positive technologies

ПРОДУКТЫ И СЕРВИСЫ POSITIVE TECHNOLOGIES

РЕАГИРОВАТЬ ИЛИ ПРЕДВОСХИЩАТЬ?

СООТВЕТСТВОВАТЬ ИЛИ ИЗМЕРЯТЬ?

ПОЛАГАТЬСЯ ИЛИ УПРАВЛЯТЬ?

positive technologies

ЛУЧШИЕ ДЕЙСТВУЮТ НА ОПЕРЕЖЕНИЕ

НАША ЭКСПЕРТИЗА

Выходим за рамки привычных сценариев, чтобы знать, как думают злоумышленники

15 лет

проводим киберфестиваль Positive Hack Days, где делимся экспертизой и усиливаем ее, изучая опыт международных специалистов

10 лет

развиваем и закрепляем навыки киберзащитников и белых хакеров на платформе Standoff 365

24/7

даем белым хакерам проверять нашу киберустойчивость и искать уязвимости в продуктах, чтобы изучать ход мыслей атакующих и усиливать свои решения

Пока другие проверяют системы по шаблону, мы видим:

→ **То, что не замечают сканеры**
Неочевидные взаимосвязи систем, превращающиеся в лазейки для атакующих

→ **То, что пропускают отчеты**
Аномалии в поведении пользователей и систем, сигнализирующие о подготовке атаки

→ **То, что еще не стало угрозой**
Потенциально опасные сценарии, которые могут быть реализованы через месяцы

Positive Technologies —

это опыт сотен экспертов по кибербезопасности, десятки тысяч обнаруженных уязвимостей и глубокое понимание технологий. Мы смотрим на инфраструктуру глазами атакующего и защитника, поэтому находим слабые места до того, как их используют против вас

НАШИ ПРОДУКТЫ

Весь опыт Positive Technologies — в ваших руках

Накопленную экспертизу в сфере кибербезопасности мы превратили в одни из лучших в своих классах продукты для предотвращения, блокировки и расследования киберинцидентов в компаниях любого масштаба

Перспективные технологии
Активно используем технологии искусственного интеллекта и машинного обучения, анализ больших данных, блокчейн и многие другие, чтобы находить угрозы быстрее

Защита в реальном времени
Единый модульный агент для конечных устройств позволяет решать задачи управления уязвимостями и конфигурациями, сбора логов и раннего выявления киберугроз на хостах

Работа с большими объемами данных
Создали LogSpace — специальную СУБД для хранения информации о событиях ИБ из разнообразных источников

Своевременные предупреждения
Вы узнаете о новых трендовых уязвимостях за 12 часов

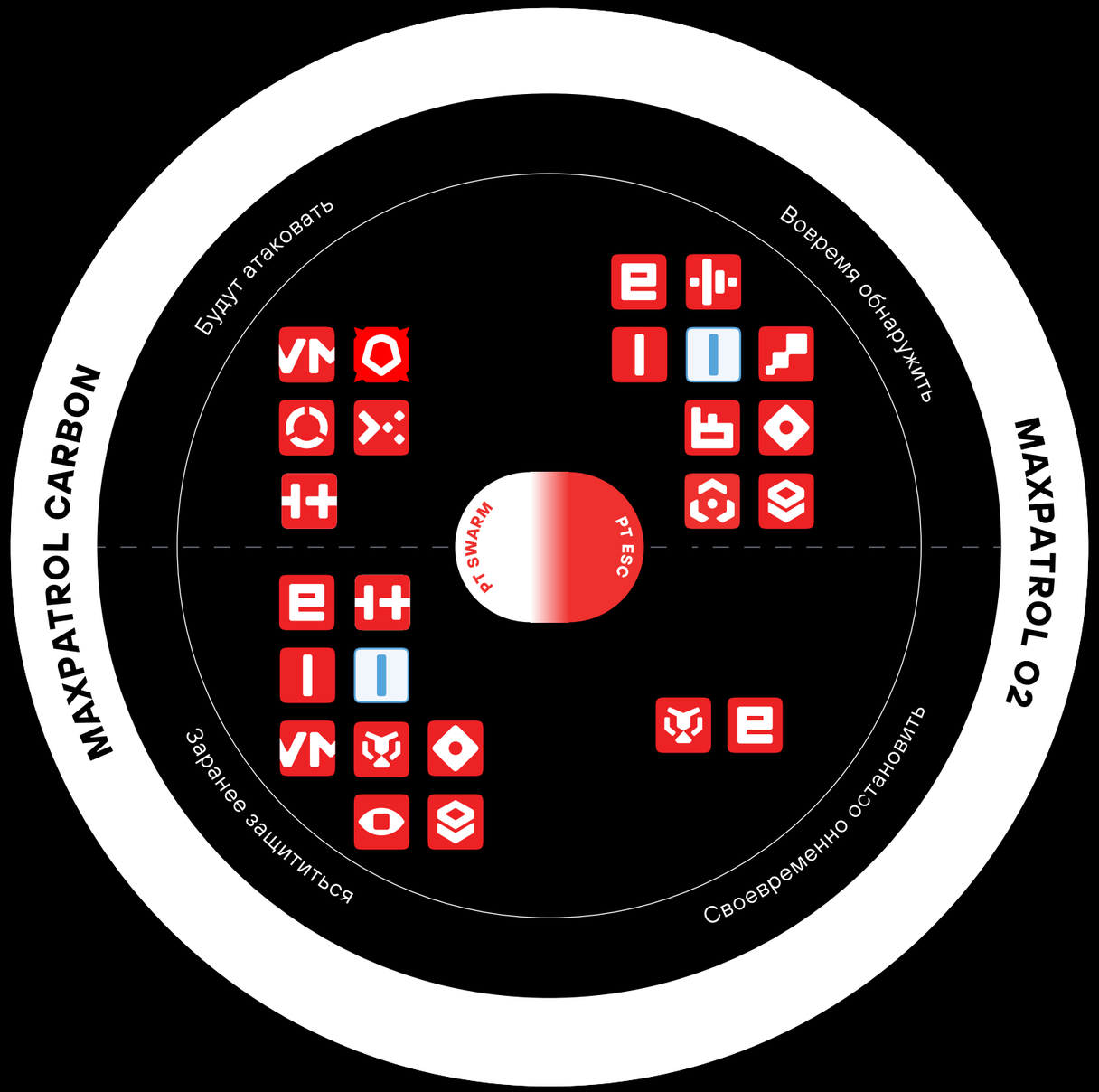
1200+

наших разработчиков, аналитиков, тестировщиков и других специалистов каждый день делают технологии лучше, а защиту — сильнее

МЫ ЗНАЕМ, КАК:

УЗНАТЬ И ЗАЩИТИТЬ

Цель: увеличить время реализации атаки



ОБНАРУЖИТЬ И ОСТАНОВИТЬ

Цель: снизить время обнаружения и реагирования

Результативная кибербезопасность: ваши действия — для защиты главного

Современный бизнес зависит от ИТ, но многие ли могут честно ответить «да» на вопрос «защищен ли я от киберугроз?». Гонка за формальными отчетами и попытки закрыть все возможные лазейки только выматывают команду, но не делают компанию реально киберустойчивой

Ключевые проблемы в сфере ИБ

[1]

- **По нашим данным, 72% организаций [1] не проверяют свою инфраструктуру и команду на готовность к сложным атакам**
- **Используемые метрики не отражают реальный уровень защищенности, а специалисты по ИБ не видят реального результата своей работы**

[2]

- **Хакеры используют все более изощренные сценарии атак. Например, растет число атак [2] через компанию-подрядчика**

Почему подход «защитить все» не работает

Попытки равномерно распределить ресурсы безопасности:

- увеличивают расходы бизнеса без повышения реальной киберустойчивости
- создают ложное ощущение защищенности
- не учитывают специфику угроз для конкретной организации
- увеличивают время адаптации ИБ к изменениям ИТ-инфраструктуры

Как следствие — хакеры всегда находят лазейки в защите периметра

Переход к результативной безопасности — это:

- Отказ от иллюзии защищенности в пользу ее измеримости
- Совместная работа отделов ИБ и ИТ для решения бизнес-задач
- Приоритизированный и понятный набор действий команды ИТ для решения задач ИБ
- Постоянное совершенствование защиты на основе практики

1 Выберите приоритеты в защите

Определение фокуса

Определите 3–5 фокусных задач и систем на основании бизнес-приоритетов организации. Это то, что может нарушить ее работу (недопустимые события)

Приоритизация защиты

Договоритесь с бизнесом о приоритизации защиты этих систем (как для отдела ИБ, так и для ИТ-подразделения), сосредоточьте усилия на критически важных активах

2 Проведите кибертрансформацию

Оценка инфраструктуры

Изучите потенциальные цепочки действий злоумышленников, которые могут привести к реализации недопустимых событий. Проанализируйте возможные методы и инструменты проведения кибератак

Усложнение пути хакера

Сформируйте для команды ИТ приоритизированный с точки зрения бизнеса набор рекомендаций по харденингу. Усильте мониторинг там, где соблюсти рекомендации невозможно

Ускорение реагирования на инциденты

Определите ключевые узлы и точки сети, с которых нужно снять трафик. Проведите тонкую настройку средств защиты и отработайте с командой ИБ процедуры реагирования на инциденты

3 Непрерывно проверяйте киберустойчивость на кибериспытаниях

Проверка защищенности организации

Привлекайте независимых белых хакеров для проверки защищенности организации и выплачивайте вознаграждение только за верифицированные экспертами цепочки кибератак

Усиление защиты

Совершенствуйте защиту, исходя из реально существующих и выявленных проблем

ИДТИ ПОЭТАПНО, ДЕЙСТВОВАТЬ ПРЯМО СЕЙЧАС

Становитесь киберустойчивыми, опираясь на понятные и измеримые этапы

1

Результат

CISO видит результат работы внедренных инструментов и процессов ИБ

Исходное состояние

Задачи

- Контроль соблюдения политик ИБ
- Усиление защиты периметра и веб-ресурсов
- Выявление недостатков инфраструктуры через мониторинг
- Контроль shadow IT

Проверка защиты

PT Knockin PT Dephaze

2

Результат

CISO берет ответственность за решение конкретных задач ИБ

Исходное состояние

Задачи

- Формирование процессов ИБ вокруг продуктов:
  - Asset management
  - Vulnerability management
  - Infrastructure security
  - Endpoint security
  - Network security
  - Application security
  - Security monitoring
  - Incident management...
- Формирование метрик работы ИБ
- Непрерывный контроль работы СЗИ (BAS, автопентест)
- Переход к режиму защиты 24/7

Проверка защиты

BUG BOUNTY
CYBERBATTLE
\+
PT Knockin
PT Dephaze

КИБЕРИСПЫТАНИЯ

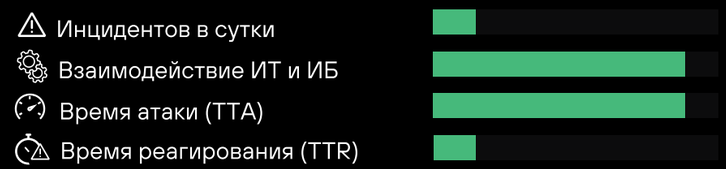
Непрерывная проверка уровня защиты от реализации НС с вознаграждением до 5 млн руб.

3

Результат

CISO уверен в киберустойчивости организации

Целевое состояние



Задачи

- Обнаружение признаков присутствия APT-группировок в инфраструктуре
- Проактивный поиск угроз (threat hunting)

Проверка защиты

КИБЕРИСПЫТАНИЯ

Непрерывная проверка уровня защиты от реализации НС с вознаграждением от 20 млн руб.

КИБЕРУЧЕНИЯ

Регулярная проверка защиты от реализации НС с привлечением внешней команды белых хакеров

\+
BUG BOUNTY
CYBERBATTLE
PT Knockin
PT Dephaze

Наша цель — сделать киберустойчивыми компании, отрасли экономики и государства. При такой разности масштабов естественно, что у каждого будет своя стартовая точка. Стремясь к вершине, идите последовательно и отслеживайте результат в моменте. Поймите, где вы находитесь сейчас, и наметьте дальнейшие шаги. Наши продукты и услуги помогут не только добиться конкретных результатов и контролировать их, но и оценить готовность к переходу на следующий этап.

Делимся опытом — готовим профессионалов

Positive Technologies делится экспертизой с рынком, чтобы формировать сильные команды, готовые к реальным цифровым угрозам. Мы делаем это в рамках двух ключевых направлений: через обучение в центре Positive Education и практику на киберполигоне Standoff

positive education

Обучение с Positive Education

Positive Education — это центр обучения, где формируются ключевые компетенции в области кибербезопасности. Мы создаем комплексные образовательные траектории — от прикладных навыков до стратегического уровня. Обучение строится вокруг ролей, реальных задач бизнеса и технологий

Корпоративные образовательные программы

Разрабатываем обучение под задачи конкретной компании с учетом отрасли, зрелости команды и распределения ролей между подразделениями ИБ, ИТ и бизнесом

Онлайн-тренажер PT EdTechLab

Среда для самостоятельной отработки навыков на реалистичных сценариях атак

Профессиональные программы для специалистов

Развиваем экспертизу в ключевых направлениях: в сфере результативной кибербезопасности, безопасной разработки, реагирования на инциденты, управления ИБ и других

Курсы по эксплуатации продуктов Positive Technologies

Обучаем использовать наши решения эффективно, раскрывая их возможности на практике

Наш подход к обучению

1

Обучение выстроено по уровням — от освоения навыков до формирования стратегии обеспечения кибербезопасности

2

Участники движутся по траектории, закрепляя знания через практику и работу с реальными кейсами

3

Программа может быть адаптирована под уровень зрелости команды и задачи бизнеса

STANDOFF

Практика на киберполигоне Standoff

Платформа Standoff 365 предназначена для повышения защищенности бизнеса с помощью практических киберучений и исследования систем безопасности. Технологическая основа платформы — киберполигон Standoff, где специалисты по ИБ развивают навыки и практикуются без ущерба для безопасности компаний

→ **Думай как хакер, действуй как защитник**
Покажем специалистам вашей команды, как думают хакеры, и научим предугадывать их действия

→ **Экспертиза белых хакеров, которая работает на вас**
Обучение происходит на реальных цепочках атак с кибербитвы Standoff

→ **Практика в реальной среде**
На киберполигоне моделируются угрозы и атаки, сценарии которых основаны на самых свежих данных об инцидентах

→ **Практика, ориентированная на ваши задачи и потребности**
Предоставляем доступ к развернутой отраслевой инфраструктуре со специализированным оборудованием — от контроллеров АСУ ТП до банковских приложений

Пошаговое развитие компетенций

Базовый уровень

Standoff Cyberbones

Самостоятельная практика на базе цепочек атак с кибербитв

→

Продвинутый уровень

Standoff Defend

Комплексное развитие навыков в области кибербезопасности при поддержке ментора

→

Экспертный уровень

Кибербитва Standoff

Отработка взаимодействия команды защиты в условиях интенсивных кибератак

ПРОДУКТЫ ПРОДУКТЫ ПРОДУКТЫ
PT DEPHAZE MAXPATROL VM MAXPA
ОДУКТЫ ПРОДУКТЫ ПРОДУКТЫ ПР
XPATROL HCC PT BLACKBOX PT KNOC
ТЫ ПРОДУКТЫ ПРОДУКТЫ ПРОДУК
NGFW PT APPLICATION FIREWALL PT
ПРОДУКТЫ ПРОДУКТЫ ПРОДУКТЫ
APPLICATION FIREWALL PT ESC PT TH
ОДУКТЫ ПРОДУКТЫ ПРОДУКТЫ ПР
LICATION INSPECTOR PT NAD MAXPA
РОДУКТЫ ПРОДУКТЫ ПРОДУКТЫ П
ONTAINER SECURITY MAXPATROL CA
РОДУКТЫ ПРОДУКТЫ ПРОДУКТЫ П

PT Dephaze

Узнать больше

Автопентест инфраструктуры для регулярной проверки защищенности

Больше 20 лет команда белых хакеров Positive Technologies помогает компаниям по всему миру проверять информационную безопасность и находить уязвимости в защите. Мы объединили экспертизу специалистов и опыт пентестов, чтобы сделать PT Dephaze — инструмент для автоматической проверки состояния инфраструктуры. Он помогает компаниям внедрять практики наступательной безопасности и выявлять уязвимые места защиты до того, как ими воспользуются киберпреступники.

Уникальные технологии и фичи

1 Тактики и техники реальных APT-группировок

PT Dephaze использует популярный у злоумышленников инструментарий, чтобы всегда находить уязвимые места в защите

2 ML-алгоритмы

В основе продукта — технологии машинного обучения, которые ускоряют рутинные процессы и помогают масштабировать тестирование

3 Гибкое технологическое ядро

Позволяет эффективно эмулировать действия злоумышленников, обходить средства защиты и получать привилегированные права доступа в критически важных для бизнеса системах

4 Больше чем BAS

PT Dephaze не просто симулирует атаки для выявления возможных векторов, а проводит реальное тестирование на проникновение, действуя как пентестер

#знаемкакбудутатаковать

Ключевые преимущества

Единственный продукт на рынке, который использует экспертизу как offense-, так и defense-команд, поэтому всегда находит и показывает недостатки в защите инфраструктуры

Наглядно показывает результаты тестирования на проникновение с помощью удобного и понятного отчета, позволяя сразу исправлять найденные недостатки

Безопасен для инфраструктуры, так как дает возможность контролировать тестирование

Разработан с учетом обратной связи от специалистов по ИБ компаний из разных отраслей

Поставляется в виде дистрибутива и не требует сложной подготовки для внедрения и проведения пилотного проекта

Поможет:

- Снизить киберриски и определить слабые места в защите, которыми хакеры воспользуются в первую очередь
- Увеличить эффективность защиты с помощью рекомендаций по устранению проблем безопасности
- Сократить расходы на оценку защищенности за счет оптимизации и масштабирования ручного пентеста

MaxPatrol VM

Узнать больше

Система управления уязвимостями с доставкой информации о трендовых угрозах за 12 часов

Начиная с запуска сканера XSpider в 1998 году мы наращивали экспертизу в области обнаружения самых опасных уязвимостей — эти знания в итоге нашли отражение в системе MaxPatrol VM. Мы понимаем, что важно не только выявить уязвимости, но и организовать системную работу с ними. MaxPatrol VM помогает выстроить процесс, результат которого виден: поддерживает актуальность данных об активах, приоритизирует уязвимости и контролирует их устранение. Больше никаких долгих сканирований и многостраничных отчетов: вся информация доступна в режиме реального времени.

Уникальные технологии и фичи

1 Технология Asset Management

Собирает более 3000 параметров ИТ-активов и позволяет провести полную инвентаризацию инфраструктуры, не оставляя слепых зон

2 ML-алгоритм

Определяет в сети опасные (трендовые) уязвимости быстрее, чем хакеры начнут активно использовать их в атаках

3 Технология быстрой доставки данных

Передает пользователю информацию о трендовых уязвимостях в течение 12 часов с момента их обнаружения и предоставляет рекомендации по исправлению

4 AI-поиск

Упрощает работу с системой и позволяет быстро находить информацию по самым распространенным запросам

#знаемкакбудутатаковать #знаемкакзащититься

Ключевые преимущества

Определяет уровень опасности уязвимостей для инфраструктуры, что позволяет приоритизировать их, установить и контролировать сроки устранения

Поддерживает актуальность данных об активах — при появлении информации о новых уязвимостях может определить их наличие в инфраструктуре без повторного сканирования

Обнаруживает уязвимости веб-приложений и Docker-контейнеров, обеспечивая анализ защищенности максимального количества систем в инфраструктуре

Контролирует состояние безопасности АСУ ТП благодаря пакету экспертизы для промышленных систем

Благодаря открытому API легко интегрируется с любыми системами и встраивается в бизнес-процессы компании

Поможет:

- Обеспечить проактивную защиту от проникновений за счет обнаружения слабых мест в инфраструктуре
- Не упустить уязвимость, которая может привести к ущербу для компании
- Отслеживать все активы инфраструктуры, не допуская появления теневых сегментов
- Наладить эффективное взаимодействие подразделений ИБ и ИТ для быстрого устранения уязвимостей

MaxPatrol HCC

Узнать больше

Ваш инструмент для комплаенс-контроля и харденинга инфраструктуры

Кроме уязвимостей в коде ПО и ОС, которые обнаруживают системы класса vulnerability management, киберугрозу несут и небезопасные настройки систем (избыточные права доступа, открытые порты, нарушения парольной политики и т. п.). Злоумышленники используют их для проникновения в контур компании и продвижения внутри инфраструктуры. Модуль MaxPatrol HCC проверяет конфигурации систем на соответствие российским и международным стандартам практической ИБ, а также внутренним требованиям компании. Мы уверены, что, соблюдая всего 20% самых важных требований безопасности, можно закрыть до 80% уязвимых мест инфраструктуры, и MaxPatrol HCC позволяет справиться с этой задачей.

Уникальные технологии и фичи

1 Технология Asset Management

Позволяет провести полную инвентаризацию сети и собрать данные о параметрах безопасности, а также избавиться от теневых сегментов инфраструктуры

2 Стандарты PT Essentials

Разработаны экспертами Positive Technologies, содержат оптимальный набор проверок для повышения уровня защищенности систем

3 Гибкая настройка

Позволяет писать кастомные требования безопасности для конкретной компании и создавать из них контролируемые стандарты

#знаемкакбудутатаковать #знаемкакзащититься

Ключевые преимущества

Приоритизирует риски и определяет, какие требования наиболее важно соблюсти, чтобы обеспечить максимальную безопасность компании

Позволяет установить в SLA сроки устранения несоответствий требованиям и контролировать изменения в инфраструктуре

Автоматически оценивает соответствие активов новым требованиям без повторного сканирования

Благодаря возможности подключения хостового агента можно сканировать компьютеры сотрудников, в том числе удаленных, а после проверять их на соответствие требованиям безопасности

Поможет:

- Обеспечить превентивную защиту от кибератак за счет корректной настройки систем
- Защитить от атак с использованием уязвимостей, для которых еще не выпущены исправления (0-day)
- Расширить возможности MaxPatrol VM и усилить защищенность инфраструктуры

PT BlackBox

Узнать больше

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

Сложно найти компанию, которая не использовала бы сайт для продвижения своих товаров или услуг, взаимодействия с клиентами и партнерами. Распространенность и общедоступность делает веб-приложения привлекательной целью для хакеров, ведь их взлом позволяет проникнуть во внутреннюю сеть организации. PT BlackBox имитирует действия злоумышленника, который пытается удаленно скомпрометировать веб-приложение или сервис. Продукт не только выявляет сторонние компоненты с известными уязвимостями, но и комбинирует разные методы анализа, чтобы находить проблемы, специфичные для конкретного приложения. Это делает PT BlackBox незаменимым инструментом как для самостоятельного применения, так и в качестве DAST-анализатора, встраиваемого в конвейер непрерывной сборки и доставки (CI/CD) приложений.

Уникальные технологии и фичи

1 Оптимизация использования ресурсов

Определяет повторяющиеся шаблонные страницы и не тратит время на их сканирование

2 Эффективное выявление уязвимостей нулевого дня

Использует комбинацию сигнатурного и эвристического анализа для выявления неизвестных уязвимостей

#знаемкакбудутатаковать

Ключевые преимущества

Методы анализа, разработанные при тесном взаимодействии с ведущими экспертами PT ESC, позволяют выявлять десятки классов уязвимостей (связанные с SQL Injection, XML External Entity, Remote Code Execution, Cross-Site Scripting и другие)

Позволяет выявлять факты раскрытия чувствительной информации, такой как адреса электронной почты, параметры окружения, структура файловой системы и т. п.

Анализ конфигурации сервера, на котором развернуто веб-приложение, позволяет выдать рекомендации по устранению проблем без необходимости вмешиваться в программный код

Проверка приложения на предмет использования сторонних компонентов, содержащих известные уязвимости, позволяет вовремя обновить версии библиотек до более современных и безопасных

При встраивании в конвейер CI/CD продукт позволяет прервать сборку, если обнаружено превышение порогового значения интегрального показателя степени уязвимости приложения

Тонкая настройка сканирования и авторизации дает учесть специфику приложения, при этом анализ проходит в автоматическом режиме

Поможет:

Проанализировать защищенность вашего веб-приложения так, как это делают реальные злоумышленники

Подготовить приложение к проведению тестирования на проникновение, оставив пентестерам только те уязвимости, которые невозможно выявить в автоматическом режиме

PT Knockin

Узнать больше

Онлайн-сервис для проверки защищенности электронной почты

Корпоративная почта — главный канал проникновения хакеров в инфраструктуру. Для предотвращения атак с использованием вредоносного ПО необходимо регулярно тестировать защищенность. PT Knockin симулирует атаки на почту, проверяя эффективность шлюзов, антивирусов, песочниц и других средств защиты, а также дает рекомендации по их настройке, которые позволяют усилить защищенность.

Уникальные технологии и фичи

1 Более 2700 вариаций атак

Подготовлено экспертами Positive Technologies для имитации нападений на почтовый сервер с использованием самого популярного ВПО

2 Проверка защиты за несколько минут

Дает быстрый результат и позволяет оперативно принять компенсирующие меры

3 Рекомендации по настройке защиты

Помогают устранить обнаруженные недостатки. Проверить эффективность рекомендаций можно сразу после внесения изменений

#знаемкакбудутатаковать

Ключевые преимущества

Использует для атаки файлы разных типов, включая запароленные архивы, а также ссылки, по которым можно скачать вредоносный контент. Это позволяет проверить защищенность от разных угроз

Работает онлайн, без установки дополнительного ПО, что позволяет оперативно проверить защищенность почты без влияния на инфраструктуру компании

Предоставляет выбор почтового сервера для отправки тестовых писем, чтобы избежать блокировки атак по адресу отправителя

Оснащен преобразователем отправки на Python, который позволяет изменять семплы ВПО для проведения кастомных симуляций атак

Позволяет гибко настраивать симуляцию атаки: конфигурацию отправляемых писем, частоту проверок и адрес отправителя

Основан на многолетней хакерской экспертизе Positive Technologies

Поможет:

- Обнаружить недостатки защиты для усиления безопасности электронной почты
- Контролировать корректность настроек почтовой защиты после установки обновлений ПО
- При соблюдении рекомендаций устранить основную точку проникновения хакеров в инфраструктуру
- Сделать проверку почтовой защиты регулярной и внести ее в политики безопасности компании

PT NGFW

Исследование BI.ZONE

Узнать больше

Высокопроизводительный и надежный межсетевой экран нового поколения

Высокопроизводительный и надежный межсетевой экран нового поколения PT NGFW защищает периметры компаний, контролирует пользователей и приложения. Мы учли распространенные ошибки в работе межсетевых экранов, прислушались к мнению пользователей и партнеров и создали высокопроизводительный и надежный NGFW. В основе PT NGFW лежит прочный технологический фундамент — модернизированный стек TCP/IP без лишних ресурсоемких операций и собственная сетевая аппаратная платформа.

Собственные разработки

1 Сетевая аппаратная платформа

Гибкая линейка моделей, разработанных без legacy-кода, для защиты любой компании: от небольшого магазина до ЦОД

2 IPS

Поиск и быстрая блокировка угроз за счет алгоритмов глубокого анализа PT DPI с поддержкой Suricata и возможностью загрузки собственных сигнатур

3 Потоковый антивирус

Эффективное предотвращение передачи зараженных файлов благодаря гибким политикам и обширной сигнатурной базе PT ESC

4 URL-фильтрация

Удобный контроль доступа корпоративных пользователей к веб-ресурсам с поддержкой категорирования

Встроенные модули безопасности

- IPS
- URL-фильтрация
- Threat intelligence
- Антивирус

#знаемкакзащититься #знаемкакостановить

Ключевые преимущества

Скорость обработки трафика в режиме фильтрации с контролем приложений — 300 Гбит/с; в режиме IPS — 60 Гбит/с

Более 8500 сигнатур от экспертного центра безопасности PT ESC

ПАК российского производства, сертифицированные ФСТЭК по 4-му классу защиты согласно новым требованиям

Производительность и стабильность по стандарту RFC 9411, подтвержденные тестированием в независимой лаборатории BI.ZONE

Работа на базе центрального процессора с архитектурой x86. Все модели имеют два блока питания, а старшие платформы поддерживают режим горячей замены блоков

Оптимизация политик безопасности в соответствии с бизнес-процессами и централизованная система управления, поддерживающая до 100 000 устройств

Собственные декодеры поддерживают более 1500 мировых и российских приложений, быстро и точно определяют, с какими сервисами работают пользователи

Поможет:

Эффективно защитить как локальный бизнес, так и международные холдинги

Закрыть любые требования к защите, надежности и высокой пропускной способности

Соблюсти требования к средствам защиты для ГИС, КИИ, ИСПДн и АСУ ТП

PT Application Firewall PRO

Узнать больше

Улучшенная версия популярного продукта для непрерывной защиты веб-приложений от кибератак

Мы разработали высокопроизводительный межсетевой экран для непрерывной защиты высоконагруженных enterprise-приложений от внешних киберугроз. Он предоставляет возможность гибкой настройки и может масштабироваться в соответствии с требованиями бизнеса. PT Application Firewall PRO содержит сильнейшую на российском рынке экспертизу по обнаружению и блокировке целенаправленных атак, основанную на собственном опыте проведения пентестов и на данных от исследовательской группы Positive Research и специалистов PT ESC. PT Application Firewall защищает приложения более 700 крупных отечественных компаний.

Уникальные технологии и фичи

1 Точечное машинное обучение

Помогает обнаруживать угрозы определенного класса (например, обфусцированный веб-шелл) и аномалии в трафике без риска появления ложных срабатываний и ухудшения производительности

2 Расширенные механизмы полноценной защиты API-трафика

Обнаруживают атаки внутри API-запросов за счет анализа вложенных данных, поддерживают современные технологии (SOAP, RestAPI, GraphQL API и JWT) и позволяют блокировать атаки из рейтинга OWASP API Security Top 10

3 Собственный модуль распознавания внедрений

Продвинутый механизм точно выявляет атаки с использованием внедрения кода (SQL Injection, JavaScript, OS Command Injection, XPath, LDAP и другие), повышает эффективность защиты и уменьшает число ложных срабатываний

4 Шаблоны политик безопасности для популярных приложений

Готовые редактируемые шаблоны минимизируют время активации защиты, учитывают особенности и специфические уязвимости для каждого языка, совместимы с CMS-решениями Bitrix, OWA, «1С» и другими

5 Виртуальный патчинг

Дополнительный уровень защиты, который помогает выявлять и блокировать попытки эксплуатации до того, как уязвимости будут исправлены

#знаемкакзащититься #знаемкакобнаружить

Ключевые преимущества

Мы анализируем отчеты о реальных векторах атак и уязвимостях приложений, полученные от белых хакеров на платформе Standoff Bug Bounty, анализируем способность PT Application Firewall защищать от таких атак и постоянно совершенствуем продукт

Экспертная база международного уровня пополняется из многообразных источников

Собственная библиотека языковых контекстов совместно с лексическим и синтаксическим анализом запросов позволяет значительно повысить точность обнаружения атак, снижая количество ложных срабатываний, по сравнению с сигнатурным анализом

Заботимся не только о приложении, но и о ваших клиентах: модуль WAF.js предотвращает атаки на пользователей, сохраняя их лояльность и защищая вашу репутацию

Поможет:

- Избежать репутационных и финансовых потерь от последствий успешных кибератак на веб-приложения и сервисы независимо от наличия уязвимостей в коде
- Настроить защиту с учетом особенностей структуры и бизнес-логики приложения
- Защитить legacy-приложения, исправить уязвимости в которых невозможно из-за прекращения поддержки

PT Cloud Application Firewall

Узнать больше

Облачная версия продукта для непрерывной защиты веб-приложений, доступная как малому бизнесу, так и продвинутым технологическим компаниям

Мы сделали enterprise-решение доступным для широкого рынка за счет облачной модели поставки. Продукт предоставляется по подписке (можно выбрать оптимальный тариф), не требует вложений в аппаратное обеспечение и в привлечение специалистов по ИБ. Установка и запуск PT Application Firewall осуществляются всего за день, а управлять им можно из любой точки мира. Это первый по-настоящему облачный продукт Positive Technologies, который защищает от кибератак, утечек данных, кражи учетных записей и нарушения работы веб-приложения.

Уникальные технологии и фичи

1 Собственный модуль распознавания внедрений

Продвинутый механизм точно выявляет атаки с использованием внедрения кода (SQL Injection, JavaScript, OS Command Injection, XPath, LDAP и другие), повышает эффективность защиты и уменьшает число ложных срабатываний

2 Шаблоны политик безопасности для популярных приложений

Готовые редактируемые шаблоны минимизируют время активации защиты, учитывают особенности и специфические уязвимости для каждого языка, совместимы с CMS-решениями Bitrix, OWA, «1С» и другими

3 Виртуальный патчинг

Дополнительный уровень защиты, который способен выявлять и блокировать попытки эксплуатации до того, как уязвимости будут исправлены

#знаемкакзащититься #знаемкакобнаружить

Ключевые преимущества

Полноценный WAF в «облаке». Пользователям доступна полная функциональность PT Application Firewall PRO, включая возможность тонкой настройки профилей защиты

Единственный в России WAF, постоянный тестируемый на Standoff Bug Bounty. Белые хакеры непрерывно ищут уязвимости в продукте, а значит, вы получаете решение, защищенность которого подтверждена и тестируется круглосуточно

Гибкая тарифная сетка. Любой бизнес может подобрать оптимальную цену защиты в зависимости от объема трафика и не переплачивать

Собственная библиотека языковых контекстов совместно с лексическим и синтаксическим анализом запросов позволяет значительно повысить точность обнаружения атак, снижая количество ложных срабатываний, по сравнению с сигнатурным анализом

Поможет:

- Избежать репутационных и финансовых потерь от последствий успешных кибератак на веб-приложения и сервисы
- Отказаться от дорогостоящих годовых лицензий в пользу регулируемой ежемесячной оплаты
- Запустить защиту за считаные часы без каких-либо вложений в инфраструктуру, даже в условиях кибератаки

PT Application Inspector

Узнать больше

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

Уязвимости есть в коде любого приложения, и каждая из них может стать точкой входа для хакера. Мало просто выявить уязвимость — гораздо важнее устранить ее и сделать это быстро. Мы реализовали поиск недостатков кода с высокой достоверностью результатов, благодаря чему по-настоящему опасные уязвимости не затеряются среди ложных срабатываний. PT Application Inspector показывает суть проблемы — это позволяет не только устранять дефекты, но и получать опыт, чтобы избежать подобных ошибок в будущем. Продукт подходит командам с разной степенью зрелости и может использоваться для разового анализа кода или встраиваться в конвейер сборки, позволяя устранять уязвимости на самых ранних этапах разработки.

Уникальные технологии и фичи

1 Абстрактная интерпретация и символьное выполнение

Эти подходы помогают определить возможность эксплуатации уязвимостей и тем самым сокращают количество ложных срабатываний

2 Гибридный подход (SAST и SCA) для выявления уязвимых сторонних библиотек

Наличие в приложении уязвимых библиотек еще не означает, что недостатки в них можно проэксплуатировать. PT Application Inspector не только обнаруживает такие библиотеки, но и определяет, действительно ли приложение использует их уязвимые части, которые могут стать точкой входа для хакера

3 Симбиоз технологий анализа

В ходе статического анализа формируются эксплойты, которые затем используются DAST-ядром для автоматической проверки возможности эксплуатации уязвимости

#знаемкакзащититься

Ключевые преимущества

Сигнатуры и правила в совокупности с более совершенными методами анализа позволяют полностью покрыть код проверками на наличие уязвимостей

PT Application Inspector обнаруживает признаки недекларированных возможностей, что помогает устранять механизмы обхода защиты, целенаправленно заложенные в код

Один инструмент для всей команды: количество анализируемых приложений, сканирований и пользователей неограниченно даже для минимальных конфигураций продукта

Мы знаем, как злоумышленники атакуют системы, и закладываем в продукт экспертизу наших специалистов, обеспечивающих защиту приложений в реальных условиях

Поможет:

- Сократить объем трудозатрат на своевременное выявление и устранение уязвимостей
- Заинтересовать команду темой кибербезопасности и заложить основы для построения эффективных процессов безопасной разработки
- Обеспечить безопасную разработку для команд любого масштаба без дополнительных затрат на лицензии
- Сэкономить ресурсы на устранение недостатков кода после запуска приложения

PT Container Security

Узнать больше

Высокотехнологичное инновационное решение для комплексной защиты инфраструктуры гибридного «облака»

Технологии контейнерной виртуализации упростили построение отказоустойчивых систем, автоматически масштабируемых под имеющуюся нагрузку, но вместе с тем создали сложности для классических средств защиты информации. Непонятно, как сегментировать сеть, узлы в которой то появляются, то исчезают, или анализировать события ИБ, детали которых скрыты или искажены механизмами изолирования процессов. Подобные проблемы решают технологии, обеспечивающие доступ к внутреннему устройству платформ контейнеризации и дополняющие классические средства защиты специфическими функциями. Именно такие технологии мы реализовали в PT Container Security — решении для обеспечения безопасности контейнеров на всех этапах жизненного цикла программных продуктов.

Уникальные технологии и фичи

1 Движок выявления аномалий

Собственный производительный движок для контроля соблюдения политик и поиска аномалий в рантайме контейнеров позволяет гибко настраивать мониторинг событий и выявляет угрозы сразу «из коробки»

2 База уязвимостей

Собственная база уязвимостей ПО, которую собирают и регулярно обновляют наши эксперты из PT ESC, позволяет с высокой точностью выявлять недостатки операционных систем ALT Linux, Astra Linux, Oracle, Red Hat, Ubuntu и «РЕД ОС», а также уязвимости из базы NVD и БДУ ФСТЭК

3 Security as code

Практическая реализация подхода, который позволяет описывать политики безопасности на языках программирования высокого уровня с использованием технологии WebAssembly, дает возможность создавать и кастомизировать конфигурации под нужды клиента

#знаемкакзащититься #знаемкакобнаружить

Ключевые преимущества

Непрерывное многолетнее тестирование продукта на платформе Standoff 365 позволило реализовать механизмы, нацеленные на защиту от реальных злоумышленников, и обеспечить эффективное противодействие техникам из матрицы MITRE ATT&CK

Покрытие всего цикла использования контейнеризованных приложений — от анализа образов инструментов для сборки кода до контроля обращений к API кластера и событий, возникающих в ходе работы

Разнообразие сценариев уведомлений — от отправки электронных писем с результатами анализа до вызова webhook для автоматического реагирования на события, в том числе для перезапуска ПО

Поддержка языков программирования для разработки политик предоставляет неограниченные возможности для реализации логики реагирования на инциденты ИБ, возникающие при работе приложений

Сотни правил для контроля API и манифестов Kubernetes позволяют защитить кластер сразу после установки продукта

Поможет:

- Автоматизировать процессы управления уязвимостями и дефектами в конфигурациях образов и контейнеров на этапе сборки, развертывания и промышленной эксплуатации приложений
- Управлять безопасностью конфигурации кластера Kubernetes
- Проводить мониторинг и реагировать на инциденты ИБ в рантайме контейнеров

MaxPatrol Carbon

Узнать больше

Интеллектуальная система для подготовки ИТ-инфраструктуры к отражению кибератак

Эффективная кибербезопасность должна обеспечивать непрерывность ключевых бизнес-процессов и защиту критически значимых активов от актуальных киберугроз. Для этого нужны подготовленная инфраструктура и системный подход. MaxPatrol Carbon — метапродукт, созданный на основе анализа тактик злоумышленников и многолетнего опыта в повышении защищенности. Он в реальном времени оценивает готовность компании к отражению кибератак, дает рекомендации по усилению защиты и помогает перейти от точечного устранения слабых мест инфраструктуры к управлению киберустойчивостью, фокусируясь на самом важном.

Уникальные технологии и фичи

1 Технология PT Threat Modeling Engine для моделирования угроз

Создает цифровую модель инфраструктуры и показывает возможности передвижения злоумышленников по сети для захвата важных активов и ресурсов

2 Моделирование кибератак на целевые системы

Уникальные алгоритмы рассчитывают маршруты хакера до целевых систем компании с учетом знаний о действиях атакующих и контекста инфраструктуры: сетевой достижимости, уязвимостей, ошибок конфигураций и избыточных привилегий на пути атаки

#метапродукт #знаемкакбудутатаковать #знаемкакзащититься

Ключевые преимущества

Комплексно оценивает опасность маршрутов

Автоматизирует трудоемкий анализ маршрутов по ключевым параметрам: количество шагов, квалификация атакующего, время реализации атаки и ее обнаружения командой ИБ

Централизованно управляет задачами усиления защищенности

Объединяет рекомендации по повышению киберустойчивости — устранение уязвимостей и ошибок конфигураций, инвентаризацию активов, настройку мониторинга и прав доступа, — приоритизируя их выполнение в зависимости от бизнес-рисков

Отслеживает выполнение задач и соблюдение сроков

Позволяет сосредоточить усилия команд ИБ и ИТ на критически важных задачах, отслеживать сроки исполнения рекомендаций и ход работ

Непрерывно контролирует защищенность компании

Комплексно оценивает защищенность целевых систем компании в режиме реального времени и обеспечивает централизованный контроль соответствия требованиям безопасности

Поможет:

- Преобразовать стратегию киберустойчивости в конкретные шаги для ее обеспечения
- Контролировать киберустойчивость и видеть, что происходит в инфраструктуре прямо сейчас
- Эффективно распределять ресурсы и время служб ИТ и ИБ для выполнения задач по повышению защищенности

MaxPatrol SIEM

Узнать больше

Лидер рынка SIEM-систем и основа крупнейших SOC в России с 2015 года

MaxPatrol SIEM обеспечивает безопасность 1000+ компаний в России и странах СНГ. Мы первыми на рынке заложили в систему принцип активоцентричности. Собирая полную информацию о событиях, продукт не оставляет в инфраструктуре слепых зон и не позволяет хакеру оставаться незамеченным. Благодаря PT ESC — одной из сильнейших мировых экспертных команд, изучающих деятельность киберпреступников, — MaxPatrol SIEM обнаруживает 70% когда-либо использованных хакерских техник из матрицы MITRE ATT&CK. А встроенные технологии поведенческого анализа на базе AI и ML автоматически выявляют даже ранее неизвестные атаки и аномалии.

Уникальные технологии и фичи

1 ML-помощник MaxPatrol BAD

Выявляет неизвестные атаки — аномалии и действия хакера, для которых еще не написаны правила корреляции, — а также акцентирует внимание на событиях с высоким уровнем риска

2 Собственная СУБД LogSpace

Разработана специально для SIEM-систем и позволяет хранить в шесть раз больше данных, чем опенсорсные аналоги с теми же ресурсами

3 Технология Asset Management

Точно определяет активы и их состав, что позволяет видеть все обновления инфраструктуры, контролировать полноту и качество сбора событий ИБ

#знаемкакобнаружить

Ключевые преимущества

Высокая производительность и стабильность при работе на потоке более чем с 540 000 событий в секунду со всеми включенными правилами позволяет использовать систему в инфраструктурах любого масштаба

350+ источников «из коробки», а также AI-инструмент для ускорения разработки коннекторов и сокращения затрат на подключение источников

Результат виден сразу после внедрения: система включает 1500+ правил корреляции, избавляя от необходимости писать и настраивать собственный контент

Механизм автоматического исключения ложных срабатываний экономит до 250 человеко-часов в неделю при анализе срабатываний и отборе реальных инцидентов

Система собирает полный контекст атаки благодаря автоматическим механизмам обогащения и позволяет быстро реагировать прямо из карточки события

Телеграм-комьюнити MaxPatrol SIEM с 6000+ участников и портал для свободного обмена наработками помогут легко погрузиться в продукт и быстро решать прикладные задачи

Поможет:

- Защитить от атак любой сложности как небольшие компании, так и инфраструктуры масштаба страны
- Эффективно выявлять угрозы независимо от квалификации специалистов по ИБ
- Обеспечить мониторинг 100% инфраструктуры и контролировать безопасность всех сегментов

MaxPatrol BAD

Узнать больше

ML-помощник в MaxPatrol SIEM для точного обнаружения скрытых и целенаправленных атак

Злоумышленники используют искусственный интеллект, чтобы автоматизировать атаки и маскировать свои действия под легитимную активность. Мы тоже используем ИИ, но для того, чтобы лишить преступников шанса остаться незамеченными. MaxPatrol BAD усиливает традиционные методы защиты, основанные на правилах корреляции и индикаторах компрометации, и выводит обнаружение угроз на новый уровень. Он анализирует поведенческие аномалии, чтобы выявлять атаки в реальном времени, и распознает то, что упускают классические средства защиты.

Уникальные технологии и фичи

1 Выявление целенаправленных атак, использования уязвимостей 0-day и неизвестных техник

Система обнаруживает нетипичную активность, даже если для нее не написаны сигнатуры, благодаря поведенческим моделям и алгоритмам машинного обучения для оценки уровня риска на основе целого спектра факторов

2 Приоритизация задач оператора

MaxPatrol BAD оценивает риск (risk score) всех событий, подсвечивая те, что необходимо обработать в первую очередь, и дает дополнительный контекст происходящего

3 Помогает не упустить false negative и избежать false positive

Приоритизация событий позволяет снизить количество ложных срабатываний, а высокая оценка риска аномальных событий препятствует их попаданию в белый список

#знаемкакобнаружить

Ключевые преимущества

Выявляет аномальное поведение процессов, пользователей и узлов, подозрительные логины, сетевые соединения и IP-адреса с помощью 62 моделей машинного обучения

Поддерживает обнаружение аномальных событий в 14 типах операционных систем, включая Unix

Результаты киберучений Positive Technologies показали, что 85% атак, помеченных в MaxPatrol BAD, не были обнаружены традиционными правилами корреляции

Работает без участия человека — не нужно обновлять и настраивать правила, автономные процессы обнаружения снижают необходимость ручного контроля

Быстрый старт — мы рекомендуем заложить на обучение системы 1 месяц, но результат будет виден сразу после внедрения

Поможет:

- Обнаружить атаку любой сложности, в том числе с использованием ИИ
- Снизить количество рутинной работы аналитика SOC
- Повысить эффективность SOC, улучшить метрики MTTD, MTTR и другие

PT NAD

Узнать больше

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

Злоумышленники совершенствуют вредоносное ПО и методы атак, чтобы быть незаметными для систем защиты, но даже самые изобретательные оставляют следы в трафике. PT NAD обнаруживает в сети скрытые кибератаки, упрощает расследование инцидентов и помогает в проактивном поиске угроз. Кроме того, продукт может сыграть важную роль в решении ИТ-задач: в поиске неучтенного оборудования, проверке соблюдения корпоративных политик и даже в защите от DDoS-атак, когда нужно составить белый список IP-адресов. Благодаря разнообразию областей применения и детальности предоставляемой информации о событиях PT NAD является базовым инструментом SOC.

Уникальные технологии и фичи

1 Собственная технология DPI

Помогает детально разбирать сетевой трафик на любых скоростях и выявлять угрозы, которых нет в базах данных сигнатур IDS, IPS и NGFW

2 Собственная ML-технология

Позволяет выявлять сетевые аномалии, уникальные для конкретной инфраструктуры (supervised learning)

3 Уникальные способы обнаружения

Больше 50 продвинутых модулей, основанных на исследованиях хакерских техник, инструментов и образцов ВПО, используют эвристический анализ, выявляют сложные угрозы, инвентаризируют сеть и коррелируют несвязанные сессии в автоматическом режиме

#знаемкакобнаружить

Ключевые преимущества

Обнаруживает атаки в режиме, близком к реальному времени, — у хакера нет возможности скрыться

Видит точки проникновения и масштаб атаки благодаря использованию восьми методов обнаружения угроз

Выявляет техники атак, популярные на территории России, благодаря индикаторам компрометации, правилам и модулям для анализа от экспертного центра безопасности PT ESC

Внедряется за один час и показывает моментальный результат благодаря 10 000+ правил, доступных «из коробки»

Позволяет подключать облачное хранилище разнообразного трафика и метаданных для масштабирования системы в сложных инфраструктурах

Максимальная детализация при разборе трафика — определяет больше 100 сетевых протоколов и 13 протоколов туннелирования, разбирает 35 наиболее распространенных из них до уровня L7

Поможет:

- Обнаружить в инфраструктуре скрытое присутствие хакера
- Расследовать сетевые атаки, чтобы усилить защиту и предотвратить подобные инциденты в будущем
- Выстроить процесс threat hunting и обнаруживать угрозы, которые не выявляются стандартными средствами защиты
- Полностью устранить теневую инфраструктуру

MaxPatrol EDR

Узнать больше

Автономный агент для защиты конечных устройств от сложных и целевых атак

Компьютеры, ноутбуки, серверы — все это входит в ИТ-ландшафт компании и вызывает интерес у любого хакера. С их помощью злоумышленники могут добраться до данных, получить доступ к внутренней сети и причинить вам серьезный ущерб. Чтобы вовремя обнаруживать кибератаки и реагировать на них, важно знать, что происходит на конечных устройствах. MaxPatrol EDR непрерывно мониторит устройства и виртуальные рабочие места, обнаруживает комплексные угрозы и моментально останавливает вредоносные действия.

Уникальные технологии и фичи

1 Обнаружение угроз в динамике

Сочетает статический и поведенческий анализ, чтобы выявлять действия хакера на ранних этапах атаки. Содержит более 700 правил корреляции и 6000 YARA-правил для обнаружения сложных угроз

2 Автономная работа

Для анализа и реагирования EDR-агенту, установленному на узле, не нужно подключаться к корпоративной сети и интернету — это позволяет защищать устройства удаленных сотрудников

3 Синергия с решениями Positive Technologies для защиты инфраструктуры

Усиливает возможности MaxPatrol SIEM, MaxPatrol VM и PT Sandbox, расширяя покрытие инфраструктуры, выявляя угрозы и реагируя на них

#знаемкакзащититься #знаемкакобнаружить #знаемкакостановить

Ключевые преимущества

Поведенческий анализ позволяет обнаруживать сложные атаки, в которых используются легитимные инструменты и которые из-за этого могут быть пропущены сигнатурными средствами защиты

Благодаря постоянно пополняющимся правилам от экспертов PT ESC выявляет 79% популярных тактик и техник киберпреступников из матрицы MITRE ATT&CK

Предоставляет 10+ вариантов реагирования, которые можно автоматизировать (изолирование узлов, завершение процессов, удаление вредоносных файлов, блокировка опасных подключений, дополнительный анализ подозрительных процессов и т. п.)

Выступает в роли единого агента для обнаружения, реагирования, сбора телеметрии и данных об уязвимостях на устройствах с Windows, Linux, macOS и в инфраструктуре виртуальных рабочих столов (VDI)

Благодаря модульной архитектуре можно гибко настроить решение под особенности инфраструктуры, снизить нагрузку и учесть уникальные требования SOC

Поддерживает 30+ версий популярных ОС, включая сертифицированные российские системы

Поможет:

- Непрерывно контролировать безопасность конечных устройств и автоматически реагировать на угрозы
- Перевести защиту инфраструктуры от APT-атак на качественно новый уровень
- Надежно защитить устройства сотрудников и компании даже за пределами офиса

PT Sandbox

Узнать больше

Песочница для защиты от целевых атак с использованием сложных и новых вредоносных программ

В каждой второй кибератаке для обхода защиты хакеры используют вредоносное ПО под видом обычных файлов и ссылок. Чтобы обнаружить неизвестный вредоносный код до того, как тот попадет на компьютер ничего не подозревающего пользователя, необходима изолированная виртуальная среда — песочница. Чтобы сделать по-настоящему хорошую песочницу, нужна мощная экспертиза в обнаружении и расследовании сложных инцидентов с применением ВПО. PT Sandbox использует знания и многолетний опыт специалистов PT ESC, поэтому обеспечивает высокое качество анализа вредоносных программ и предотвращает их проникновение в инфраструктуру. Информация о новых угрозах попадает в продукт всего за 2,5 часа, позволяя оперативно реагировать на меняющийся ландшафт атак.

Уникальные технологии и фичи

1 Многоуровневое обнаружение ВПО

Обнаружение не только на уровне пользовательского и ядерного пространства, но и на уровне гипервизора помогает выявлять специфическое ВПО, такое как руткиты и буткиты

2 Уникальный асинхронный API

Позволяет встраивать PT Sandbox в любую инфраструктуру и контролировать все каналы передачи файлов и ссылок

3 Собственные ML-технологии

С высокой точностью выявляют аномальное поведение вредоносных программ, позволяя эффективно обнаруживать неизвестные угрозы

#знаемкакзащититься #знаемкакобнаружить

Ключевые преимущества

Покрытие 100% тактик и техник, связанных с ВПО, из матрицы MITRE ATT&CK для Windows- и Linux-систем обеспечивает результативную защиту

Гибкие возможности кастомизации виртуальных сред помогают выявить угрозы с учетом отраслевой специфики компании

Точное обнаружение угроз обеспечивается благодаря комбинации поведенческого анализа с настраиваемым машинным обучением, статического анализа несколькими антивирусами, собственных YARA-правил, репутационного анализа и проверки содержимого ссылок

Гарантированная защита от шифровальщиков за счет конфигурируемого набора файлов-приманок обезопасит бизнес от шифрования данных

Защита от самых действенных техник обнаружения песочниц (Pafish на 100%, AI-Khaser — на 95%) исключает вероятность пропустить вредоносный объект

Механизм автоматического исключения ложных срабатываний экономит до 250 человеко-часов в неделю при анализе срабатываний и отборе реальных инцидентов

Поможет:

- Защититься как от массовых, так и от целевых атак с использованием ВПО
- Предотвратить попадание вредоносных программ в контур организации
- Проверять файлы и ссылки из почтового трафика, файловых хранилищ, передаваемые по сетевому трафику и полученные от любых источников

PT ISIM

Узнать больше

Единая система мониторинга и реагирования на события ИТ и ИБ в промышленных инфраструктурах

Цифровизация сделала технологические сети не менее уязвимыми, чем корпоративные. Если раньше АСУ ТП были защищены от кибератак благодаря своей физической изоляции, то с развитием ИТ-инфраструктуры, которая помогает совершенствовать процессы, у хакеров появилась лазейка к ПО для оборудования. А вмешательство в работу АСУ ТП может привести к серьезным авариям и даже технологическим катастрофам. PT ISIM помогает отслеживать и контролировать изменения в промышленных ИТ-инфраструктурах, обнаруживает инциденты и дополняет их технологическими данными, позволяя вовремя выявлять угрозы для критически важных систем предприятий.

Уникальные технологии и фичи

1 Визуализация и контроль изменений промышленных ИТ-инфраструктур

Предоставляет максимум информации о технологической сети: ресурсах, структуре, пользователях и сетевых взаимодействиях

2 Мониторинг безопасности по трафику и на конечных узлах

Глубокий разбор более 130 промышленных и общесетевых протоколов, а также анализ событий в системном и прикладном индустриальном ПО на конечных точках позволяет обнаруживать события ИБ, подозрительные и потенциально опасные операции пользователей

3 Объединение множества инцидентов в цепочки событий

Помогает быстро определить направление и цель атаки, проактивно реагировать на угрозы и расследовать инциденты

#знаемкакобнаружить

Ключевые преимущества

Использует для обнаружения угроз более 10 000 правил и индикаторов, охватывающих промышленное ПО и оборудование в инфраструктурах на Windows и Linux

Поддерживает российские операционные и SCADA-системы, минимизируя риски промышленных предприятий и других объектов КИИ, которые могут возникнуть при импортозамещении

Обнаруживает целенаправленные атаки благодаря контролю параметров технологического процесса, выявлению отклонений при скрытой компрометации SCADA-систем и обогащению событий технологическим контекстом

Сертифицирован ФСТЭК России на соответствие требованиям профиля защиты СОВ уровня сети не ниже четвертого класса

Поможет:

- Инвентаризировать и контролировать безопасность инфраструктур любого масштаба — от одной технологической установки до крупного холдинга
- Выполнять задачи службе ИБ, ИТ-администраторам и ответственным за непрерывность производства
- Обеспечить непрерывность технологических процессов
- Обеспечить выполнение регуляторных требований к безопасности объектов КИИ
- Передавать актуальные данные о состоянии промышленных ИТ-инфраструктур во внешние бизнес-системы предприятия

PT Threat Intelligence Feeds

Узнать больше

Уникальные потоки данных об угрозах

Данные об угрозах помогают выстроить надежную защиту, потому что опираются на сведения о реальных атаках. Но чтобы добыть их, нужны серьезные аналитические ресурсы. Или можно обратиться к опыту сильнейшей в России команды кибербразведки. PT ESC — наши исследователи угроз, эксперты по реагированию и безопасности, которые изучают деятельность хакерских группировок, техники и инструменты злоумышленников. На результатах их работы основаны PT Threat Intelligence Feeds — потоки данных, которые служат для информирования команд ИБ об актуальных киберугрозах.

Уникальные технологии и фичи

1 Проверенные индикаторы компрометации

Мы получаем индикаторы в ходе расследований реальных атак и исследования деятельности APT-группировок. Кроме того, доступны данные обезличенной телеметрии из инсталляций продуктов Positive Technologies, которые позволяют понять, что происходит в мире ИБ прямо сейчас

2 Расширенный контекст

Обогащение индикаторов компрометации дополнительными данными дает аналитикам SOC необходимую информацию, чтобы разработать план устранения угрозы и повысить скорость реагирования на инциденты

3 Готовые наборы данных

Индикаторы компрометации объединены в 30+ фидов по целям их применения: для выявления таргетированных атак, определенных семейств ВПО, конкретных вредоносных кампаний и т. п.

#знаемкакобнаружить

Ключевые преимущества

Обогащает данными средства защиты и повышает их эффективность, что позволяет обнаруживать и предотвращать атаки на ранних этапах

Помогает приоритизировать угрозы, оценить возможный ущерб компании от их реализации и сфокусироваться на предотвращении самых опасных

Поддерживает разные форматы и широкий перечень средств защиты, который постоянно растет. Благодаря этому легко интегрируется с продуктами Positive Technologies и других вендоров

Поможет:

- На ранней стадии выявлять угрозы и превентивно их блокировать
- Реализовать проактивную защиту за счет регулярно обновляемых сведений об угрозах
- Отслеживать угрозы, актуальные для конкретной компании или отрасли, и применять адекватные защитные меры

MaxPatrol O2

Узнать больше

Автопилот для обнаружения и остановки кибератак с минимальным участием человека

Обеспечение киберзащиты компании в режиме 24/7 требует создания SOC с командой высококвалифицированных экспертов. MaxPatrol O2 меняет этот подход. Метапродукт автоматизирует все сложные и рутинные процессы — от обнаружения и расследования кибератак до оперативного реагирования на них, — привлекая специалиста только для подтверждения угрозы и запуска сценария реагирования. Это позволяет достичь экспертного уровня киберзащиты, сохраняя компактную команду специалистов по ИБ.

Уникальные технологии и фичи

1 Выявление цепочек кибератак в реальном времени

Анализирует множество отдельных событий из разных средств защиты, выявляя цепочки подозрительных активностей, которые характерны для атаки

2 Авторасследование инцидентов

Восстанавливает хронологию действий злоумышленника на основе знаний и опыта экспертов PT ESC, а после визуализирует полный контекст атаки для аналитика

3 Остановка атаки за несколько минут

Генерирует сценарий реагирования для каждой цепочки и выполняет его по нажатию одной кнопки, что позволяет быстро остановить атаку и вернуть контроль над захваченными ресурсами без привлечения ИТ-специалистов

#метапродукт #знаемкакобнаружить #знаемкакостановить

Ключевые преимущества

Максимальная устойчивость к кибератакам любого уровня

Благодаря автоматическим механизмам обнаружения повышает уровень экспертизы SOC, обеспечивая выявление и отражение даже самых сложных кибератак

Быстродействие в условиях ограниченных ресурсов

Помогает компактной команде действовать более продуктивно: сокращает время реагирования на кибератаки, снижает нагрузку и позволяет выполнять больший объем работы без расширения штата

AI-технологии в помощь человеку

ML-алгоритмы автоматически выявляют аномалии, определяют неочевидные связи между событиями, упрощают анализ цепочек активностей и повышают скорость принятия решений

Единое рабочее пространство

Обеспечивает удобный процесс расследования и позволяет запускать реагирование в одном интерфейсе, без переключения между несколькими консолями

Защита, подтвержденная практикой

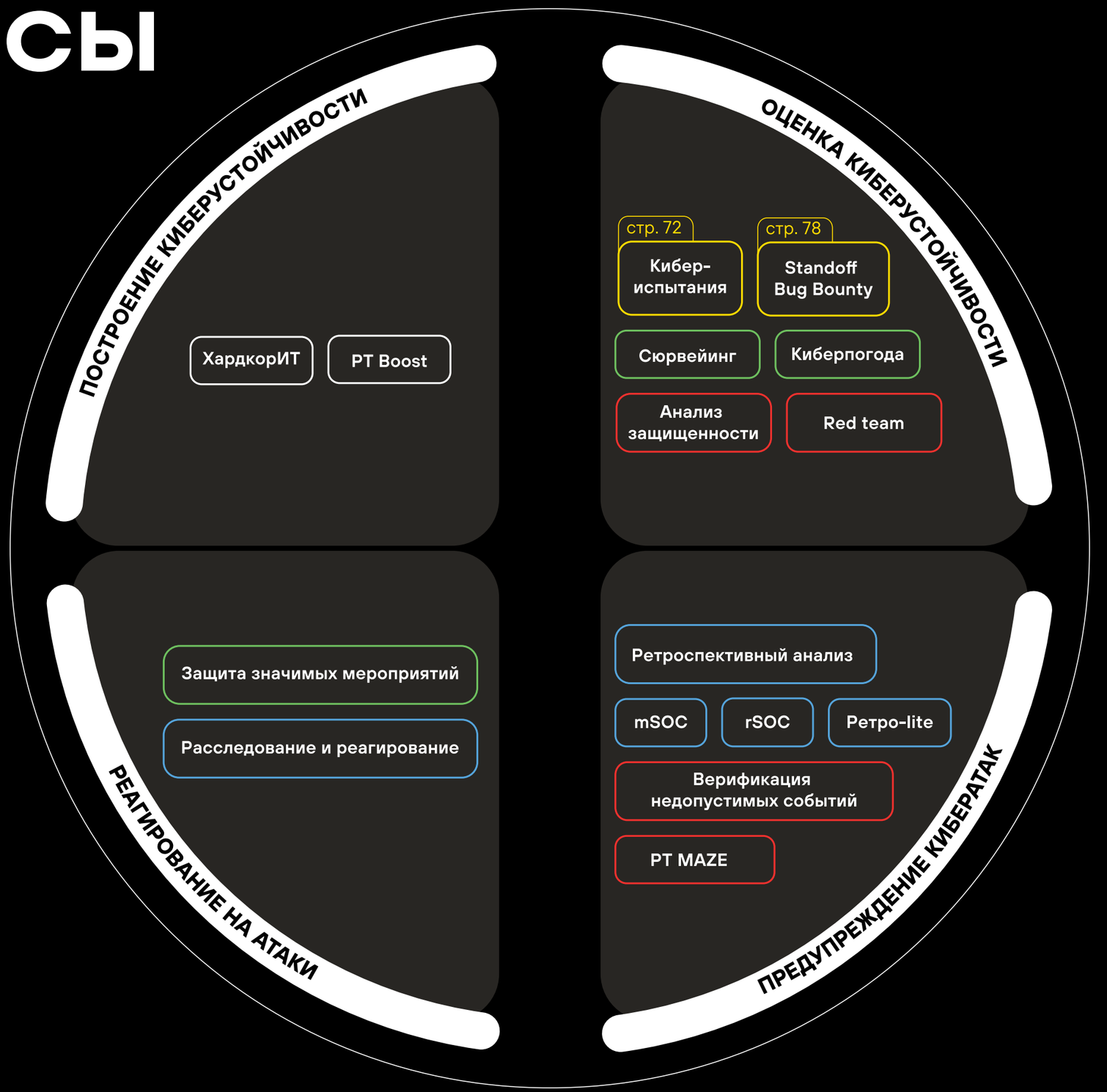
Обеспечивает защиту больших инфраструктур, обнаруживая среди прочего атаки APT-группировок мирового уровня, и регулярно доказывает свою эффективность в ходе киберучений

Поможет:

- Защитить компанию от недопустимых событий
- В десятки раз сократить время расследования инцидентов и реагирования на них
- Построить эффективный SOC даже в условиях нехватки квалифицированных специалистов

ЭКСПЕРТНЫЕ СЕРВИСЫ POSITIVE
ИТ PT BOOST ЗАЩИТА ЗНАЧИМЫХ М
ЕРТНЫЕ СЕРВИСЫ POSITIVE TECHN
БЕРПОГОДА СЮРВЕЙИНГ КИБЕРИСП
РТНЫЕ СЕРВИСЫ POSITIVE TECHN
ИЗ ЗАЩИЩЕННОСТИ STANDOFF BU
КСПЕРТНЫЕ СЕРВИСЫ POSITIVE TE
ОСПЕКТИВНЫЙ АНАЛИЗ MSOC RSOC
СПЕРТНЫЕ СЕРВИСЫ POSITIVE TEC
УСТИМЫХ СОБЫТИЙ PT MAZE РЕТР
КСПЕРТНЫЕ СЕРВИСЫ POSITIVE TE
ОВАНИЕ И РЕАГИРОВАНИЕ КИБЕРП
ЭКСПЕРТНЫЕ СЕРВИСЫ POSITIVE

ЭКСПЕРТНЫЕ СЕРВИСЫ



Услуги по оценке защищенности от команды белых хакеров PT SWARM, нацеленные на обнаружение слабых мест в системе безопасности и предупреждение возможных атак на инфраструктуру

Услуги экспертного центра безопасности PT ESC по обнаружению, расследованию сложных инцидентов и реагированию на них, а также по мониторингу безопасности корпоративных систем

Комплексные экспертные сервисы Positive Technologies по оценке киберустойчивости

Услуги по построению киберустойчивой ИТ-инфраструктуры

Услуги платформы Standoff 365 помогают бизнесу на практике проверять устойчивость систем к киберугрозам и комплексно прокачивать навыки мониторинга, расследования и реагирования специалистов по ИБ

PT MAZE

Узнать больше

Сервис по защите мобильных приложений от реверс-инжиниринга

Мобильные приложения являются желанной целью для хакеров, при этом одной из самых распространенных их проблем остается недостаточная защищенность кода. PT MAZE — первый в России сервис для защиты приложений от реверс-инжиниринга, разработанный белыми хакерами. Мы много лет анализируем мобильные приложения, знаем, как действуют злоумышленники, и можем выстроить правильную защиту. Сервис полностью прозрачен для разработчика и подходит для приложений на Android и iOS.

Уникальные технологии и фичи

1 Не требует доступа к исходному коду

PT MAZE работает с бинарными сборками, которые доступны после публикации приложений, что исключает риски, связанные с вмешательством в исходный код

2 Модификация вместо дополнения

PT MAZE внедряет механизмы безопасности в приложение, модифицируя исполняемые файлы, что не позволяет злоумышленникам обойти защиту

3 Децентрализация

Каждый модуль может настраиваться и работает независимо, что делает защиту распределенной внутри приложения

4 SaaS

Загруженное мобильное приложение модифицируется на собственном сервере PT MAZE. При этом владельцу приложения доступны все версии модификаций

5 Не требует настройки

Мы подготовили стандартные конфигурации защиты, чтобы вы могли запустить сервис нажатием одной кнопки — без долгой настройки

#знаемкакзаранеезащититься

Ключевые преимущества

Для Android

Защита в статике

- Обфускация (запутывание) кода приложения
- Сокрытие бизнес-логики приложения (исполняемые файлы байт-кода)
- Контроль целостности приложения — защита от переупаковки в целях исследования или несанкционированного создания копий

Защита в динамике

- Контроль и аттестация устройства при запуске приложения
- Проверка разблокированного загрузчика
- Защита от секретов памяти
- Защита от обнаружения прав суперпользователя
- Проверка на кастомные прошивки устройства при загрузке приложения

Для iOS

- Обфускация (запутывание) защитного кода
- Обнаружение устройства с джейлбрейком при запуске приложения
- Частичное шифрование файлов приложения
- Закрепление защитной библиотеки PT MAZE в приложении

Поможет:

Защитить приложение от создания клонов и модификаций, несанкционированной разблокировки платных и иных ограниченных функций, от поиска уязвимостей и изучения внутреннего устройства третьими лицами

Используется криптография по ГОСТ: хеш-функция ГОСТ Р 34.11-212 для проверки целостности приложения и подлинности установления TLS-соединения, а также симметричное блочное шифрование ГОСТ Р 34.12-215 (ключ 256 бит)

Оценка защищенности и тестирование от PT SWARM

Команда белых хакеров Positive Technologies поможет обнаружить слабые места в системе безопасности и предупредить возможные атаки на инфраструктуру

Комплексное тестирование на проникновение (пентест)

Поиск векторов атак на инфраструктуру со стороны внешнего нарушителя и пользователя, получившего доступ к определенным сегментам сети

Red team

Эмуляция целенаправленных кибератак для проверки эффективности реагирования службы ИБ на инциденты информационной безопасности

Оценка уровня защищенности инфраструктуры в соответствии с Указом Президента № 250

Моделирование атак и разработка плана мероприятий по повышению общего уровня кибербезопасности путем модернизации инфраструктуры ИТ и ИБ

Верификация недопустимых событий

Экспертная оценка уровня защищенности инфраструктуры от недопустимых событий, основанная на моделировании атак

Анализ защищенности

Мы поможем выявить уязвимости и другие недостатки, которые могут быть использованы для взлома, чтобы вы могли вовремя принять меры для их устранения

АСУ ТП

Выявление путей проникновения в сетевой сегмент АСУ ТП и технических уязвимостей, связанных с недостатками архитектуры и ошибками разработки ПО

Беспроводные сети

Выявление недостатков в архитектуре и организации беспроводного доступа, которые может использовать злоумышленник

Инфраструктура на базе платформы контейнеризации приложений

Выявление уязвимостей в контейнерной среде и получение объективной независимой оценки ее защищенности

Внешний периметр

Разовое или периодическое инструментальное сканирование объектов сетевого периметра

Мобильные, веб-приложения и системы ДБО

Выявление уязвимостей и проблем, допущенных в ходе проектирования, разработки и эксплуатации приложений

Банкоматы, платежные терминалы и постаматы

Оценка уровня защищенности от фрода, несанкционированного доступа к ячейкам, от утечки персональных данных и типовых атак

Блокчейн-приложения

Поиск уязвимостей в бизнес-логике, уязвимых и неэффективных шаблонов проектирования, проверка соответствия размещенной логики смарт-контракта исходному коду

Реагирование и защита силами PT ESC

Экспертный центр безопасности Positive Technologies оказывает услуги по обнаружению, расследованию сложных инцидентов и реагированию на них, а также проводит мониторинг безопасности корпоративных систем

Нам доверяют самое важное

Экспертиза команды PT ESC проверена в ходе расследования инцидентов и защиты систем на ключевых событиях международного и федерального уровня

- Общероссийское голосование в 2020 году
- Чемпионат мира по футболу в 2018 году
- «Игры будущего» в 2024 году

Реагирование на инциденты

Мы остановим развитие инцидента, восстановим хронологию событий ИБ, приведших к нему, оценим уровень опасности и дадим рекомендации для предотвращения подобных инцидентов в будущем

Ретроспективный анализ

Выявим факты текущих и прошлых атак, следы компрометации объектов инфраструктуры и критически важных компонентов. Покажем, к каким последствиям привела атака, и оценим, к каким проблемам инцидент может привести в будущем

Мониторинг и анализ инцидентов

Выполним мониторинг вашей инфраструктуры и реагирование на инциденты с помощью средств защиты Positive Technologies

Ретроспективный анализ событий ИБ

Обнаруживаем прошлые атаки и следы компрометации в ИТ-инфраструктуре, оцениваем и прогнозируем связанные с ними риски

Когда необходим ретроспективный анализ

1. **Есть отраслевые риски**
   Если сфера, в которой работает ваша компания, входит в топ атакуемых, нужно убедиться, что хакеры не добрались до вас
2. **Есть изменения**
   Если в компании обновились политики безопасности и вы хотите проверить системы на соответствие новым правилам
3. **Есть подозрения**
   Если вы обнаружили следы подозрительной активности и хотите проверить, был ли взлом и до чего хакеры смогли дотянуться
4. **Есть факт восстановлений**
   Если пришлось делать восстановление данных из резервных копий, будет полезно узнать, нет ли на восстановленных узлах признаков компрометации

Подход Positive Technologies

Полный ретроспективный анализ

Сигнатурное сканирование файловой системы, оперативной памяти узлов инфраструктуры, а также сбор и глубокий анализ ретроспективных и имеющихся forensic-артефактов

Ретро-lite

Сигнатурное сканирование файловой системы, оперативной памяти наиболее значимых узлов инфраструктуры, сбор и быстрый анализ ретроспективных и имеющихся forensic-артефактов

Специализированный ретроспективный анализ

Анализ событий ИБ, зафиксированных отдельными инструментами (MaxPatrol SIEM, PT NAD, PT Application Firewall), а также разработка рекомендаций по усилению защиты

Реагирование и расследование

Восстанавливаем хронологию и обстоятельства инцидента и локализуем атаку, организуем проактивное реагирование и устранение последствий

Что проверяем

ИТ-инфраструктуру

Какие задачи решаем

Определяем границы инцидента

Устраняем последствия инцидента совместно с вашей командой

Оцениваем масштаб и характер нанесенного ущерба

Даем рекомендации по предотвращению повторных инцидентов

Как устроено расследование и реагирование

1. Опрашиваем всех, кто может знать об инциденте
2. Оцениваем, насколько опасен инцидент и к каким последствиям он может привести
3. Определяем причину успешной атаки
4. Выявляем факты компрометации и признаки инцидентов
5. Собираем и анализируем события ИБ
6. Восстанавливаем цепочку атаки
7. Формируем антикризисную команду с вашей службой ИБ
8. Устраняем последствия и подсказываем, как усилить защиту

mSOC | Managed SOC

Профессионально управляем средствами защиты Positive Technologies в вашей инфраструктуре для мониторинга и реагирования на инциденты ИБ

Что проверяем

ИТ-инфраструктуру

Эффективность работы службы безопасности

Какие задачи решаем

Непрерывный мониторинг инфраструктуры, обнаружение и анализ инцидентов и кибератак

Реагирование на инциденты при помощи агентов MaxPatrol EDR

Регулярный ретроспективный поиск следов злоумышленников и обнаружение киберугроз

Киберпогода

Узнайте состояние киберпространства вокруг вашей компании и будьте на несколько шагов впереди злоумышленников

>60%
составил рост общего числа кибератак в 2024 году

5 дней
в среднем нужно хакерам, чтобы проникнуть во внутреннюю сеть

3 шага
требуется для проникновения в локальную сеть в 75% атак

10 дней
необходимо для реализации недопустимого для бизнеса события

Что мы предлагаем

Мы оценим возможность реализации кибератак и угроз безопасности на основе публично доступной информации о вашей компании и хакерской активности

Как устроен прогноз киберпогоды

1 Заключение договора

Подписываем договор и соглашения о неразглашении информации, получаем от вас перечень оцениваемых организаций, список узлов и разрешения (например, на сканирование внешнего периметра или на обработку персональных данных, обнаруженных в ходе поиска утечек)

2 Оценка и аналитика

- Собираем данные более чем из 1000 источников (открытых, неиндексируемых и находящихся в дарквебе)
- Проверяем данные и обогащаем их при помощи внутренней экспертизы Positive Technologies
- Оцениваем киберугрозы с использованием технологий искусственного интеллекта

3 Подготовка отчета

Представляем отчет, включающий оценку состояния киберпространства (открытые порты, забытые сервисы, уязвимые системы, теневые активы, фишинговые сайты, скомпрометированные данные и другое), а также рекомендации и стратегии по снижению риска кибератак

4 Результат

- Детальная информация о вашей компании на основе анализа открытых данных
- Данные об атаках на компании из вашей отрасли
- Оценка киберугроз для вашей компании
- Возможность минимизации риска кибератак

Заказать пилотный проект

Напишите нам, чтобы организовать пилотный проект киберпогоды в вашей компании

secserv@ptsecurity.com

Сюрвейинг

Сервис, позволяющий получить независимую комплексную оценку киберустойчивости любой организации, взаимодействующей с вашей компанией

>80% утечек
происходят в результате кибератак, а регуляторы ужесточают ответственность и повышают требования к защите данных

41% пострадавших компаний
связывают кибератаки с другими организациями

50% компаний
не понимают, какие уязвимости есть в цепочке поставок и во взаимодействии с другими организациями

Как работает сюрвейинг

1. Вместе с вами формируем перечень дочерних организаций и партнеров для оценки и составляем план
2. Подписываем договор и согласие на проведение оценки устойчивости к кибератакам с каждой организацией
3. Проводим объективную оценку киберустойчивости: исследуем процессы, внешний периметр (включая веб-ресурсы и почту), определяем утечки, проводим ретроспективный анализ и другое
4. Представляем отчет с рейтингом киберустойчивости, выявленными недостатками и рекомендациями по их устранению

Что вы получаете

Детальную оценку состояния инфраструктуры клиента и вероятности совершения кибератаки на него

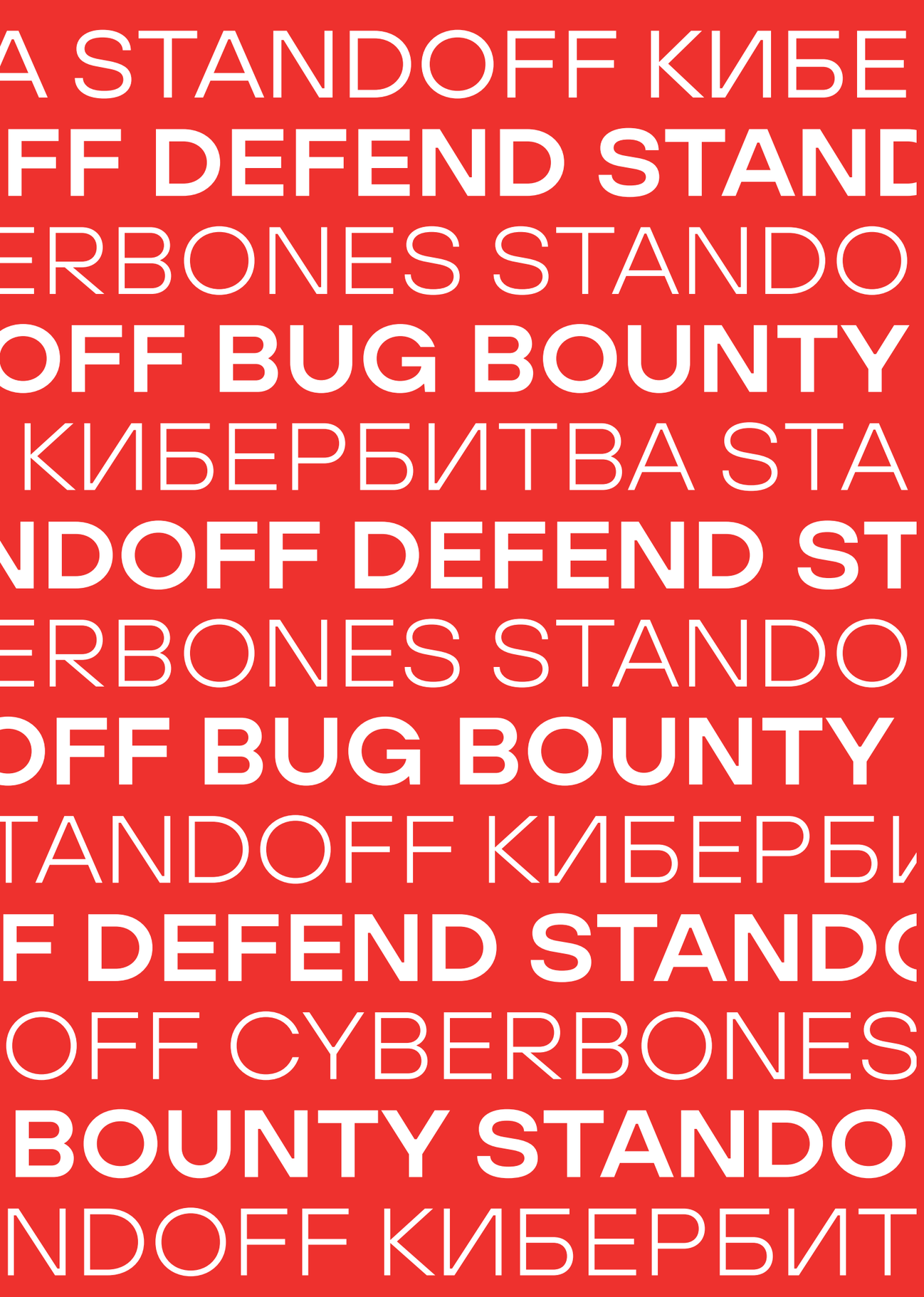
Лояльность и доверие клиентов за счет объективной оценки

Возможность предлагать выгодные условия страхования организациям с высоким уровнем киберзащиты

Возможность пересматривать условия полисов в зависимости от уровня защищенности клиента

Возможность минимизировать вероятность наступления страховых случаев и убытков

Дополнительные аналитические данные для разработки новых страховых продуктов



ПРОДУКТЫ ПЛАТФОРМЫ STANDOFF 365

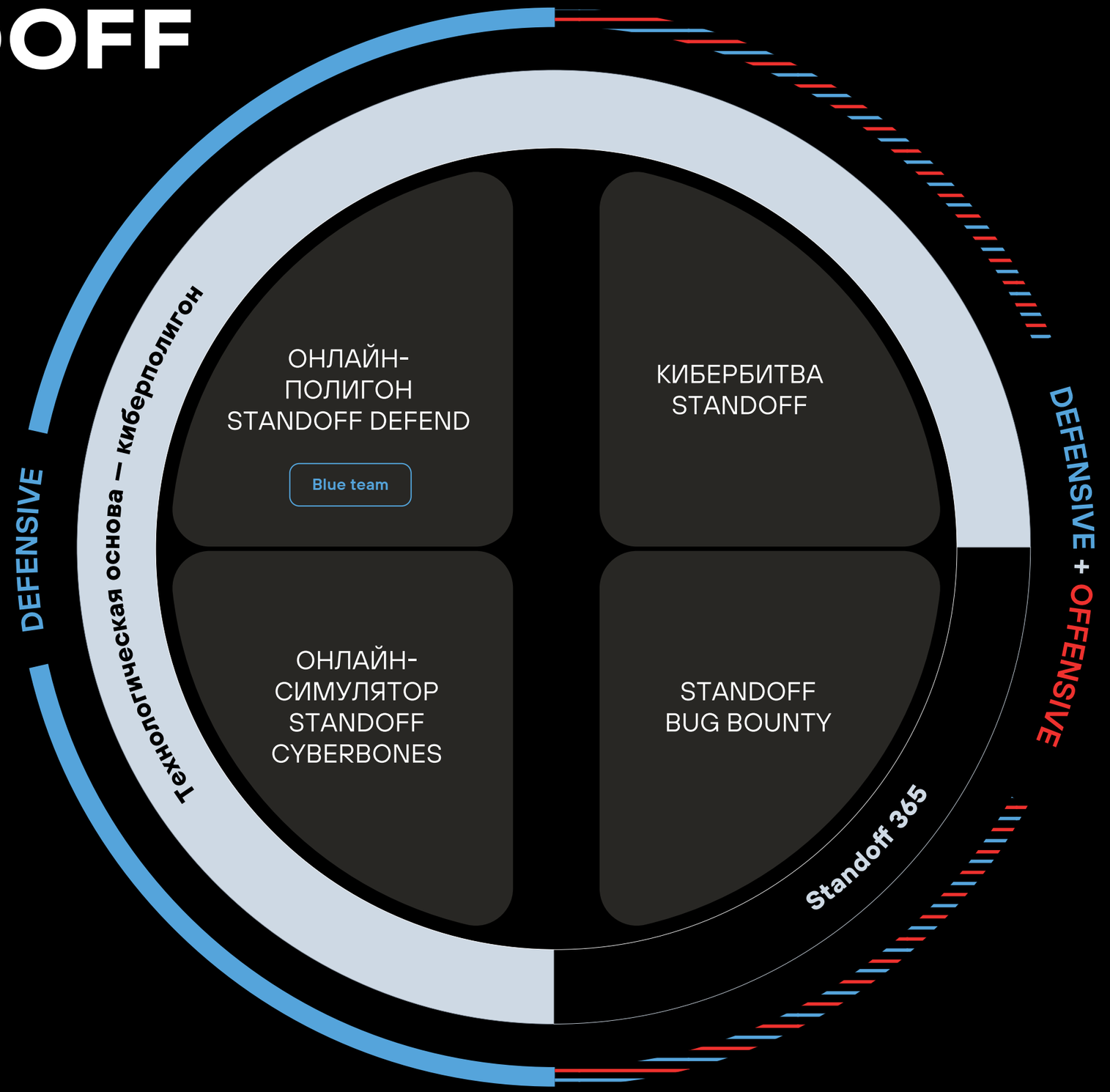
Здесь бизнес работает с белыми хакерами

Платформа Standoff 365 предназначена для повышения защищенности бизнеса с помощью практических киберучений и исследования систем безопасности.

Решения платформы помогают:

- Бизнесу — на практике проверять устойчивость систем к киберугрозам и усиливать навыки своих специалистов по ИБ для повышения качества защиты компании
- Исследователям безопасности — изучать различные инфраструктуры, улучшать свои методы поиска уязвимостей и получать вознаграждение

ЧТО ТАКОЕ STANDOFF



Кибербитва Standoff

Международное соревнование для повышения уровня зрелости службы ИБ в условиях интенсивных кибератак

Международное офлайн-мероприятие, которое с 2016 года объединяет специалистов по ИБ и исследователей безопасности для проверки и оттачивания навыков на примере максимально реалистичной инфраструктуры. Каждый участник кибербитвы может смело тестировать свои стратегии, чтобы использовать полученный опыт в повседневной работе.

Уникальность

1 Самый масштабный и узнаваемый ивент в своем сегменте

За 9 лет было проведено 14 битв, в которых совокупно приняло участие более 5000 экспертов по кибербезопасности, а более 500 компаний стали устойчивее к кибератакам

2 Самое большое комьюнити белых хакеров

Специалисты могут погрузиться в условия настоящего сражения с участием лучших атакующих для подготовки к отражению любых кибератак

3 Реалистичные отраслевые сегменты

Здесь воссозданы инфраструктуры и воспроизведены бизнес-процессы 10 отраслей экономики, включая энергетическую, атомную, металлургическую и банковский сектор

4 Наглядная визуализация последствий атак

На макете виртуального государства в режиме реального времени отображаются последствия действий хакеров: прорыв нефтепровода, отключение электричества или сход грузового поезда с рельсов

#знаемкакпроверитьипрокачатьнавыки

Узнать больше

Решаемые задачи

- Проверка навыков практической кибербезопасности
- Знакомство с разными техниками кибератак и инструментами защиты
- Возможность прокачать уровень зрелости службы ИБ в условиях интенсивных кибератак для эффективной защиты организаций в реальной жизни
- Отработка гипотез по защите от киберугроз без последствий для компании
- Лучшее понимание хода мыслей злоумышленников на примере реалистичной инфраструктуры

Поможет:

- Проверить слаженность работы команды ИБ под воздействием интенсивных кибератак
- Проверить гипотезы и стратегии защиты компании в условиях реальных киберугроз
- Познакомиться с разными техниками злоумышленников и инструментами защиты
- Лучше понимать ход мыслей хакеров на примере реалистичной инфраструктуры

Standoff Defend

Онлайн-полигон для непрерывного развития навыков специалистов по ИБ

Виртуальная ИТ-инфраструктура компаний, доступная 24/7, где специалисты по ИБ в комфортном режиме комплексно прокачивают навыки выявления и расследования атак при поддержке опытных менторов.

Уникальность

1 Реальная подготовка

До 15 сценариев крупнейших APT-атак и практика с живым хакерским трафиком

2 Все как в повседневной жизни

Связанная инфраструктура из 1500+ виртуальных машин и 500+ единиц ПО, максимально похожего на то, с которым вы работаете каждый день

3 Индивидуальный подход

Персональные рекомендации, работа с ментором, доступ к обширной библиотеке теоретических материалов и практических задач

4 Практика 24/7

Изучайте материалы и расследуйте атаки в удобное время

5 Отслеживание динамики

Личная статистика для каждого пользователя и сводные метрики по команде для руководителя

6 Простой доступ

Не требует внедрения и установки, для старта достаточно зарегистрироваться на платформе Standoff 365

#знаемкакпроверитьипрокачатьнавыки

Узнать больше

Решаемые задачи

Отработка стратегии выявления и расследования киберугроз для защиты компании в реальной жизни

Выстраивание взаимодействия внутри команды ИБ, а также проверка готовности к отражению кибератак

Регулярная проверка навыков специалистов по ИБ и повышение их квалификации 24/7

Что входит в состав продукта:

- Подготовленная инфраструктура с полным описанием и набор встроенных СЗИ
- Регулируемые атаки разного уровня сложности с имитацией действий крупнейших APT-группировок
- Воркшопы по разбору атак с ментором-экспертом
- База знаний с теоретическими и практическими материалами
- Практические задания, основанные на реальных атаках с кибербитвы Standoff
- Индивидуальное и командное менторство
- Мини-кибербитва для отработки взаимодействия специалистов вашей команды

Standoff Cyberbones

Онлайн-симулятор для самостоятельной практики специалистов по ИБ

Узнать больше

Мы собрали логи атак реальных белых хакеров с кибербитвы Standoff и загрузили их в средства защиты информации, чтобы специалисты по ИБ могли прокачивать навыки расследования и практиковаться в использовании решений различных классов в режиме 24/7.

Уникальность

1 Реальные кейсы

Изучайте, как могут действовать злоумышленники, исследуя шаги лучших белых хакеров на кибербитве Standoff

2 Удобный формат

Расследуйте кибератаки в комфортном темпе и в удобное время 24/7

3 Простой доступ

Для перехода к заданиям достаточно регистрации на платформе Standoff 365 и настройки VPN

#знаемкакпроверитьипрокачатьнавыки

Решаемые задачи

- Инструмент, обеспечивающий эффективную подготовку специалистов по ИБ
- Отработка навыков расследования кибератак, реализованных белыми хакерами
- Практический опыт работы с различными классами СЗИ, которые используют крупнейшие компании
- Быстрый способ оценки навыков начинающих специалистов по ИБ

Что входит в состав продукта:

- Более 70 заданий на основе атомарных инцидентов
- 5 цепочек атак, реализованных белыми хакерами

Расследуйте инциденты, используя актуальные версии продуктов:

- MaxPatrol SIEM
- PT Network Attack Discovery
- PT Industrial Security Incident Manager
- PT Application Firewall
- PT Sandbox

Standoff Bug Bounty

Крупнейшая российская платформа для поиска уязвимостей в системах компании

Организации могут проверить надежность своих ресурсов, используя знания и опыт комьюнити независимых исследователей безопасности.

Уникальность

1 Экспертиза лучших

Более 20 000 российских и иностранных белых хакеров с различными специализациями помогут найти уязвимости, о которых вы не подозревали

2 Непрерывный поиск уязвимостей

Исследователи изучают сервисы, находят проблемные места и сообщают о них команде платформы, которая дает рекомендации по устранению уязвимостей

3 Поддержка со стороны опытных экспертов

Обеспечивается на каждом этапе — от подготовки к выходу на Standoff Bug Bounty до выплаты вознаграждений белым хакерам

4 Объединение багхантеров

Возможность привлекать целые команды независимых исследователей, а не только отдельных белых хакеров, чтобы увеличить импакт и глубину проработки при тех же затратах

#знаемкакпроверитькиберустойчивость

Узнать больше

Решаемые задачи

Поиск уязвимостей 24/7/365: непрерывная проверка безопасности любого цифрового актива компании — от компонентов ПО и отдельных сервисов до ИТ-инфраструктуры в целом

Обучение команды ИБ работе с потоком данных об уязвимостях за счет доступа к экспертизе лучших независимых исследователей безопасности

Постоянный анализ защищенности ИТ-систем компании — инструмент, необходимый для построения процесса безопасной разработки

Поиск слабых мест в системе обеспечения ИБ, которые могли не заметить собственные специалисты или внешние пентестеры

Поможет:

- Найти уязвимости в приложениях и инфраструктуре компании с привлечением большого числа независимых исследователей
- Повысить уровень безопасности за счет своевременного устранения выявленных уязвимостей
- Узнавать об уязвимостях и проверять их устранение сразу, не дожидаясь проведения регулярного пентеста
- Быстро проверять новые сервисы компании, одновременно работая над их развитием и безопасностью
- Подчеркнуть статус технологически зрелой и ответственной компании

Решение внесено в реестр отечественного ПО

POSITIVE EDUCATION POSITIVE EDU
EDUCATION POSITIVE EDUCATION P
IVE EDUCATION POSITIVE EDUCATIO
SITIVE EDUCATION POSITIVE EDUCA
VE EDUCATION POSITIVE EDUCATION
TIVE EDUCATION POSITIVE EDUCATI
OSITIVE EDUCATION POSITIVE EDUCA
IVE EDUCATION POSITIVE EDUCATIO
SITIVE EDUCATION POSITIVE EDUCAT
VE EDUCATION POSITIVE EDUCATIO
OSITIVE EDUCATION POSITIVE EDUCA
EDUCATION POSITIVE EDUCATION P
POSITIVE EDUCATION POSITIVE EDU

Positive Education

Центр обучения Positive Technologies

Узнать больше

Наш опыт в цифрах

13 000+
обученных специалистов

50+
крупных компаний готовы нас рекомендовать

1500+
преподавателей развивают обучение вместе с нами

Мы создаем корпоративные программы, усиливаем команды, развиваем культуру кибербезопасности и готовим специалистов, которые способны действовать эффективно в условиях реальных киберугроз.

Направления

1 **Корпоративные программы для бизнеса**
Учим снижать риски и обеспечивать киберустойчивость с учетом отраслевой специфики, развивая команды из разных подразделений компании

2 **Образовательные программы для профессионалов**
Создаем практические программы по защите инфраструктуры и веб-приложений, построению SOC, аудиту, анализу инцидентов и реагированию на атаки

3 **Практические тренажеры и продукты для автономного обучения**
Создаем симуляционные среды, которые позволяют специалистам по ИБ отрабатывать действия в условиях, приближенных к реальности, и учиться в удобном темпе

4 **Программы для управленцев**
Формируем у топ-менеджеров стратегическое понимание необходимости бороться с цифровыми угрозами, обучаем принципам киберустойчивости и работе с недопустимыми событиями, помогаем встроить информационную безопасность в систему управления бизнесом

5 **Курсы по эксплуатации продуктов Positive Technologies**
Помогаем клиентам и партнерам использовать наши решения эффективно

Уникальность

Внедрение обучения в рабочие процессы
Используем гибкие форматы (очно, онлайн, с отрывом и без отрыва от работы), внедряем профессиональное развитие в повседневную практику

Фокус на практике и реальные задачи
Все программы создаются с участием специалистов, ежедневно работающих с инцидентами ИБ, кибератаками и защитой инфраструктуры

Сильная методология и структура
Курсы и программы построены на проверенных подходах, учитывают уровень подготовки специалистов и цели компании

Развитие культуры кибербезопасности
Формируем понимание важности обеспечения кибербезопасности у руководителей и специалистов всех подразделений

Инициативы

Школа преподавателей
Учим преподавателей вузов, колледжей и школ передовым практикам ИБ и повышаем качество образовательной системы страны

Учебные программы для вузов
Разрабатываем учебные программы совместно с преподавателями ведущих университетов

Международные программы обучения
Ежегодно проводим интенсивы для молодых специалистов в области ИБ из стран БРИКС

Сотрудничество с бизнес-школами
Обучаем топ-менеджеров принимать стратегические решения и формировать запрос на безопасность в компаниях вместе с ведущими бизнес-школами

Positive Education вправе оказывать образовательные услуги совместно с образовательными партнерами

ДЛЯ ЗАМЕТОК

ОСТАВЬТЕ ЗАЯВКУ
НА КОНСУЛЬТАЦИЮ

ПОДЕЛИТЕСЬ СВОИМ
МНЕНИЕМ О КАТАЛОГЕ