



POSITIVE TECHNOLOGIES

Positive Technologies Network Attack Discovery

PT NAD

Описание продукта

В 2 раза

выросло в 2017 году число компаний, которые стали жертвами целевых атак

197 дней

среднее время присутствия злоумышленника в инфраструктуре

90% атак

не выявлялись жертвами из-за отсутствия процессов threat hunting и расследования сетевых инцидентов

Только 1 из 20

компаний хранит сырой трафик для расследований

Почему нужно хранить и анализировать сетевой трафик

Среднее время присутствия атакующих в корпоративных инфраструктурах составляет 197 дней¹, и лишь 10% атак выявлялись самими жертвами². Это связано с тем, что растет количество инструментов для реализации атак, а способы компрометации постоянно адаптируются к методам защиты. В результате растет количество сложных многоступенчатых атак. Число компаний, столкнувшихся с целевыми атаками, увеличилось в 2017 году почти вдвое³.

Традиционных средств безопасности, таких как IDS/IPS, межсетевые экраны, антивирусные средства, уже недостаточно для противодействия угрозам. Вовремя выявлять атаки и качественно им противодействовать помогают:

- процесс постоянного поиска следов компрометации (threat hunting) — он позволяет выявлять угрозы до того, как они нанесли ущерб;
- расследование инцидентов (позволяет выработать компенсирующие меры для предотвращения аналогичных атак в будущем).

Детально расследовать инциденты помогает сырой трафик подозрительных сессий и метаданные. Они позволяют определить, не является ли срабатывание ложным, оценить успешность атаки и понять ее контекст — IP-адрес атакующего, все активности с этого адреса, наличие соединений с атакующим изнутри инфраструктуры, периодичность соединений, объем переданных данных, репутацию передаваемых объектов, задействованные порты и приложения.

Проведенные нами расследования показывают, что только 5% российских компаний хранят сырой трафик.

Обзор продукта

PT Network Attack Discovery — решение для выявления следов компрометации в сетевом трафике и расследования атак.

Глубоко анализирует сетевой трафик

Определяет 50 протоколов и разбирает до уровня L7 включительно 30 наиболее распространенных из них.

Выявляет сетевые атаки и аномалии

Использует более 3000 сигнатур и технологию выявления сетевых аномалий, разработанные экспертами Positive Technologies, а также репутационные списки.

Помогает детально расследовать атаки

Дает глубокое понимание контекста атаки за счет того, что хранит сырой трафик и 1200 параметров сессий без ограничений по времени.

1 Cost of Data Breach Study: securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

2 Кибербезопасность 2016–2017: от итогов к прогнозам: ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016-2017-rus.pdf

3 Кибербезопасность (2017–2018): цифры, факты, прогнозы: ptsecurity.com/upload/corporate/ru-ru/analytics/cybersecurity-2017-2018-rus.pdf

Как работает

PT Network Attack Discovery захватывает и разбирает сетевой трафик не только на периметре, но и в инфраструктуре. Это позволяет выявлять активность атакующих извне и специфические внутренние атаки.

Служба ИБ или внешние эксперты анализируют в системе метаданные и сырой трафик, что помогает выявлять следы компрометации, подтверждать атаку, проводить расследование и собирать доказательную базу.

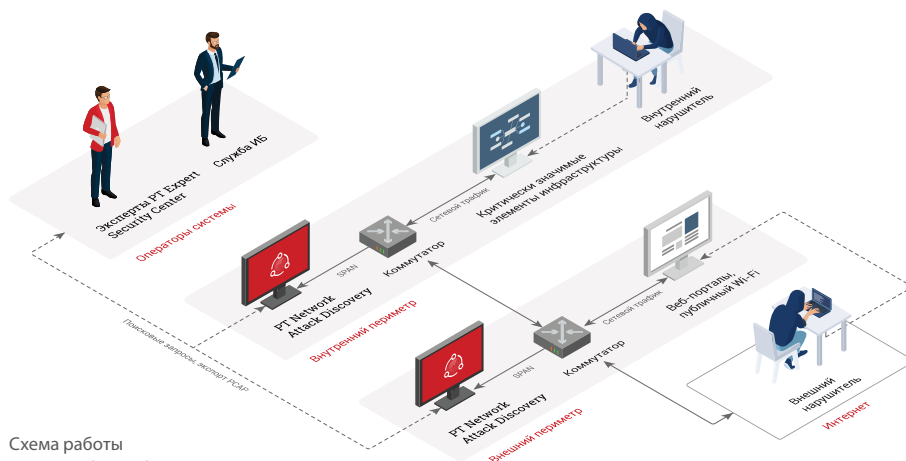


Схема работы
PT Network Attack Discovery

Автоматический анализ вредоносного ПО с помощью PT MultiScanner

Благодаря глубокой интеграции продуктов подозрительные файлы автоматически отправляются на сканирование в систему выявления вредоносного программного обеспечения PT MultiScanner. После анализа файла система возвращает в PT Network Attack Discovery результат сканирования. Это ускоряет реагирование на атаки с применением вредоносного ПО и их расследование.

Особенности

Собственные сигнатуры, востребованные мировыми лидерами

Наши сигнатуры признают лидеры рынка threat intelligence. Emerging Threats расширяет ими набор правил ET Open, а Cisco Talos включает их в пакеты сигнатур для системы обнаружения и предотвращения вторжений Snort.

Сквозная фильтрация по 1200 параметрам сессий

Проверяйте гипотезы для поиска следов компрометации: оперативно находите нужные сессии и фильтруйте подозрительные по 1200 параметрам (IP-адреса, значения полей протоколов, репутация передаваемых объектов, задействованные порты, приложения).

Автоматическое извлечение файлов для анализа на наличие вредоносного ПО

Извлекайте и анализируйте в антивирусных системах подозрительные файлы, передаваемые через протоколы прикладного уровня — HTTP, FTP, POP3, SMTP, SMB, NFS.

Экспорт и импорт трафика для экспертного анализа

Загружайте сырой трафик в формате PCAP из других систем для поиска следов компрометации и извлекайте его для передачи экспертам на глубокий анализ в рамках расследования.

Хранение данных об атаках внутри компании

PT Network Attack Discovery хранит все данные в инфраструктуре заказчика и не передает сведения об атаках вовне. Это позволяет избежать нежелательного распространения информации.

Интеграция с антивирусными и SIEM-системами

Управляйте инцидентами в SIEM-системах и выявляйте вредоносный контент в передаваемых по сети файлах при помощи антивирусных решений.

Результаты применения

Предотвращает потери.

Выявляет сетевые атаки до того, как они нанесли серьезный денежный или репутационный ущерб.

Повышает результативность расследований.

Подробно анализирует трафик, позволяет реконструировать сессии, хранит сырой трафик без ограничений по времени и помогает выявлять признаки компрометации, не обнаруженные ранее.

Помогает выявлять целевые атаки.

PT Network Attack Discovery в комплексе с MaxPatrol SIEM и PT MultiScanner помогает выстроить эффективную систему защиты от целевых атак.

Помогает соответствовать требованиям законодательства.

PT Network Attack Discovery позволяет выполнить требования по защите:

- критической информационной инфраструктуры (приказ ФСТЭК России № 239, методические рекомендации ФСБ России по созданию центров ГосСОПКА),
- персональных данных (приказ ФСТЭК России № 21),
- информации в ГИС, в АСУ ТП и в информационных системах общего пользования (приказы ФСТЭК России № 17, 31 и 489).

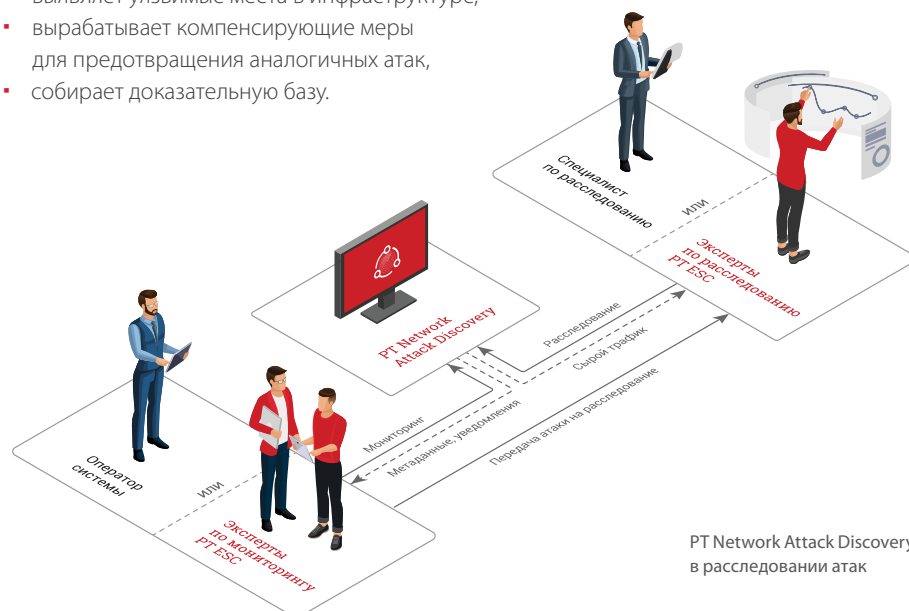
Сценарии использования

Для расследования атак

Внутренний оператор ИБ или специалист PT Expert Security Center в рамках услуг по экспертному мониторингу отслеживает атаки и, анализируя метаданные, делает вывод об их успешности. О выбранных типах атак PT Network Attack Discovery уведомляет автоматически.

Специалист передает сообщение об атаке внутренней или сторонней команде, которая занимается расследованием инцидентов. С помощью PT Network Attack Discovery команда:

- восстанавливает хронологию атаки,
- оценивает нанесенный ущерб,
- выявляет уязвимые места в инфраструктуре,
- вырабатывает компенсирующие меры для предотвращения аналогичных атак,
- собирает доказательную базу.



Поддержка экспертами PT Expert Security Center

Специалисты центра безопасности PT Expert Security Center дополняют команду ИБ при недостатке экспертизы или полностью берут на себя задачи по мониторингу событий безопасности сетевого трафика и расследованию атак.

Для обнаружения атак

Для выявления атак PT Network Attack Discovery использует сигнатуры, репутационные списки, технологии выявления аномалий и автоматически сгенерированных доменов. Сигнатуры срабатывают, когда эксплуатируется уязвимость, распространяется вредоносное ПО или атакующие используют специальный инструментарий. Также сигнатуры помогают обнаружить нарушение политик безопасности и ошибки в конфигурации систем.

Репутационные списки содержат индикаторы компрометации и помогают выявить ботов, фишинг, вредоносные сайты и файлы.

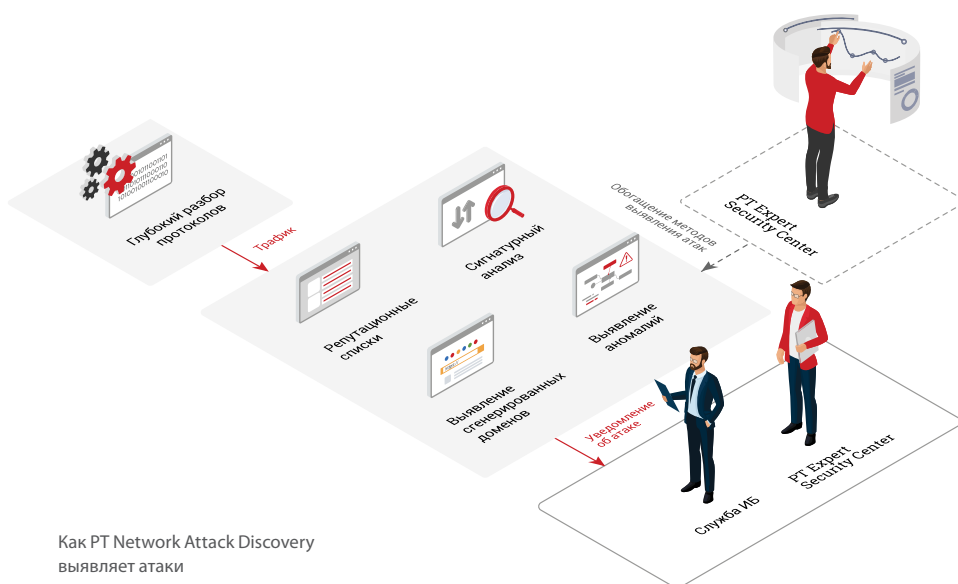
Технология выявления аномалий следит за отклонениями в поведении пользователей и нестандартными показателями в сетевом трафике, что помогает выявить присутствие злоумышленника.

На основе технологии машинного обучения специальный модуль распознает доменные имена, созданные при помощи алгоритмов генерации доменов (DGA). Это помогает выявить вредоносное ПО, которое пытается через подобные домены установить соединение со своим командным центром.

Сигнатуры, написанные экспертами PT ESC, выявляют эксплуатацию уязвимостей, программы для взлома, вредоносное ПО, которые не детектируются сигнатурами ET Open.

- Для написания правил для выявления эксплуатации уязвимостей мы автоматически собираем информацию о новых уязвимостях, в том числе о тех, которые еще не попали в базу данных CVE. Это ускоряет выпуск новых правил и позволяет выявлять эксплуатацию до наступления серьезных последствий.
- Наши эксперты проводят более ста пентестов в год, расследуют сложные атаки, постоянно изучают новые угрозы. Поэтому они знают обо всех распространенных тактиках атакующих, и созданные ими сигнатуры выявляют применение всех популярных хакерских инструментов.
- Для написания правил выявления вредоносных программ мы используем специальный механизм, который группирует образцы ВПО по схожей активности в трафике. В результате одно правило срабатывает сразу на все семейство вредоносных программ. Это сокращает количество сигнатур, не снижая их эффективности.

Эксперты PT Expert Security Center еженедельно пополняют набор репутационных списков и сигнатур. С обновлением набора пользователи могут провести ретроспективный анализ трафика и выявить не обнаруженные ранее атаки.



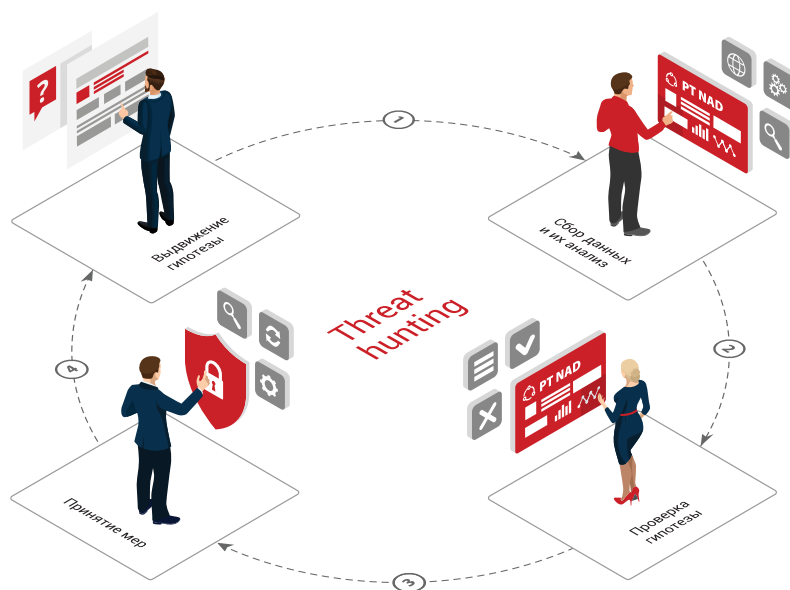
Почему PT Network Attack Discovery не разбирает протокол HTTPS

HTTPS в пользовательском трафике с каждым днем все больше. Ежедневно анализируемые нами образцы вредоносного ПО показывают, что их разработчики либо шифруют данные на зараженной машине и передают их поверх TCP, либо используют самописные протоколы. Мы разрабатываем сигнатуры, которые умеют выявлять такие соединения без необходимости заглядывать в содержимое.

Threat hunting — выявление скрытых атак

PT Network Attack Discovery помогает выстроить процесс threat hunting в организации и выявлять даже скрытые угрозы, которые не обнаруживаются стандартными средствами кибербезопасности.

Аналитик ИБ или специалист PT Expert Security Center, обладая необходимой квалификацией и знаниями об инфраструктуре, выдвигает гипотезы, например о присутствии хакерской группировки в сети, проведении конкурентной разведки, наличии внутреннего нарушителя или об утечке данных. PT Network Attack Discovery помогает проверять гипотезы и выявлять угрозы до того, как они нанесли серьезный ущерб.

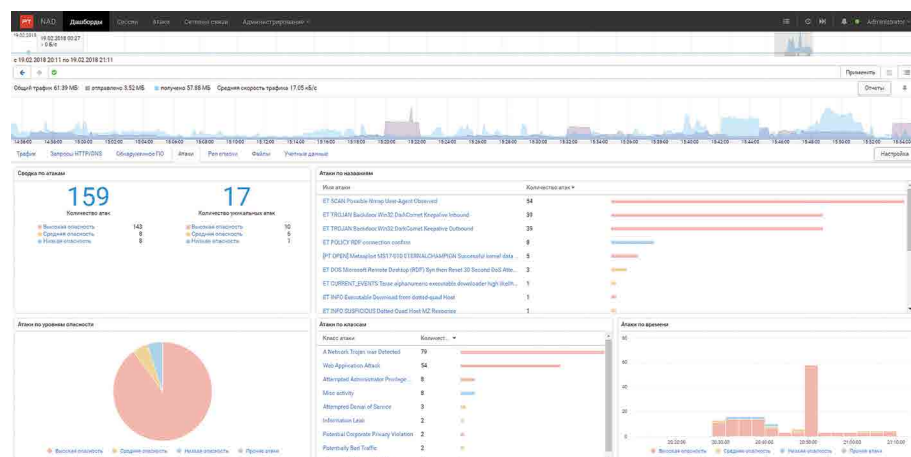


Использование PT Network Attack Discovery в процессе threat hunting

Ключевые возможности

Мониторинг атак

На дашборде выводятся количество атак в динамике и уровень их опасности. Здесь можно получить детальную информацию об атаках, которая поможет специалистам оперативно расследовать инциденты и принимать решения о реагировании.



Ретроспективный анализ

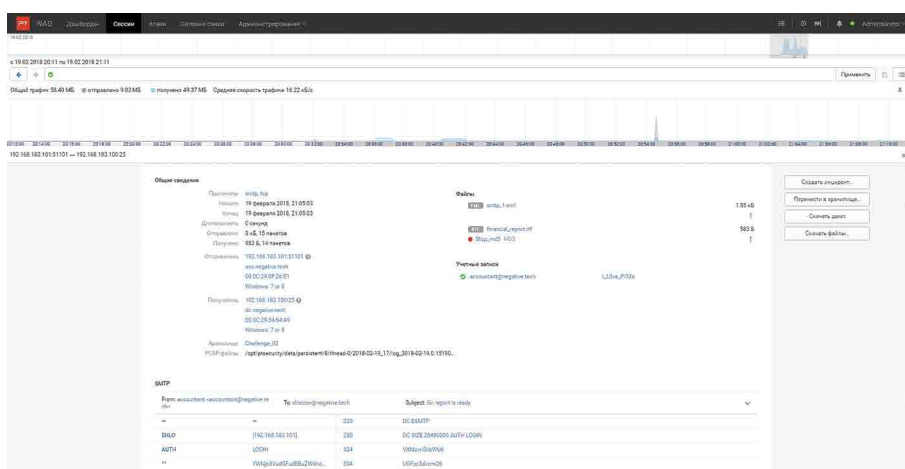
После обновления набора сигнатур или репутационных списков пользователи могут повторно проанализировать трафик и метаданные, что позволяет выявлять не обнаруженные ранее признаки компрометации.

Отсканируйте QR-код и [посмотрите](#), как PT Network Attack Discovery помогает проводить ретроспективный анализ.



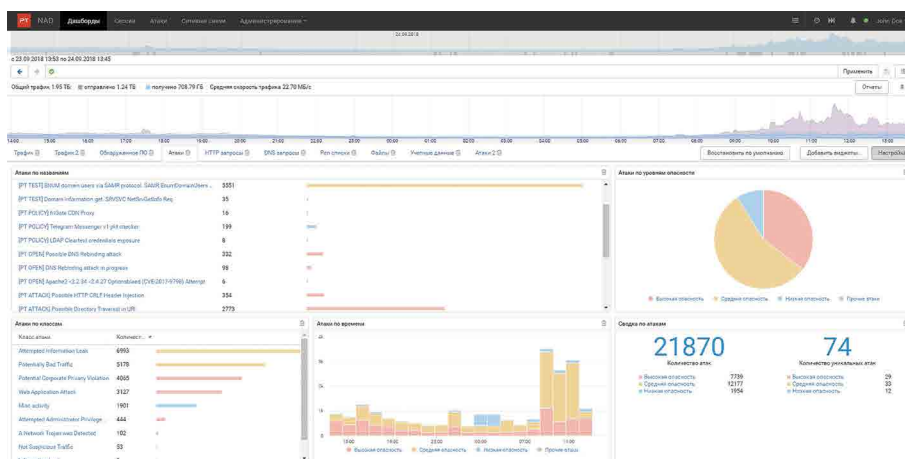
Реконструкция сессий

Оператор ИБ может проанализировать любую подозрительную сессию: сырой трафик хранится с привязкой к конкретной сессии и в один клик извлекается в формате PCAP.



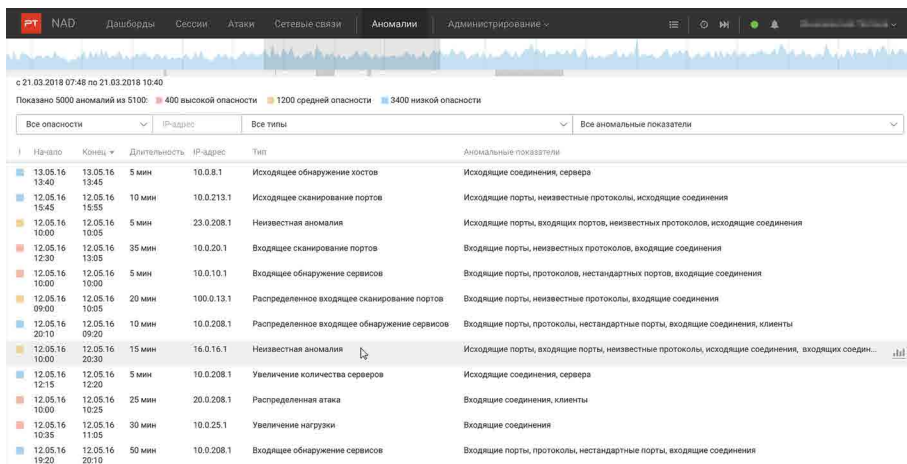
Выявление атак

Система информирует о сработавших сигнатурах и автоматически назначает уровень опасности атак. Оператор ИБ видит список атак, может отфильтровать его по полям сессий и изучить подробную карточку каждой атаки.



Выявление сетевых аномалий

На основе технологии машинного обучения система определяет отклонения показателей в сетевом трафике и сообщает об аномалиях. С помощью автоматического назначения уровня опасности аномалий оператор приоритизирует их обработку.



Начало	Конец	Длительность	IP-адрес	Тип	Аномальные показатели
13.05.16 13:40	13.05.16 13:45	5 мин	10.0.0.1	Исходящее обнаружение хостов	Исходящие соединения, сервера
12.05.16 15:45	12.05.16 15:55	10 мин	10.0.213.1	Исходящее сканирование портов	Исходящие порты, неизвестные протоколы, исходящие соединения
12.05.16 10:00	12.05.16 10:05	5 мин	23.0.208.1	Неизвестная аномалия	Исходящие порты, входящие порты, неизвестных протоколов, исходящие соединения
12.05.16 12:30	12.05.16 13:05	35 мин	10.0.20.1	Входящее сканирование портов	Входящие порты, неизвестных протоколов, входящие соединения
12.05.16 10:00	12.05.16 10:05	5 мин	10.0.10.1	Входящее обнаружение сервисов	Входящие порты, протоколов, нестандартных портов, входящие соединения
12.05.16 09:00	12.05.16 10:05	20 мин	100.0.13.1	Распределенное входящее сканирование портов	Входящие порты, неизвестные протоколы, входящие соединения
12.05.16 20:10	12.05.16 09:20	10 мин	10.0.208.1	Распределенное входящее обнаружение сервисов	Входящие порты, протоколы, нестандартные порты, входящие соединения, клиенты
12.05.16 10:00	12.05.16 20:20	15 мин	16.0.16.1	Неизвестная аномалия	Исходящие порты, входящие порты, неизвестные протоколы, исходящие соединения, входящих соедин...
12.05.16 12:15	12.05.16 12:20	5 мин	10.0.208.1	Увеличение количества серверов	Исходящие соединения, сервера
12.05.16 10:00	12.05.16 10:25	25 мин	20.0.208.1	Распределенная атака	Входящие соединения, клиенты
12.05.16 10:35	12.05.16 11:05	30 мин	10.0.25.1	Увеличение нагрузки	Входящие соединения
12.05.16 19:20	12.05.16 20:10	50 мин	10.0.208.1	Входящее обнаружение сервисов	Входящие порты, протоколы, нестандартные порты, входящие соединения

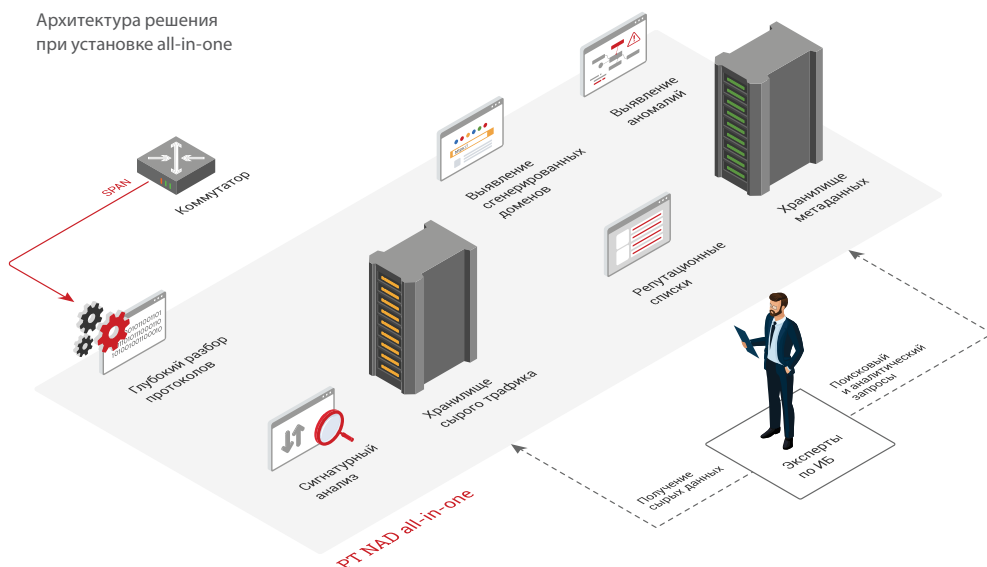
Модели развертывания

Для повышения эффективности выявления атак и следов компрометации рекомендуем разворачивать систему как во внутренней инфраструктуре, так и на периметре. Такой подход позволяет выявлять атаки на разных этапах их развития.

Развертывание возможно в двух вариантах — all-in-one и распределенное.

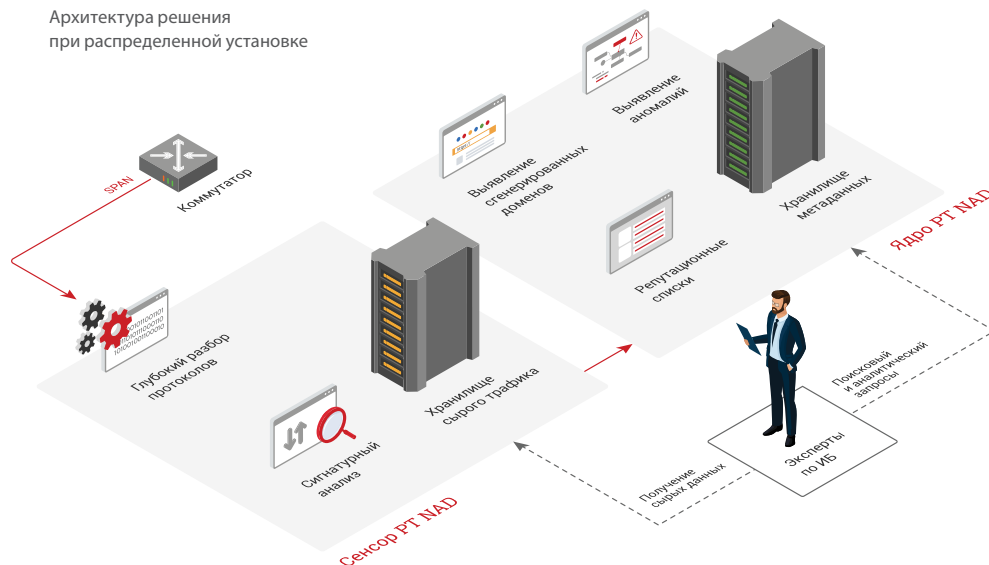
В случае установки all-in-one используется один сервер.

Архитектура решения при установке all-in-one



При распределенной установке необходимы как минимум два сервера: один для сенсора NAD и хранения сырого трафика, второй для ядра системы Core и хранения метаданных. В случае большого объема трафика могут потребоваться дополнительные серверы.

Архитектура решения
при распределенной установке



Варианты поставки

PT Network Attack Discovery поставляется в двух вариантах:

- Virtual Appliance для развертывания на виртуальной машине;
- Hardware Appliance для развертывания на физическом сервере. Включает компоненты аппаратного обеспечения, системного программного обеспечения и программного обеспечения PT Network Attack Discovery.

Для поставки PT Network Attack Discovery в варианте Hardware Appliance необходимо приобрести права на использование программного обеспечения PT Network Attack Discovery и аппаратное обеспечение Positive Technologies.

Благодаря внедрению PT Network Attack Discovery мы получили полезный инструмент для исследования инцидентов, смогли решить проблему контроля вредоносной и злонамеренной активности в сетевом трафике, а также провели подготовку к выполнению требований регулирующих органов.

Дмитрий Сафронов, начальник отдела защиты информации ВГТРК



Попробуйте бесплатно

Узнайте, как вас атакуют, — закажите «пилот» PT Network Attack Discovery.



О компании

ptsecurity.com
pt@ptsecurity.com

facebook.com/PositiveTechnologies
facebook.com/PHDays

Positive Technologies — один из лидеров европейского рынка систем анализа защищенности и соответствия стандартам, а также защиты веб-приложений. Организации во многих странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, для выполнения требований регулирующих организаций и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня в вопросах защиты SCADA- и ERP-систем, крупнейших банков и телеком-операторов.

Деятельность компании лицензирована Минобороны России, ФСБ России и ФСТЭК России, продукция сертифицирована Минобороны России и ФСТЭК России.