Positive Technologies

Positive Technologies уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявлять, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня у компании семь офисов на территории России (в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Новосибирске, Академгородке и Томске) и офис в Казахстане (Нур-Султан). В нашей команде более тысячи сотрудников, в том числе более 250 экспертов мирового уровня по защите ERP, SCADA, банков и телекомов, веб- и мобильных приложений.

Репутация экспертов мирового уровня по вопросам защиты самых разнообразных устройств и инфраструктур подтверждена обширным списком наших партнеров и клиентов:

- в числе наших клиентов в России — 80% участников рейтинга «Эксперт-400», крупнейших компаний страны, с нами сотрудничает более 2000 компаний в 30 странах;
- нам доверяют Cisco, Google, Honeywell, Huawei, Microsoft, Oracle, SAP, Schneider Electric Siemens и другие крупные мировые вендоры;
- нас высоко оценивают международные аналитические агентства. Так, компания трижды становилась «визионером» в исследовании Gartner Magic Quadrant по системам защиты веб-приложений (WAF).

Мы знаем об информационной безопасности почти все и с удовольствием делимся этим с другими:

- уже десять лет проводим собственный научно-практический форум Positive Hack Days - крупнейшее мероприятие в области информационной безопасности в России и СНГ, в работе которого ежегодно участвуют тысячи посетителей – экспертов в ИТ и ИБ, представителей бизнеса и государственных структур, студентов и школьников. В рамках конференции проходят сотни докладов и мастер-классов по самым острым темам ИБ, а также практические конкурсы по анализу защищенности промышленных систем управления, банковских сервисов, мобильной связи и веб-приложений;
- аккумулируем самые свежие новости индустрии на нашем портале SecurityLab.ru;
- разрабатываем образовательные программы для ведущих вузов страны и помогаем растить первоклассных специалистов со студенческой скамьи: учебные материалы, подготовленные экспертами компании в рамках образовательной программы Positive Education, используют в своих курсах уже более 50 российских вузов.

Продукты, решения и сервисы Positive Technologies

Все решения Positive Technologies проектируются с учетом большого опыта защиты бизнеса в различных отраслях. Специалисты компании участвуют в работе технических комитетов Росстандарта и рабочих групп ФСТЭК, Центробанка, АДЭ, СИГРЭ, GSMA и других организаций, оказывая экспертную помощь в формировании требований безопасности. Наши продукты максимально соответствуют российским и международным стандартам безопасности, включая стандарты PCI DSS и ЦБ РС БР ИББС-2.6-2014, приказы ФСТЭК № 17 и 21.

В продуктовом портфеле компании сегодня 10 высокотехнологичных продуктов, позволяющих:

- 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.

На базе продуктовой линейки сформировано несколько решений, учитывающих опыт Positive Technologies по защите бизнеса в различных сферах и специфику российских и международных стандартов безопасности. В частности, клиенты компании имеют возможность использовать 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;
- организации безопасной удаленной работы и контроля удаленного доступа.

Также компания оказывает ряд сервисов и консультационных услуг в области кибербезопасности (в частности, непрерывный анализ защищенности бизнеса, обнаружение, реагирование и расследование сложных инцидентов, мониторинг защищенности корпоративных систем).

Продуктовый портфель

MaxPatrol 8 — предназначен для объективной оценки уровня защищенности IT-инфраструктуры компании. Система позволяет своевременно обнаружить уязвимости информационной системы, провести комплексный анализ сетевого оборудования, операционных систем, СУБД, прикладных и ERP-систем, веб-приложений, а также контролировать соответствие основным стандартам информационной безопасности (ISO 27001, PCI DSS, CIS). MaxPatrol 8 гибко масштабируется и подходит как для небольших компаний, так и для крупных территориально-распределенных предприятий.

MaxPatrol SIEM — система выявления инцидентов с уникальным подходом к обеспечению прозрачности IT-инфраструктуры и глубокой экспертизой в обнаружении угроз. Он постоянно пополняется знаниями экспертов о способах детектирования угроз и адаптируется к изменениям в защищаемой сети.

PT Industrial Security Incident Manager — программно-аппаратный комплекс глубокого анализа технологического трафика. Обеспечивает поиск следов нарушений информационной безопасности в сетях АСУ ТП, помогает на ранней стадии выявлять кибератаки, активность вредоносного ПО, неавторизованные действия персонала (в том числе злоумышленные) и обеспечивает соответствие требованиям законодательства (187-ФЗ, приказы ФСТЭК № 31, 239, ГосСОПКА) к изменениям в защищаемой сети.

PT Application Firewall — межсетевой экран уровня веб-приложений, предназначенный для защиты веб-ресурсов организации от известных и неизвестных атак.

PT Application Inspector — решение для выявления уязвимостей в исходном коде или готовом приложении, путем комбинации статических (SAST), динамических (DAST) и инфраструктурных (IAST) методов анализа.

PT MultiScanner — система защиты от вредоносных программ. Выявляет угрозы, блокирует их распространение и обнаруживает скрытое присутствие зловредов, используя набор антивирусов и репутационные списки Positive Technologies.

XSpider — профессиональный сканер безопасности, предназначенный для проверки сети на наличие уязвимостей. Регулярное сканирование позволяет защитить информационную систему компании до того, как злоумышленник обнаружит ее слабые места и проведет атаку. По итогам сканирования XSpider предоставляет подробный отчет о выявленных недостатках в защите, а также рекомендации по их устранению.

PT Network Attack Discovery — система глубокого анализа сетевого трафика (NTA/NDR) для выявления атак на периметре и внутри сети. PT NAD знает, что происходит в сети, обнаруживает активность злоумышленников даже в зашифрованном трафике и помогает в расследованиях.

PT Sandbox — передовая песочница, которая позволяет защитить компанию от целевых и массовых атак с применением современного вредоносного ПО. Она поддерживает гибкую удобную кастомизацию виртуальных сред для анализа и обнаруживает угрозы не только в файлах, но и в трафике.

ПТ Ведомственный центр — система управления инцидентами. Она автоматизирует процесс реагирования на инциденты и информирует о них Национальный координационный центр по компьютерным инцидентам (НКЦКИ).

Портфель решений

Построение центра ГосСОПКА — комплексное решение для создания центра ГосСОПКА и взаимодействия с НКЦКИ, созданное на основе продуктов Positive Technologies, с помощью которых служба ИБ сможет самостоятельно реализовать функции центра ГосСОПКА, а также услуги экспертного центра безопасности Positive Technologies (PT ESC).

PT Anti-APT — комплексное решение для выявления и предотвращения целевых атак. Позволяет максимально быстро обнаружить присутствие злоумышленника в сети и воссоздать полную картину атаки для детального расследования.

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. Платформа включает в себя набор технических средств, который помогает выполнить основные требования законодательства, автоматизирует процессы ИБ в организации и значительно повышает их эффективность.

Безопасная удаленная работа — комплексное решение, позволяющее обеспечить мониторинг работы сотрудников на удаленке и объединяющее систему глубокого анализа сетевого трафика PT Network Attack Discovery и систему выявления инцидентов MaxPatrol SIEM.

Контроль удаленного доступа в сетях АСУ ТП — решение, позволяющее обеспечить мониторинг работы удаленных сотрудников и подрядчиков, основанное на комплексном использовании средств инструментального мониторинга действий пользователей, подключенных к сети АСУ ТП.

Безопасность объектов КИИ — система безопасности значимых объектов КИИ в соответствии с требованиями закона № 187-ФЗ, объединяет в себе продукты Positive Technologies, которые позволяют выполнить основные законодательные требования по защите значимых объектов КИИ, предотвращать и выявлять атаки и автоматизировать взаимодействие с ГосСОПКА.

PT Unified Application Security — уникальное интегрированное решение, отвечающее на все современные вызовы к безопасности приложений, помогает сокращать расходы и выпускать обновленные приложения в срок или быстрее.

Сервисный портфель

PT Expert Security Center (PT ESC) — экспертный центр безопасности Positive Technologies предоставляет услуги по обнаружению, реагированию и расследованию сложных инцидентов, а также по мониторингу защищенности корпоративных систем. Сервисы безопасности на базе продуктов Positive Technologies, которые предлагает PT ESC, доказали свою эффективность во время экспертного сопровождения зимней Олимпиады-2014 в Сочи и во время Чемпионата Мира по футболу-2018, в ходе которого компания помогла отразить 38 тыс. кибератак на сервисы транспортной дирекции ЧМ-2018.

Непрерывный анализ защищенности бизнеса — услуги Positive Technologies по анализу защищенности бизнеса от киберугроз помогают непрерывно оценивать уязвимость компании перед действиями злоумышленников, своевременно предотвращать атаки и устранять 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 помогут устранить риски информационной безопасности, связанные с уязвимостями аппаратных платформ.

POSITIVE TECHNOLOGIES