Positive Technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400».

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 170 тысяч акционеров.

Новый класс решений — метапродукты — ориентирован на результативный подход к кибербезопасности. Первый из них — MaxPatrol O2 — позволяет автоматически выявлять и предотвращать атаки до того, как будет нанесен неприемлемый для компании ущерб. MaxPatrol O2 заменяет целую команду центра мониторинга кибербезопасности, а чтобы им управлять, достаточно одного человека. Такая система защиты требует от специалистов минимума знаний и усилий.

Чтобы продемонстрировать эффективность результативного подхода к ИБ, компания проводит киберучения, в том числе на собственной инфраструктуре, и публично тестирует свои продукты. Решения Positive Technologies построены на двадцатилетнем исследовательском опыте и экспертизе нескольких сотен специалистов по кибербезопасности.

Сегодня у компании семь офисов на территории России (в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Новосибирске, Академгородке (Новосибирск) и Томске) и один в Казахстане. Команда насчитывает более 1800 сотрудников, в их числе эксперты мирового уровня в вопросах защиты SCADA- и ERP-систем, банков и телекомов, мобильных и веб-приложений.

Специалисты Positive Technologies участвуют в работе технических комитетов Росстандарта и рабочих групп ФСТЭК, Центробанка, АДЭ, СИГРЭ и других организаций, оказывают экспертную помощь в формировании требований безопасности.

Компанию высоко оценивают международные аналитические агентства: Positive Technologies трижды становилась визионером в исследовании Gartner Magic Quadrant, посвященном системам защиты веб-приложений (WAF), а в 2021 году вошла в тройку мировых вендоров с наибольшим годовым приростом продаж SIEM-систем (по данным IDC).

Компания обеспечивала кибербезопасность таких важных мероприятий, как:

2013 г. — Всемирная летняя универсиада в Казани;

2014 г. — Олимпиада в Сочи;

2018 г. — чемпионат мира по футболу;

2018 г. — выборы Президента России;

2019 г. — Всемирная зимняя универсиада в Красноярске;

2020 г. — голосование по поправкам к Конституции;

2021 г. — выборы в Госдуму.

Positive Technologies известна мировому сообществу как визионер и лидер в области этичного исследования проблем безопасности. Ежегодно специалисты компании выявляют сотни уязвимостей нулевого дня в IT-системах различных классов и типов, в том числе в продуктах Cisco, Citrix, IBM, Intel, Microsoft и VMware. За обнаружение опасных уязвимостей наши эксперты отмеченыв залах славы таких компаний, как Adobe, Apple, AT&T, GitLab, Google, IBM, Mastercard, Microsoft, PayPal, VK и «Яндекс». Сведения обо всех без исключения найденных уязвимостях компания предоставляет производителям ПО в рамках политики ответственного разглашения (responsible disclosure) и не публикует до тех пор, пока вендоры не выпустят соответствующее обновление.

Команда Positive Technologies знает об информационной безопасности многое и с удовольствием делится опытом с другими:

- уже 12 лет проводит собственный научно-практический форум Positive Hack Days — крупнейшее мероприятие в области информационной безопасностив России и СНГ. Компания привлекает к диалогу небезразличных к вопросам кибербезопасности людей со всего мира, в том числе экспертов в области ИТи ИБ, руководителей бизнеса и представителей государственных структур, белых хакеров

и исследователей безопасности, студентов и школьников. В рамках PHDays проходят сотни выступлений и мастер-классов, а также практические конкурсы по анализу защищенности промышленных систем управления, банковских сервисов, мобильной связи и веб-приложений. В 2023 году форум впервые прошел в формате открытого городского фестиваля по кибербезопасности и объединил экспертов в сфере ИБ, людей, развивающих технологии, жителей и гостей города Москвы;

- аккумулирует самые свежие новости индустрии на портале SecurityLab.ru;
- разрабатывает учебные программы для ведущих вузов страны и помогает растить первоклассных специалистов со студенческой скамьи: материалами, подготовленными экспертами компании в рамках образовательной программы Positive Education, пользуются более 65 вузов России;
- проводит крупнейшую в мире кибербитву Standoff, на которой собираются лучшие специалисты России и зарубежья в области нападения и защиты. На полигоне воссоздаются производственные цепочки, бизнес-сценарии и технологический ландшафт, характерные для компаний различных отраслей, а также изучаются возможности реализации недопустимых событий и их предотвращения.

Продукты, решения и сервисы Positive Technologies

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

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

В портфеле Positive Technologies — более десятка высокотехнологичных продуктов. Они позволяют:

- останавливать хакера в автоматическом режиме силами одного человека;
- контролировать защищенность инфраструктуры и своевременно находить в ней уязвимости;
- выявлять инциденты ИБ в инфраструктуре любых масштабов, включая закрытые промышленные системы;
- детектировать атаки во внутреннем и внешнем трафике компаний;
- защищать веб-приложения от сложных атак;
- обнаруживать уязвимости и ошибки в приложениях, а также поддерживать процесс безопасной разработки;
- обнаруживать и отражать целевые и массовые атаки с применением современного вредоносного ПО;
- реагировать на киберугрозы как на конечных точках, так и в инфраструктуре в целом, объединяя для верификации атаки события и контекст из множества систем ИБ.

На базе продуктовой линейки Positive Technologies сформировано несколько решений, которые аккумулируют опыт по защите бизнеса в различных сферах и специфику российских и международных стандартов безопасности.
В частности, компания предлагает решения:

- для построения распределенных систем кибербезопасности;
- построения SOC, в том числе в небольших инфраструктурах;
- раннего выявления сложных угроз;
- защиты веб-приложений;
- обеспечения безопасности объектов КИИ (включая взаимодействие с главным центром ГосСОПКА);
- построения центра ГосСОПКА.

Кроме того, компания предоставляет сервисное обслуживание и консультационные услуги в области кибербезопасности: непрерывный анализ защищенности бизнеса, обнаружение сложных инцидентов, реагирование на них и расследование, мониторинг защищенности корпоративных систем.

Метапродукты

MaxPatrol O2 — метапродукт, который позволяет обнаруживать и останавливать атаки злоумышленников в автоматическом режиме с измеримым эффектом силами одного человека. Решает проблему серьезного дефицита квалифицированных кадров в индустрии и помогает защитить организации по всему миру.

Продуктовый портфель

MaxPatrol VM — система, позволяющая выстроить процесс управления уязвимостями и контролировать защищенность IT-инфраструктуры компании. Продукт собирает, обновляет и хранит полную информацию об активах, на основе этих данных определяет новые уязвимости на узлах и предоставляет пользователю информацию о них, включая знания о трендовых и наиболее опасных уязвимостях (то есть тех, которые необходимо закрыть в первую очередь).

MaxPatrol SIEM — система мониторинга событий информационной безопасности. Постоянно пополняется знаниями экспертов о способах детектирования актуальных угроз и адаптируется к изменениям в защищаемой сети. В 2020 году количество продаж MaxPatrol SIEM выросло на 85%. За счет этого компания вошла в тройку мировых вендоров с наибольшим годовым приростом продаж SIEM-решений. Согласно исследованию IDC Global, Positive Technologies — единственный российский вендор в топ-20 мирового рынка SIEM-систем (2021).

PT Network Attack Discovery — система глубокого анализа сетевого трафика (network traffic analysis, NTA) для выявления атак на периметре и внутри сети. Обеспечивает видимость происходящего в сети, обнаруживает активность злоумышленников, в том числе в зашифрованном трафике, и помогает в расследованиях.

PT Sandbox — песочница, позволяющая защитить инфраструктуру компании от целевых и массовых атак с применением вредоносного ПО и эксплуатацией уязвимостей нулевого дня. Проверяет в изолированной виртуальной среде поступающие в компанию файлы и ссылки, выдает вердикт об их вредоносности или легитимности, блокирует угрозы.

PT XDR — решение для выявления сложных киберугроз и реагирования на них. Собирает и анализирует разрозненные данные из множества систем, позволяет обнаруживать действия хакера в любой инфраструктуре и автоматически реагировать на атаки. Основано на экосистеме продуктов Positive Technologies и использует уникальные экспертные знания об угрозах для выявления атак.

PT ISIM — система анализа трафика сетей АСУ ТП. Позволяет находить следы нарушений информационной безопасности в технологических сетях, помогает на ранней стадии выявлять кибератаки, активность вредоносного ПО, неавторизованные действия персонала (в том числе злоумышленные) и обеспечивает соответствие требованиям законодательства.

PT Application Firewall — межсетевой экран уровня веб-приложений. Предназначен для защиты веб-ресурсов организаций от кибератак (DDoS-атак (L7) и атак нулевого дня), а также от угроз из списков OWASP Top 10 и WASC. Визионер магического квадранта Gartner.

PT Application Inspector — инструмент для выявления уязвимостей в приложениях. Принцип работы продукта основан на сочетании статического (SAST), динамического (DAST), интерактивного (IAST) методов и анализа сторонних компонентов (SCA). Позволяет специалистам по ИБ выявлять и подтверждать уязвимости в исходном коде, а разработчикам — ускорить исправление кода на ранних стадиях разработки.

PT MultiScanner — система защиты от вирусных угроз. Выявляет вредоносные программы, блокирует их распространение в инфраструктуре и обнаруживает скрытое присутствие зловредов.

MaxPatrol 8 — система, используемая для оценки защищенности IT-инфраструктуры. Позволяет определить эффективность процессов ИБ, а также обеспечивает выполнение требований стандартов.

XSpider — сканер уязвимостей, позволяющий оценить уровень защищенности сети компании. Проверяет рабочие станции, серверы, сетевые устройства и веб-приложения. Исследует узлы без применения заранее установленных агентов.

«ПТ Ведомственный центр» — система управления инцидентами. Автоматизирует процесс реагирования на инциденты и информирует о них Национальный координационный центр по компьютерным инцидентам (НКЦКИ) и другие отраслевые CERT.

PT Platform 187 — (комплексное решение, объединяющее ряд продуктов PT) — программно-аппаратный комплекс для реализации основных функций безопасности значимых объектов КИИ и взаимодействия с главным центром ГосСОПКА. Включает в себя набор технических средств, который помогает выполнить основные требования законодательства, автоматизирует процессы ИБ в организации и значительно повышает их эффективность.

PT BlackBox — сканер безопасности приложений, работающий методом черного ящика. Дает рекомендации по устранению проблем. Упрощает работу специалистов R&D.

Сервисный портфель

Услуги по обнаружению сложных инцидентов, реагированию на них и расследованию, а также по мониторингу защищенности корпоративных систем предоставляет экспертный центр безопасности Positive Technologies (PT Expert Security Center (PT ESC)). Сервисы безопасности на базе продуктов, которые предлагает PT ESC, доказали свою эффективность во время экспертного сопровождения зимней Олимпиады-2014 в Сочи и чемпионата мира по футболу — 2018: специалисты помогли отразить 38 тысяч кибератак на сервисы транспортной дирекции.

Непрерывный анализ защищенности бизнеса — услуги Positive Technologies по анализу защищенности бизнеса от киберугроз. Помогают непрерывно оценивать уязвимость компании для действий злоумышленников, своевременно предотвращать атаки и устранять их последствия. Спектр услуг включает три направления: Pentest 360, эмуляцию APT и red team vs. blue team.

Исследование угроз и уязвимостей аппаратных решений — услуги экспертной команды Positive Technologies, которые помогут устранить риски ИБ, связанные с уязвимостями аппаратных платформ.