиях

Мастер-класс рассчитан на аналитиков SOC, специалистов по реагированию на инциденты и всех, кто хочет понять, как выглядит расследование изнутри.

Для полного погружение в расследование атаки необходим ноутбук.

Где: зал «Бухара»

Когда: в 17:20

Онлайн-практикумы

Управление уязвимостями: от теории к практике

Старт: 25.05.2026

Набор идёт

Харденинг ИТ: от дизайна до настроек

Старт: 01.06.2026

Набор идёт

Анализ сетевого трафика: искусство обнаружения атак

Старт: 08.06.2026

Набор идёт

Архитектура сетевой безопасности предприятия

Старт: 17.08.2026

Набор идёт

Безопасность приложений: курс для инженеров

Старт: 07.09.2026

Набор идёт

Построение SOC 2.0: от концепции до реализации

Старт: 14.09.2026

Набор идёт

Что мы создаем
для борьбы с хакерами:

ПРОДУКТЫ И СЕРВИСЫ

Создаем продукты и решения для достижения киберустойчивости

Все продукты от одного вендора

25+ продуктов, которые закрывают все задачи для достижения измеримых результатов

Инвестируем в разработку и создаем технологии для реальной защиты

9,1 млрд руб.

инвестировано в разработку продуктов по итогам 2024 года
(38% от совокупной выручки Positive Technologies)

1300+

разработчиков и аналитиков в команде R&D Positive Technologies

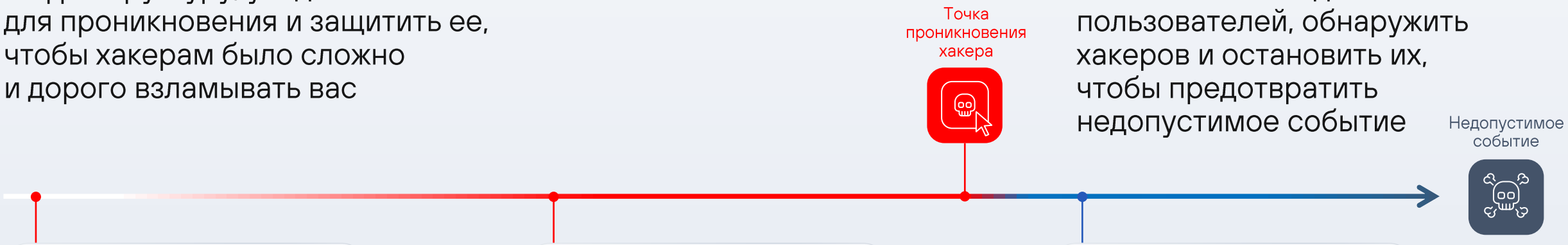
Увеличиваем время атаки и сокращаем время реагирования

Увеличиваем время АТАКИ

Продукты помогут проверить вашу инфраструктуру, увидеть лазейки для проникновения и защитить ее, чтобы хакерам было сложно и дорого взламывать вас

Сокращаем время РЕАГИРОВАНИЯ

Продукты помогут увидеть аномалии в поведении пользователей, обнаружить хакеров и остановить их, чтобы предотвратить недопустимое событие



Узнать

- Моделирование кибератак, выявление уязвимостей и мисконфигураций
- Проверка защищенности с помощью автопентеста

Защитить

- Защита инфраструктуры (сети, конечные устройства, электронная почта)
- Защита приложений

Обнаружить и остановить

- Мониторинг и реагирование на инциденты
- Использование сенсоров и агентов

Знаем, как заранее защититься

ЦЕЛЬ — УВЕЛИЧИТЬ ВРЕМЯ РЕАЛИЗАЦИИ КИБЕРАТАКИ

Оценить и усилить защищенность

МОДЕЛИРОВАНИЕ КИБЕРАТАК, ВЫЯВЛЕНИЕ УЯЗВИМОСТЕЙ И МИСКОНФИГУРАЦИЙ

MaxPatrol Carbon
Интеллектуальная система для управления киберугрозами и анализа киберустойчивости компании

MaxPatrol VM
Система для управления уязвимостями

MaxPatrol HCC
Модуль комплаенс-контроля

ПРОВЕРКА ЗАЩИЩЕННОСТИ

PT Dephaze
Автопентест инфраструктуры для регулярной проверки защищенности

PT Knockin
Сервис для онлайн-проверки защищенности электронной почты

Защитить

ЗАЩИТА ИНФРАСТРУКТУРЫ И ДАННЫХ

PT NGFW
Высокопроизводительный и надежный межсетевой экран нового поколения

MaxPatrol EPP
Антивирусная защита конечных устройств

PT Sandbox
Песочница для защиты от целевых атак с использованием ВПО

PT Data Security
Платформа для инвентаризации, автоматизированной классификации и мониторинга данных

PT Email Security
Защита почты от всех векторов атак

ЗАЩИТА ПРИЛОЖЕНИЙ

PT Container Security
Решение для комплексной защиты инфраструктуры гибридного облака

PT BlackBox
Анализатор защищенности веб-приложений, способный выявлять уязвимости без доступа к исходному коду

PT Application Inspector
Продукт для эффективного выявления уязвимостей в программном коде приложений и заимствованных компонентах

PT Application Firewall
Высокопроизводительный межсетевой экран для непрерывной защиты веб-приложений и их API

PT Maze
Решение для защиты iOS и Android приложений от реверс-инжиниринга, создания клонов и взлома

Знаем, как обнаружить и остановить

ЦЕЛЬ — СНИЗИТЬ ВРЕМЯ ОБНАРУЖЕНИЯ И РЕАГИРОВАНИЯ НА ИНЦИДЕНТ

Мониторинг и реагирование на инциденты

ТЕХНОЛОГИИ ДЛЯ СИЛЬНОГО SOC

MaxPatrol O2

Автоматизирует все сложные и рутинные процессы — от обнаружения и расследования кибератак до оперативного реагирования на них

MaxPatrol SIEM

Превращает поток событий в список приоритизированных инцидентов с нужным для расследования контекстом

MaxPatrol 360

Единый центр управления расследованиями и операционной работой SOC

ИТ-ИНФРАСТРУКТУРА (СЕНСОРЫ)

PT NAD

Эталонный источник данных о сети для контроля инфраструктуры и обнаружения действий хакеров в трафике

MaxPatrol EDR

Автономный агент для защиты конечных устройств от сложных и целевых атак

PT Sandbox

Песочница для защиты от целевых атак с использованием ВПО

Если нужно одно решение для достижения киберустойчивости

ДЛЯ БЫСТРОГО СТАРТА В ЗАЩИТЕ С ГАРАНТИЕЙ РЕЗУЛЬТАТА

PT X

Облачное решение для мониторинга и реагирования с финансовой гарантией результата

ДЛЯ ЗАЩИТЫ ТЕХНОЛОГИЧЕСКИХ И ПРОМЫШЛЕННЫХ ИНФРАСТРУКТУР

PT ISIM

Единая система обеспечения киберустойчивости промышленных инфраструктур, на базе которой можно выстраивать защиту всего промышленного контура

Индивидуальный подход к каждому клиенту:

- Проведем презентацию и демонстрацию
- Проведем тест-драйв или испытания
- Поможем качественно внедрить
- Окажем техническую поддержку

Сертификаты

Сертификаты:

- Система мониторинга событий ИБ **SIEM**
- Система управления уязвимостями **VM**
- Система мониторинга и реагирования на конечных устройствах **EDR**

В планах на 2026:

- Система выявления внутрисетевых угроз **Network Attack Discovery (NAD)**
- Система защиты приложений от несанкционированного доступа **Application Firewall PRO (AF PRO)**
- Система статического и динамического анализа для выявления вредоносных объектов **Sandbox**

НАЦИОНАЛЬНАЯ СИСТЕМА СЕРТИФИКАЦИИ РЕСПУБЛИКИ УЗБЕКИСТАН

ОРГАН ПО СЕРТИФИКАЦИИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ (ОС ИКТ/СЗИ) ГУП «ЦЕНТР КИБЕРБЕЗОПАСНОСТИ»

Республика Узбекистан, г. Ташкент, Мирабадский район, ул. Т.Шевченко, д.20, № O'ZAK.MS.0004

(Наименование органа по сертификации, адрес, № в Гос. реестре)

№ 0011004

СЕРТИФИКАТ СООТВЕТСТВИЯ

Зарегистрирован в Государственном реестре "12" марта 2026 г.

№ UZ.SMT.01.0004.07 000 031

Действителен до "12" марта 2029 г.

Код ТН ВЭД 8523499900 (справочный)

ООО «Прорывные Технологии», Российская Федерация

(предприятие, фирма, страна-изготовитель)

Настоящий сертификат удостоверяет, что идентифицированная должным образом продукция:

Программное обеспечение «Система мониторинга событий информационной безопасности и выявления инцидентов Security Information and Event Management» (версии серии 27)

Серийное производство

(количество или серийное производство) (наименование, тип, вид, марка)

соответствует требованиям нормативной документации.

O'z DSt 2814:2014 п.9.1, п.9.2, п.9.4; O'z DSt 2816:2014 п.5.3.

Схема сертификации: 3 (три)

Заявитель (изготовитель, продавец) ООО «Прорывные Технологии»

(нужное подчеркнуть)

Российская Федерация, г. Москва, вн.тер.г муниципальный округ Сокольники, ул. Маленковская, д.14, к.3, помещение 4, этаж 1, комната 1, офис 205

(адрес)

Сертификат выдан на основании:

а) документов Акт идентификации и отбора образцов ИКТ/СЗИ № 014/2025 от 16.09.2025г.

б) испытания образцов Протоколы испытаний № 014/2025-Л6-П от 03.10.2025г. и № 004/2026-Л6-П от 27.02.2026г. Аккредитованная испытательная лаборатория ГУП «Центр кибербезопасности» (O'ZAK.SL.0001)

в) акта проверки производства Акт обследования состояния производства № 1 от 06.03.2026

Инспекционный контроль осуществляет с периодичностью: Согласно «Соглашению по использованию знака соответствия и проведению периодической оценки»

Особые отметки: «Действие настоящего сертификата соответствия распространяется на серийно производимое Программное обеспечение при условии соблюдения «Соглашения по использованию знака соответствия и проведению периодической оценки». При необходимости передачи конфиденциальной информации за пределы контролируемой зоны должны использоваться сертифицированные средства криптографической защиты информации»

Знак соответствия проставляется: на бланке лицензии на ПО и в «Руководстве администратора»

Примечание: Копия сертификата соответствия действительна только после заверения печатью органом по сертификации или держателем подлинника.

Руководитель органа по сертификации М.П. (подпись) Юсупов Ж.А. (Ф.И.О.)

Эксперт М.П. (подпись) Дурель А.В. (Ф.И.О.)

НАЦИОНАЛЬНАЯ СИСТЕМА СЕРТИФИКАЦИИ РЕСПУБЛИКИ УЗБЕКИСТАН

ОРГАН ПО СЕРТИФИКАЦИИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ (ОС ИКТ/СЗИ) ГУП «ЦЕНТР КИБЕРБЕЗОПАСНОСТИ»

Республика Узбекистан, г. Ташкент, Мирабадский район, ул. Т.Шевченко, д.20, № O'ZAK.MS.0004

(Наименование органа по сертификации, адрес, № в Гос. реестре)

№ 0011005

СЕРТИФИКАТ СООТВЕТСТВИЯ

Зарегистрирован в Государственном реестре "12" марта 2026 г.

№ UZ.SMT.01.0004.07 000 032

Действителен до "12" марта 2029 г.

Код ТН ВЭД 8523499900 (справочный)

ООО «Прорывные Технологии», Российская Федерация

(предприятие, фирма, страна-изготовитель)

Настоящий сертификат удостоверяет, что идентифицированная должным образом продукция:

Программное обеспечение «Система управления уязвимостями Vulnerability Management» (версии серий 27)

НАЦИОНАЛЬНАЯ СИСТЕМА СЕРТИФИКАЦИИ РЕСПУБЛИКИ УЗБЕКИСТАН

ОРГАН ПО СЕРТИФИКАЦИИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ (ОС ИКТ/СЗИ) ГУП «ЦЕНТР КИБЕРБЕЗОПАСНОСТИ»

Республика Узбекистан, г. Ташкент, Мирабадский район, ул. Т.Шевченко, д.20, № O'ZAK.MS.0004

(Наименование органа по сертификации, адрес, № в Гос. реестре)

№ 0011003

СЕРТИФИКАТ СООТВЕТСТВИЯ

Зарегистрирован в Государственном реестре "12" марта 2026 г.

№ UZ.SMT.01.0004.07 000 030

Действителен до "12" марта 2029 г.

Код ТН ВЭД 8523499900 (справочный)

ООО «Прорывные Технологии», Российская Федерация

(предприятие, фирма, страна-изготовитель)

Программное обеспечение «Система мониторинга и реагирования на конечных устройствах (Endpoint Detection and Response)» (версии серии 8)

Серийное производство

Руководитель органа по сертификации М.П. (подпись) (Ф.И.О.)

Эксперт М.П. (подпись) Дурель А.В. (Ф.И.О.)

Если нужно одно решение для быстрого старта в защите, — есть PT X

Облачное решение для мониторинга и реагирования

Внедряется как продукт, работает как сервис

Быстрый старт

Первые результаты будут видны уже через несколько часов после установки легких агентов

В реальном времени

Наши ведущие эксперты отвечают за своевременное обнаружение и остановку атак 24/7

Версии продукта

1. **PT X Base**
   Стандартный уровень защиты от хакерских атак
2. **PT X PRO**
   Продвинутый уровень защиты от APT-атак

Не нужно покупать продукты отдельно — все внутри PT X

- MaxPatrol EDR
- PT NAD
- PT Sandbox
- MaxPatrol SIEM
- MaxPatrol VM
- MaxPatrol HCC

ОТВЕЧАЕМ ЗА РЕЗУЛЬТАТ, А НЕ ФОРМАЛЬНЫЕ SLA

Выведем вас на кибериспытания и выплатим вознаграждение белым хакерам в случае реализации недопустимого события

Команда в Центральной Азии

Артём Нюхалов

Представитель в странах Центральной Азии

anyukhalov@ptsecurity.com

+996 221 210172
@artem_kg

Азиз Мирбакиев

Консультант по технологиям PT

amirbakiev@ptsecurity.com

+996 770 777060
@Intelli9ent

Адиль-Ай Жакшылыкова

Координатор проектов в Центральной Азии

adzhakshylykova@ptsecurity.com

+996 559 290797
@vbezd

Галымхан Ерден

Инженер пилотных проектов

Оксана Галкина

Customer & partner success lead

ogalkina@ptsecurity.com

@nemour6696

Фархад Артыков

КАМ Узбекистан

fartykov@ptsecurity.com

@Storyteller2506

Спасибо!

Регистрация на кибербитву в Москве 16-19 июня

Ежеквартальное исследования Positive Research

Примеры недопустимых событий для вашей отрасли

Открытая методология результативной кибербезопасности

Сертификаты ЦКБ

Практикумы и курсы

Артём Нюхалов

Представитель Positive technologies
в странах Центральной Азии

anyukhalov@ptsecurity.com

@artem_kg

ptsecurity.com

Лучшие действуют на опережение

ptsecurity.com