positive technologies

Positive Technologies — один из лидеров в области 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.

Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.

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.

Для демонстрации эффективности результативного подхода к ИБ компания проводит киберучения, в том числе на собственной инфраструктуре, и публично тестирует свои продукты. Решения Positive Technologies построены на экспертизе и исследовательском опыте, накопленном более чем за 20 лет несколькими сотнями специалистов по кибербезопасности. Сегодня у компании шесть офисов на территории России (в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Новосибирске и Томске). В команде работают эксперты мирового уровня в вопросах защиты SCADA- и ERP-систем, банков и телекомов, мобильных и веб-приложений.

Специалисты Positive Technologies участвуют в деятельности технических комитетов Росстандарта и рабочих групп Федеральной службы по техническому и экспортному контролю (ФСТЭК), Центрального банка Российской Федерации, Ассоциации документальной электросвязи, Международного совета по большим электрическим системам высокого напряжения (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 2018 году стала единственной новой компанией, включенной в магический квадрант Gartner по тестированию безопасности приложений. В 2021 году компания вошла в тройку мировых вендоров с наибольшим годовым приростом продаж SIEM-систем (по данным IDC).

Компания обеспечивала кибербезопасность таких важных мероприятий, как:

2013 — Всемирная летняя универсиада в Казани;

2014 — Олимпиада в Сочи;

2018 — чемпионат мира по футболу;

2018 — выборы Президента России;
2019 — Всемирная зимняя универсиада в Красноярске;
2020 — голосование по поправкам к Конституции;
2021 — выборы в Госдуму;
2024 — международный мультиспортивный фиджитал-турнир «Игры будущего».

Positive Technologies известна мировому сообществу как визионер и лидер в области этичного исследования проблем безопасности. Ежегодно специалисты компании выявляют сотни уязвимостей нулевого дня в ИТ-системах различных классов и типов, в том числе в продуктах Cisco, Citrix, IBM, Intel, Microsoft и VMware. За обнаружение опасных уязвимостей наши эксперты отмечены в 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 делится опытом с другими:

- Уже 13 лет проводит Positive Hack Days — крупнейшее мероприятие в области информационной безопасности в России и странах СНГ. Компания привлекает к диалогу небезразличных к вопросам кибербезопасности людей со всего мира, в том числе экспертов в области ИТ и 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 мероприятие впервые прошло в формате открытого городского фестиваля по кибербезопасности и объединило 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 60 вузов в России и странах СНГ.
- 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 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 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 помогает решить такие задачи, как:

- построение распределенных систем кибербезопасности;
- построение SOC, в том числе в небольших инфраструктурах;
- раннее выявление сложных угроз;
- защита веб-приложений;
- обеспечение безопасности объектов КИИ (включая взаимодействие с главным центром ГосСОПКА);
- построение 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 — обнаруживает злоумышленника, определяет захваченные им ресурсы, прогнозирует сценарий развития атаки с учетом недопустимых событий и останавливает атаку до того, как компании будет нанесен непоправимый ущерб. Решает проблему дефицита кадров в индустрии ИБ.

MaxPatrol Carbon — помогает подготовить ИТ-инфраструктуру к отражению атак и обеспечивает непрерывный контроль киберустойчивости в реальном времени, делая невозможным причинение ущерба компании. Позволяет действовать превентивно: анализирует, как в конкретной инфраструктуре могут быть совершены кибератаки, и формирует практические рекомендации для усиления ее защиты.

Продуктовый портфель

MaxPatrol VM — система, позволяющая выстроить процесс управления уязвимостями и контролировать защищенность ИТ-инфраструктуры компании. Продукт собирает, актуализирует и хранит полную информацию об активах. С ее помощью он обнаруживает бреши в защите узлов и предоставляет пользователю данные о них, включая знания о трендовых и наиболее опасных уязвимостях (то есть о тех, которые необходимо устранить 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 чего компания вошла в тройку мировых вендоров с наибольшим годовым приростом продаж SIEM-решений. Объем отгрузок MaxPatrol SIEM продолжает увеличиваться: в 2023 году прирост составил 74%. Согласно исследованию IDC Global, Positive Technologies — единственный российский вендор в топ-20 мирового рынка SIEM-систем (2021).

PT NGFW — межсетевой экран нового поколения, призванный защитить компании от кибератак. Встроенные в продукт модули безопасности — IPS-система, потоковый антивирус, фильтрация URL и обогащение данными об угрозах — позволяют закрыть потребности в защите от актуальных угроз без потерь в производительности.

MaxPatrol EDR — система для выявления сложных киберугроз, целевых атак на конечных устройствах и для реагирования на них. Благодаря статическому и поведенческому анализу, экспертным правилам PT Expert Security Center и гибкой настройке правил обнаружения продукт определяет угрозы, а также тактики и техники злоумышленников.

PT Knockin — онлайн-сервис для проверки защищенности электронной почты. Он симулирует атаки, проверяя эффективность почтовых средств защиты (почтового шлюза, антивирусов, песочниц и других), и выдает вердикт с рекомендациями.

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 ISIM — система мониторинга безопасности промышленных ИТ-инфраструктур. Позволяет находить следы нарушений ИБ 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, а также от угроз из списков OWASP Top 10 и WASC.

PT Cloud Application Firewall — облачный межсетевой экран для веб-приложений, который защитит от кибератак, утечек данных и не позволит злоумышленникам получить доступ к учетным записям пользователей и нарушить работу вашего бизнеса. Доступен по подписке.

PT Container Security — решение для комплексной защиты инфраструктуры гибридного облака. Обеспечивает безопасность разработки программных систем, использующих механизмы контейнерной виртуализации.

PT Application Inspector — инструмент для выявления уязвимостей и тестирования безопасности приложений. Позволяет специалистам по ИТ и ИБ находить слабые места в коде ПО и уязвимости внешних библиотек, а также подтверждать недокументированные возможности.

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 ИТ-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 Positive Technologies; 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.

PT Threat Intelligence Feeds — потоки данных об индикаторах компрометации (вредоносных доменах, IP-адресах, ссылках и хеш-суммах файлов). Они позволяют SOC-командам быть в курсе актуальных угроз ИБ.

PT Threat Analyzer — это программная платформа для накопления знаний о существующих и потенциальных угрозах информационной безопасности, а также о способах их обнаружения.

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 в Сочи (2014) и чемпионата мира по футболу (2018): специалисты помогли отразить 38 тысяч кибератак на сервисы транспортной дирекции.

Услуги Positive Technologies по непрерывному анализу защищенности бизнеса помогают 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 недостатками аппаратных платформ.