Кратко о продуктах Positive Technologies

Подробно
о продуктах:
ptsecurity.com

POSITIVE TECHNOLOGIES

MaxPatrol SIEM

Выявление инцидентов ИБ и расследование атак.

Кому предлагать:

Всем отраслям. В приоритете — банки, госсектор, промышленность.

Как понять потребность:

1. Заказчик хочет построить SOC.
2. Нужно защищать КИИ, ИСПДн, ГИС.
3. Заказчик хочет строить центр ГосСОПКА.
4. Нужно выполнять требования ГОСТ Р 57580.1-2017 о безопасности банковских операций.
5. Есть другой SIEM: Splunk или ArcSight.
6. Есть много разных средств защиты и нет единой точки контроля безопасности.
7. Заказчик пытается выявлять инциденты, но не знает как.

Ключевые преимущества:

- Лидирующее отечественное SIEM-решение.
- Детально знает IT-инфраструктуру.
- База знаний для обнаружения угроз регулярно дополняется новыми пакетами экспертизы.
- Быстро развивается и постоянно упрощается, чтобы работать с ним мог даже новичок.
- Умеет собирать данные с популярных систем российских вендоров.
- Выполняет требования законодательства по защите информации.

Ключевые слова:

SIEM, выявление инцидентов, SOC, корреляция событий ИБ, мониторинг событий ИБ, asset management

PT Network Attack Discovery

Система глубокого анализа трафика (NTA) для выявления атак на периметре и внутри сети.

Кому предлагать:

Всем отраслям. В приоритете – госсектор, промышленность, энергетика, банки.

Как понять потребность:

1. Есть SOC, необходимо повысить видимость сети и научиться расследовать атаки на сетевом уровне.
2. Заказчик понимает, что защита периметра — не панацея и нужно следить за тем, что происходит внутри сети.
3. Есть бюджет на защиту от целевых атак и сложных угроз.
4. У заказчика есть SIEM- и/или EDR-системы.
5. Заказчик думает, что у него инцидент и нужно провести расследование.
6. Хочется IDS (хотя PT NAD относится к другому классу решений, часто заказчики покупают его за счет бюджета, заложенного на IDS).
7. Заказчик хочет купить Group-IB Threat Hunting Framework (модуль Sensor) или «Гарда Монитор».
8. Есть объект КИИ, который необходимо защищать по 187-ФЗ.
9. Заказчик хочет проводить threat hunting.

Ключевые преимущества:

- Видит активность злоумышленников как на периметре, так и внутри сети.
- Выявляет атаки и их последствия даже в шифрованном трафике.
- Полезен в расследованиях и threat hunting.
- Определяет техники и тактики из модели MITRE ATT&CK.
- Помогает выполнить требования по защите информации.

Ключевые слова:

network traffic analysis (NTA), network detection and response (NDR), выявление атак, SOC, расследование атак, безопасность корпоративной сети, IDS, Anti-APT, threat hunting

PT Sandbox

Песочница для защиты от целевых и массовых атак с применением вредоносного ПО.

Кому предлагать:

Всем отраслям. В приоритете – госсектор, промышленность, энергетика, банки, IT.

Как понять потребность:

1. Заказчик хочет именно песочницу и пока выбирает/планирует закупать либо уже использует продукт другого вендора (CheckPoint Sandblast, FortiSandbox, TrendMicro Deep Discovery Analyzer, Kaspersky Sandbox, Group-IB Malware Detonation Platform).
2. Есть SOC, необходимо повысить его эффективность и научиться выявлять и расследовать атаки, связанные с неизвестным вредоносным ПО.
3. Есть бюджет на защиту от целевых атак и сложных угроз.
4. Заказчик думает, что у него инцидент, связанный с вредоносным ПО, и нужно провести расследование.
5. Заказчик хочет проводить threat hunting.

Ключевые преимущества:

- Позволяет максимально точно имитировать реальные компьютеры заказчика (гибкая кастомизация виртуальных сред).
- Обеспечивает комплексную проверку файлов (статический и динамический анализ с помощью уникальных правил PT ESC + антивирусы).
- Выявляет угрозы не только в файлах, но и в сетевом трафике, включая шифрованный.
- Безопасно провоцирует хакеров выдать себя (deception-технологии, приманки).
- Выявляет скрытые угрозы в сети с помощью ретроспективного анализа.

Ключевые слова:

песочница, sandbox, защита от неизвестных угроз, защита от целевых атак, Anti-APT, поведенческий анализ файлов, SOC, threat hunting

Решение PT Anti-APT

Комплекс для раннего выявления и предотвращения целевых атак. Состоит из PT NAD, PT Sandbox и сервисов PT ESC.

Кому предлагать:

Всем отраслям. В приоритете – госсектор, промышленность, оборонка, банки.

Как понять потребность:

1. Есть бюджет под выявление целевых атак.
2. У заказчика уже проводили расследование инцидента.
3. Заказчик хочет купить или уже использует KATA, TDS, TrendMicro Deep Discovery или другое anti-APT решение.
4. Заказчик строит свой SOC.
5. У заказчика уже есть MaxPatrol SIEM.

Ключевые преимущества:

- Выявляет целевые атаки как на периметре, так и внутри сети, сокращает время скрытого присутствия угрозы в сети.
- Обнаруживает с помощью ретроспективного анализа атаки, которые не были выявлены ранее.
- Дает всю необходимую информацию для быстрого и эффективного расследования инцидентов ИБ.
- Для выявления угроз использует наиболее релевантные для РФ и СНГ знания.

Ключевые слова:

целевая атака, таргетированная атака, APT, Anti-APT, защита от сложных угроз, хакерские группировки

PT Application Firewall

Межсетевой экран уровня веб-приложений (Web Application Firewall, WAF).

Кому предлагать:

Банки, госсектор, онлайн-ритейл, медицина, страховые, медиа.

Как понять потребность:

1. Есть важные для бизнеса сайты: онлайн-платежи, онлайн-магазины, порталы.
2. Есть сайты, где публикуется чувствительная информация: новости, медиа.
3. Есть веб-приложения (неважно, публичные или нет).
4. ЦОД, предоставляющий услуги по безопасности своим клиентам.
5. Был инцидент, связанный с веб-приложениями: утечка данных, финансовые убытки и т. д.
6. Есть WAF от Imperva, F5, Код Безопасности или любой другой on-premise WAF.

Ключевые преимущества:

- Блокирует массовые и целевые атаки.
- Выявляет атаки, распределенные во времени.
- Быстро встраивается в инфраструктуру.
- Сертифицированное решение (реестр российского ПО, сертификат ФСТЭК, соответствия республики Казахстан).
- Дополнительные модули:
  - M-Scan (мультивендорная антивирусная проверка загружаемого на приложения контента);
  - P-Code (поиск уязвимостей в защищаемых приложениях и формирование виртуальных патчей).

Ключевые слова:

межсетевой экран уровня приложений, web application firewall, WAF, OWASP Top 10, DDoS уровня приложений, защита API, защита от ботов, виртуальный патчинг

Кратко о продуктах Positive Technologies

Подробно
о продуктах:
ptsecurity.com

POSITIVE TECHNOLOGIES

PT Application Inspector

Поиск уязвимостей в приложениях (Application Security Testing, AST).

Кому предлагать:

Банки, госсектор, онлайн-ритейл, медицина, медиа, разработчики.

Как понять потребность:

1. Есть свои веб-приложения.
2. Разрабатывают веб-приложения для других.
3. Нужно принимать разработанные подрядчиками приложения (приемка кода).
4. Хотят выстроить процесс безопасной разработки (SDL, DevSecOps).

Ключевые преимущества:

- Минимум ложных срабатываний.
- Встраивание в процессы разработки.
- Быстрое закрытие уязвимостей (интеграция с PT Application Firewall).
- Сертифицированное решение (реестр российского ПО, сертификат ФСТЭК, соответствия республики Казахстан).

Ключевые слова:

анализ исходного кода, SAST, DAST, IAST, выявление уязвимостей в веб-приложениях, виртуальный патчинг, приемка кода, безопасная разработка, SSDL, SDLC, SDL, DevSecOps.

XSpider

Сканер уязвимостей.

Кому предлагать:

Небольшим заказчикам с сильно ограниченным бюджетом. Всем отраслям.

Как понять потребность:

1. SMB, регионы, ограниченный бюджет.
2. Нужно бюджетное базовое решение для выявления уязвимостей в сети.
3. Заказчик хочет знать:
   - легко ли проникнуть в его сеть, обладая минимальными знаниями о системах;
   - к каким его ресурсам можно получить доступ через интернет;
   - насколько сложно подобрать пароли к активам компании.

Ключевые преимущества:

- Обширная и пополняемая база знаний уязвимостей.
- Качественная проверка парольной защиты.
- Простая система лицензирования.
- Не требует установки дополнительного ПО или агентов.
- Выполняет требования законодательства по защите информации.

Ключевые слова:

дешевый сканер уязвимостей, сканер безопасности, выявление уязвимостей, сканирование портов, сетевой сканер, проверка парольной защиты, тестирование на проникновение, пентест, Blackbox-сканер

MaxPatrol 8

Контроль защищенности и соответствия стандартам информационной системы – тестирование на проникновение, глубокая проверка систем, оценка соответствия стандартам.

Кому предлагать:

Всем отраслям. Компаниям любого масштаба, включая любой Enterprise.

Как понять потребность:

1. Заказчик хочет выявить уязвимости и ошибки конфигурации в инфраструктуре.
2. Необходимо проверять системы на соответствие требованиям стандартов информационной безопасности (ГОСТ ИСО/МЭК 27001, СТО БР, CIS, ФСТЭК).
3. Необходимо провести внутренний и внешний аудит.
4. Нужно защищать КИИ, ГИС, ИСПДн.
5. Заказчик хочет автоматизировать контроль защищенности в организации.

Ключевые преимущества:

- Является стандартом де-факто анализа защищенности (доля рынка РФ более 80%).
- Обширная и пополняемая база знаний уязвимостей.
- Подходит для сетей любого масштаба, ориентирован на LE.
- Имеет самое большое на рынке количество поддерживаемых систем (более 1000).
- Богатый опыт внедрения в компании разных сфер, более 10 лет на рынке.
- Проверяет системы на соответствие широкому перечню технических и высокоуровневых международных стандартов ИБ, поддерживает более 180 из них.

Ключевые слова:

управление уязвимостями, VM, выявление уязвимостей, контроль соответствия требованиям, комплаенс, контроль обновлений, сканер уязвимостей, анализ защищенности

MaxPatrol VM

Позволяет выстроить полноценный процесс управления уязвимостями, результаты которого видны.

Кому предлагать:

Всем отраслям. Компаниям любого масштаба, включая любой Enterprise. Особенно тем, у кого есть MaxPatrol SIEM.

Как понять потребность:

1. Заказчик хочет управлять уязвимостями и повышать уровень защищенности компании.
2. Заказчику важно понимать, какие уязвимости и на каких активах необходимо закрыть в первую очередь.
3. Важна быстрая реакция на опасные уязвимости.
4. Необходимо выстроить эффективное взаимодействие отделов ИБ и IT.

Ключевые преимущества:

- Позволяет выстроить полноценный процесс управления уязвимостями в компании и отслеживать повышение уровня защищенности.
- Автоматически определяет все активы компании и контролирует их защиту.
- Информирует о приоритетных и критически важных задачах. Отслеживает трендовые уязвимости.
- Находит уязвимости без повторного сканирования, реагировать на них можно гораздо быстрее.

Ключевые слова:

управление уязвимостями, vulnerability management, VM, выявление уязвимостей, анализ защищенности, трендовые уязвимости, определение уязвимостей без сканирования, контроль устранения уязвимостей, контроль защищенности, asset management, управление активами, приоритизация уязвимостей.

PT ISIM

Система глубокого анализа трафика технологических сетей (Industrial NTA/NDR). Выявление разнообразных нарушений ИБ в сетях АСУ ТП (в том числе атак).

Кому предлагать:

Любым предприятиям, имеющим промышленные сети (АСУ ТП).

Как понять потребность:

1. Есть АСУ ТП.
2. Заказчик является КИИ и должен соответствовать законодательству.
3. Уже был чувствительный инцидент.

Ключевые преимущества:

- Самая большая и пополняемая экспертная база для обнаружения атак и нарушений в промышленных сетях: поддержка новых протоколов, устройств, новые алгоритмы выявления аномалий (более 4500 индикаторов на 2021 год).
- Полный разбор и нормализация всего спектра трафика АСУ ТП для целей Threat Hunting. Другие решения на рынке этого не делают.
- Тесная бесшовная интеграция со штатными средствами SOC (SIEM, SOAR и др.). На моновендорной платформе в составе «MP SIEM + PT ISIM + PT Sandbox» можно собрать полноценный промышленный SOC.

Ключевые слова:

выявление нарушений ИБ в АСУ ТП, защита промышленных сетей, инвентаризация АСУ ТП, контроль действий персонала и подрядчиков

Кратко о продуктах Positive Technologies

Подробно
о продуктах:
ptsecurity.com

POSITIVE TECHNOLOGIES

PT MultiScanner

Система защиты от вирусных угроз.

Кому предлагать:

Всем отраслям.

Как понять потребность:

1. Нужна проверка файлов (почта, веб, файловое хранилище и т. д.), но не хватает бюджета на песочницу.
2. Нужна очень быстрая «молотилка» огромного потока файлов (песочница не подходит из-за особенностей динамического анализа).

Ключевые преимущества:

- Эффективно выявляет распространенное и известное вредоносное ПО.
- Позволяет оперативно и точно локализовать угрозу в сети и провести реагирование.
- Выявляет скрытые угрозы в сети с помощью ретроспективного анализа.
- Легко интегрируется в существующую инфраструктуру, обеспечивает очень высокую производительность.

Ключевые слова:

антивирусная защита, статический анализ, проверка файлов

PT Platform 187

Несколько продуктов PT в одном комплексе. Позволяет реализовать основные функции кибербезопасности в сетях до 500 узлов. Если больше 500 — предлагаем постепенное расширение до enterprise-версий продуктов.

Кому предлагать:

1. Небольшим заказчикам, у которых есть объекты КИИ (например, региональным органам власти).
2. Большим заказчикам с распределенной инфраструктурой, где можно выделить сегменты с объектами КИИ размером не более 500 сетевых узлов.
3. Есть АСУ ТП.

Как понять потребность:

1. Заказчик хочет или должен соответствовать законодательству (КИИ, ИСПДн, ГИС).
2. Нужно приобрести много средств защиты, а денег сразу на все не хватает.
3. Заказчик хочет построить SOC.

Ключевые преимущества:

- Присутствует в 5 конфигурациях, состав комплекса подбирается в зависимости от типа бизнеса и его инфраструктурных особенностей.
- Выполнение основных требований 187 ФЗ.
- Подходит для небольших инфраструктур.

Ключевые слова:

коробочное решение, 187-ФЗ, ГосСОПКА, КИИ, ИСПДН, ГИС, построение основных процессов ИБ

ПТ Ведомственный центр

Управление инцидентами и взаимодействие с ГосСОПКА (ФСБ) и ФинЦЕРТ.

Кому предлагать:

1. Компаниям с объектами КИИ.
2. Всем, кто хочет подключиться к ГосСОПКА.
3. Компаниям, которые начинают строить SOC.

Как понять потребность:

1. Заказчик хочет (должен) передавать инциденты в ГосСОПКА или в ФинЦЕРТ.
2. Необходима автоматизация и контроль процесса реагирования на инциденты.

Ключевые преимущества:

- Визуальный контроль процесса реагирования на инциденты.
- Гибкая конфигурация системы учитывает особенности компании.
- Автоматизация базовых сценариев работы с инцидентами, а также возможность создания автоматического сценария под задачи заказчика.
- Взаимодействие с НКЦКИ и ФинЦЕРТ.
- Автоматическое формирование карточки инцидента в «правильном» для регулятора формате.

Ключевые слова:

ГосСОПКА, 187-ФЗ, 161-ФЗ, взаимодействие с НКЦКИ, взаимодействие с ГосСОПКА, взаимодействие с ФСБ России, взаимодействие с ФинЦЕРТ, регистрация инцидентов, управление инцидентами, автоматические сценарии для обработки инцидентов.