PT Network Attack Discovery для IT

t.me/PTNADChat

Заказать пилот PT NAD

ptsecurity.com

Оглавление

Предпосылки

Проблема shadow IT («теневых ИТ») по-прежнему остается одной из самых острых для IT-специалистов. В корпоративных сетях продолжают использоваться сервисы и программы, которые нарушают внутренний регламент. На первый взгляд, решение этой проблемы уже существует. Есть целый ряд ПО, которое может контролировать параметры сети и все, что в ней установлено. Например, Microsoft Endpoint Configuration Manager (MECM) дает возможность управлять IT-инфраструктурой на базе Windows. MECM помогает следить за обновлениями, развертывать ПО и операционные системы, инвентаризировать аппаратное и программное обеспечение, удаленно управлять сетевыми узлами, виртуальными и мобильными системами. В целом этот инструмент должен решать большую часть операционных проблем IT-специалистов. На практике не все так гладко.

Для того чтобы использовать MECM, нужно подключить все сетевые узлы к Active Directory и установить на каждый из них агент. Сделать это централизованно для всех компьютеров с Windows — утопичное решение, в итоге все равно что-нибудь пойдет не так. Часть узлов по какой-то причине не подключится к Active Directory, агенты MECM запустятся не на всех узлах, все это вместе — еще одна головная боль для IT.

Что касается пользователей корпоративной сети, то они — главный источник проблем: подключают собственные устройства (BYOD) со сторонним ПО, устанавливают сомнительный софт, работают на отличных от Microsoft операционных системах (Linux, macOS). Не стоит забывать и о средах виртуализации. Например, сотрудники могут для собственных нужд создавать виртуальные рабочие станции внутри гипервизора с разнообразным набором ОС и ПО и обходить корпоративный регламент IT.

Таким образом, стандартный инструмент не помогает решить проблему shadow IT. Используя только его, все равно придется дополнительно анализировать инфраструктуру и контролировать ее состояние с помощью дополнительных средств. Иначе айтишник останется без малейшего представления о том, что происходит в сети, какое ПО и какие ОС используются на сетевых узлах, а самое главное — не сможет вовремя принять меры.

Какие задачи решает PT NAD

PT NAD — система глубокого анализа сетевого трафика (NTA) 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 NAD обнаруживает следы хакера в сети компании, но также работает и с копией трафика, а значит, может быть полезен для IT-подразделений.

Какие задачи IT решает PT NAD:

1. Запись, разбор (анализ) и хранение копии трафика с сетевого оборудования.
2. Анализ загрузки каналов и построение статистики на основе копии трафика.
3. Сбор информации об используемых ОС и ПО.
4. Контроль состояния сетевых подключений.
5. Поиск новых сетевых узлов и управление ими.
6. Профилирование сетевых узлов.
7. Определение учетных данных пользователей.
8. Обнаружение средств удаленного администрирования.
9. Обнаружение использования сторонних сервисов.

Чем NTA полезен для IT

PT NAD помогает решить ряд IT-задач с помощью технологии DPI.

1. Захват пакетов и хранение дампов трафика

Проблема: сеть постоянно изменяется. Приложений появляется все больше, контролировать их становится сложнее. В определенный момент могут возникнуть проблемы с сетью: потеря связи, «дропы» пакетов трафика, ошибки. Для того чтобы определить проблемные участки сети и выяснить, кто «засоряет эфир», необходимо поработать с копией трафика и метаданными, собранными за конкретный период. И не просто поработать, а тщательно разобрать и понять трафик. Без специальных инструментов сделать это сложно.

Решение: PT NAD записывает, разбирает и хранит сырой трафик. Продукт определяет следующие сетевые протоколы: amqp, bittorrent, canon-bjnp, clickhouse, db2-drba, dcerpc, dhcp, dhcpv6, dns, drweb, dtls, elasticsearch, encrypted, facebook, falcongaze, fb-zero, ftp, guardant, http, icap, imap, infowatch, isakmp, jrmi, kerberos, ksn, ldap, llmnr, lotus, mc-nmf, mdns, memcache, mongodb, ms-scom, ms-update, mysql, nat-t, nbns, nfs, ntlm, ntp, openvpn, oracle-tns, p2p-dc, pop3, postgresql, pptp, printer-pjl, printer-ps, quic, radius, rdp, redis, rfb, rlogin, rsync, rtcp, rtsp, sip, skinny-voip, skype, smb, smb-mailslot, smtp, snmp, socks5, ssdp, ssh, stakhanovets, stun, stun-apple, stun-classic, syslog, tds, teamviewer, telnet, tftp, thrift, tls, trueconf, umeye-app, viber, vipaks-data, vipnet, vipnet-mftp, vipnet-sync, vpn_kontinent, vmware, whatsapp, wireguard, ws-discovery, xmpp, zabbix, zmtp, zmtp_v2.

PT NAD использует DPI и анализирует более 1200 параметров в следующих протоколах: dcerpc, dhcp, dns, ftp, http, imap, kerberos, ldap, mc-nmf, mysql, nfs, ntlm, ntp, oracle-tns, pop3, postgresql, quic, rdp, sip, smb, smtp, snmp, socks5, ssh, telnet, tftp, tls.

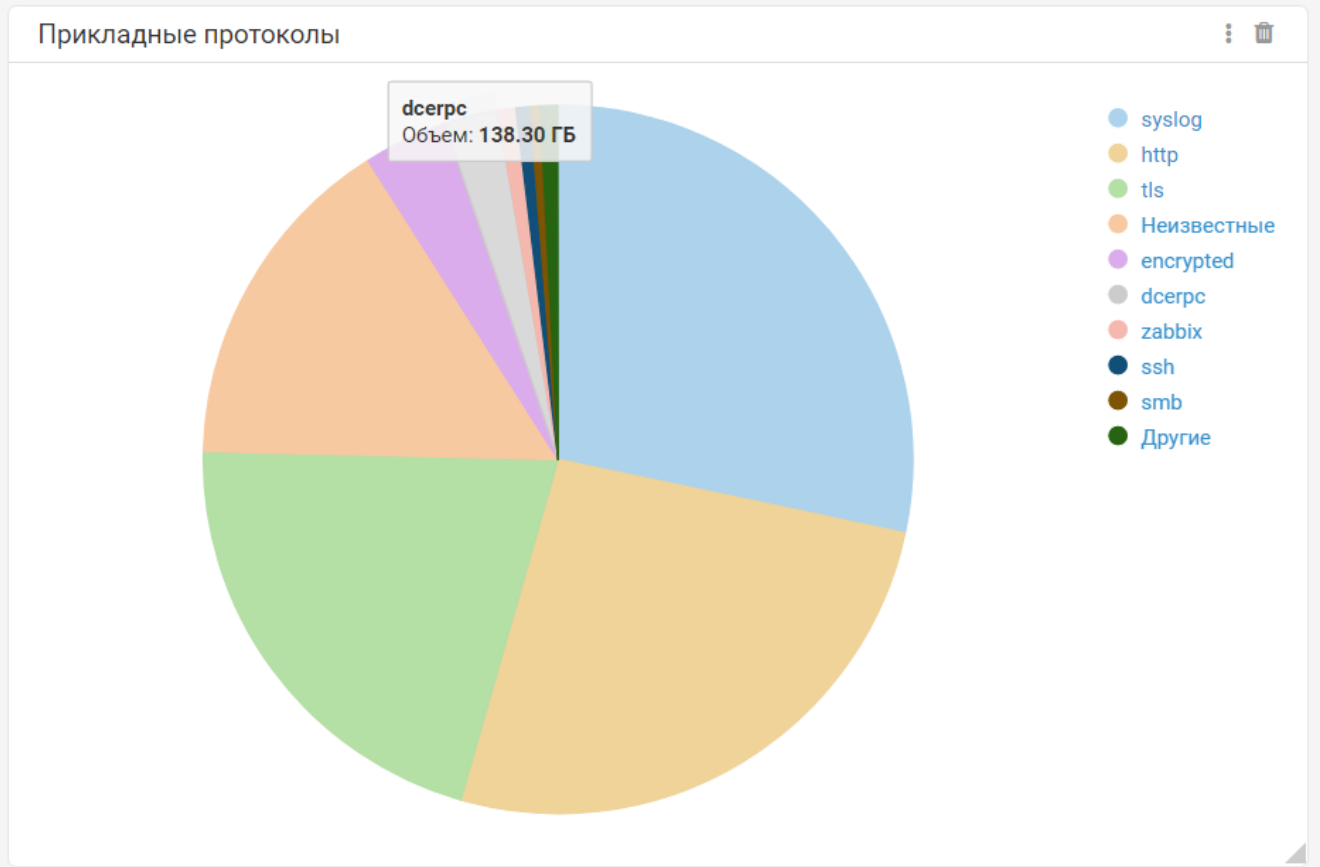

Рисунок 1. Прикладные протоколы в PT NAD

На основе сырого трафика PT NAD формирует метаданные. Для сырого трафика и метаданных предусмотрены раздельные хранилища. Обнаружив проблемы с сетью, PT NAD поможет определить сетевой узел, который «засоряет эфир». Сырой трафик поможет определить довольно точно, когда с узлом произошли изменения. Выгрузив сырой трафик из PT NAD, можно вручную проанализировать пакеты и понять, в чем заключается проблема.

В продукт можно загрузить записанный трафик и проанализировать его. Это полезно в случае, когда нужно протестировать новую систему или программное обеспечение. PT NAD проверит, какие сетевые соединения создает целевая система, и с учетом этого поможет правильно донастроить уже имеющиеся системы.

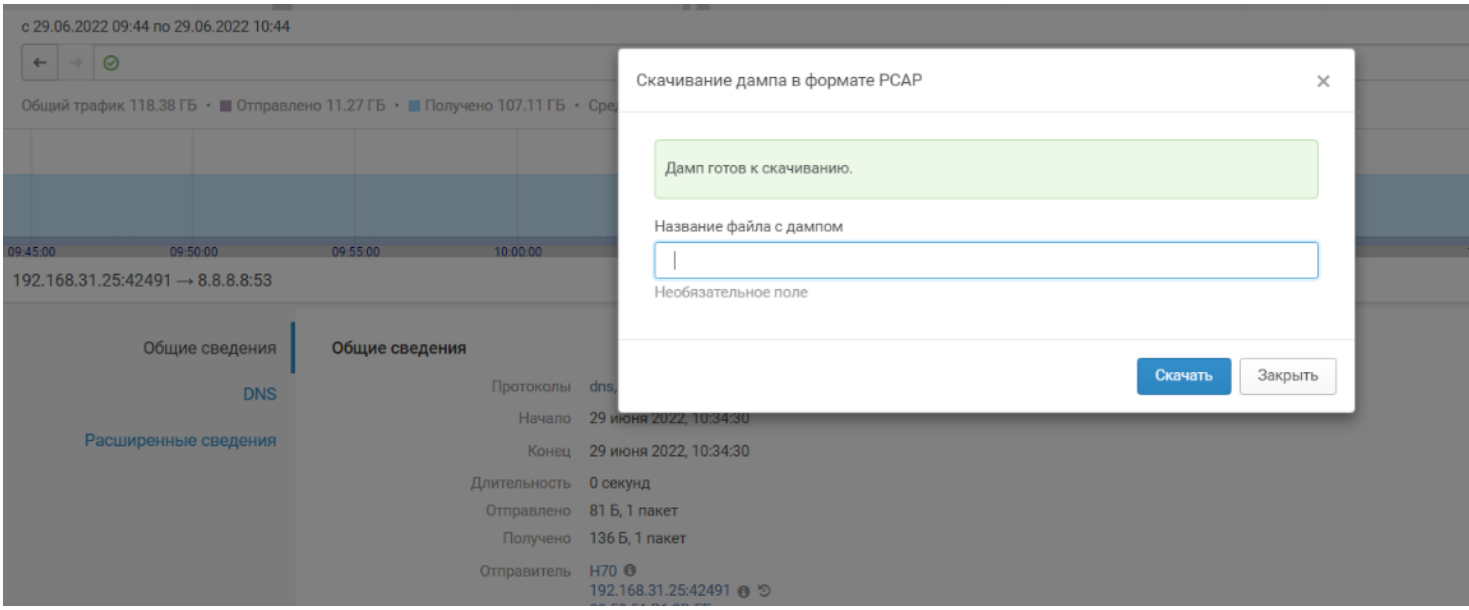

Рисунок 2. Выгрузка сырого трафика из PT NAD

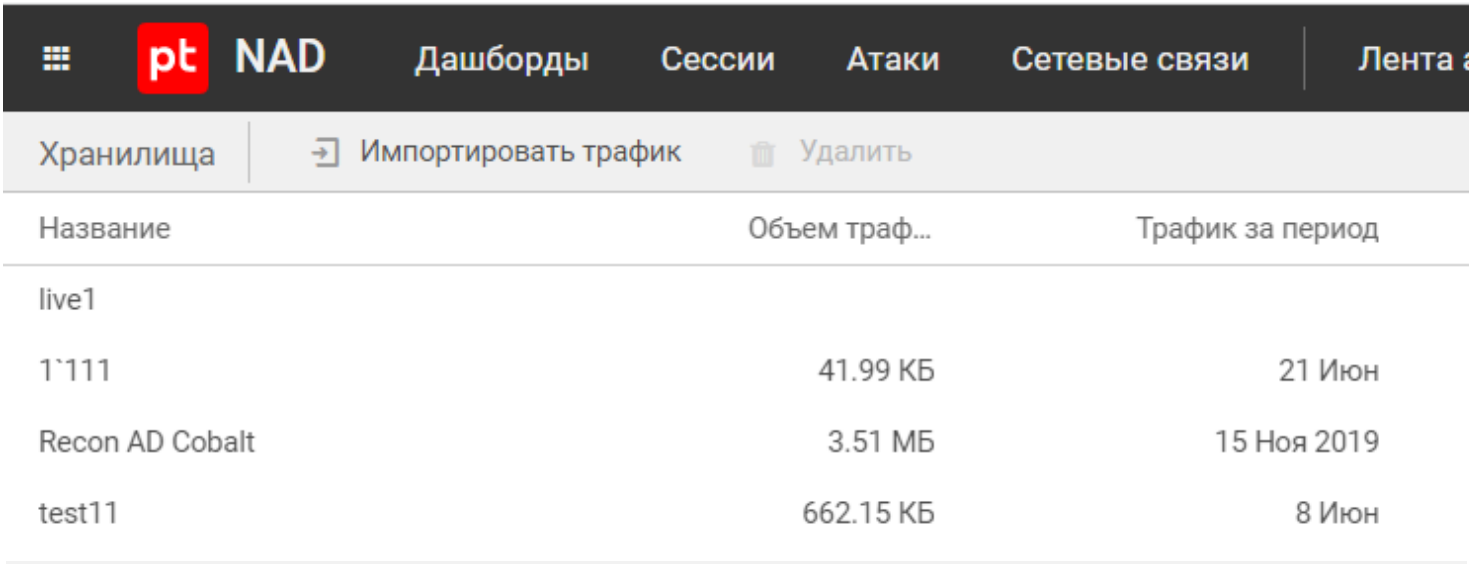

Рисунок 3. Хранилища в PT NAD

2. Анализ загруженности каналов и построение статистики

Проблема: падает производительность сети. Необходимо определить, какие сетевые узлы создают самый большой объем трафика, какое приложение или протоколы при этом используются, а самое главное — нужно понять, в какой момент и с какой частотой это происходит.

Решение: PT NAD работает с копией сетевого трафика и проводит его глубокий анализ, используя технологию DPI. Продукт дает информацию о каждом сетевом узле: об объеме трафика, его интенсивности и доли используемых транспортных и прикладных протоколов. Информация представляется на виджетах дашборда. Ниже приведен пример графического отображения.

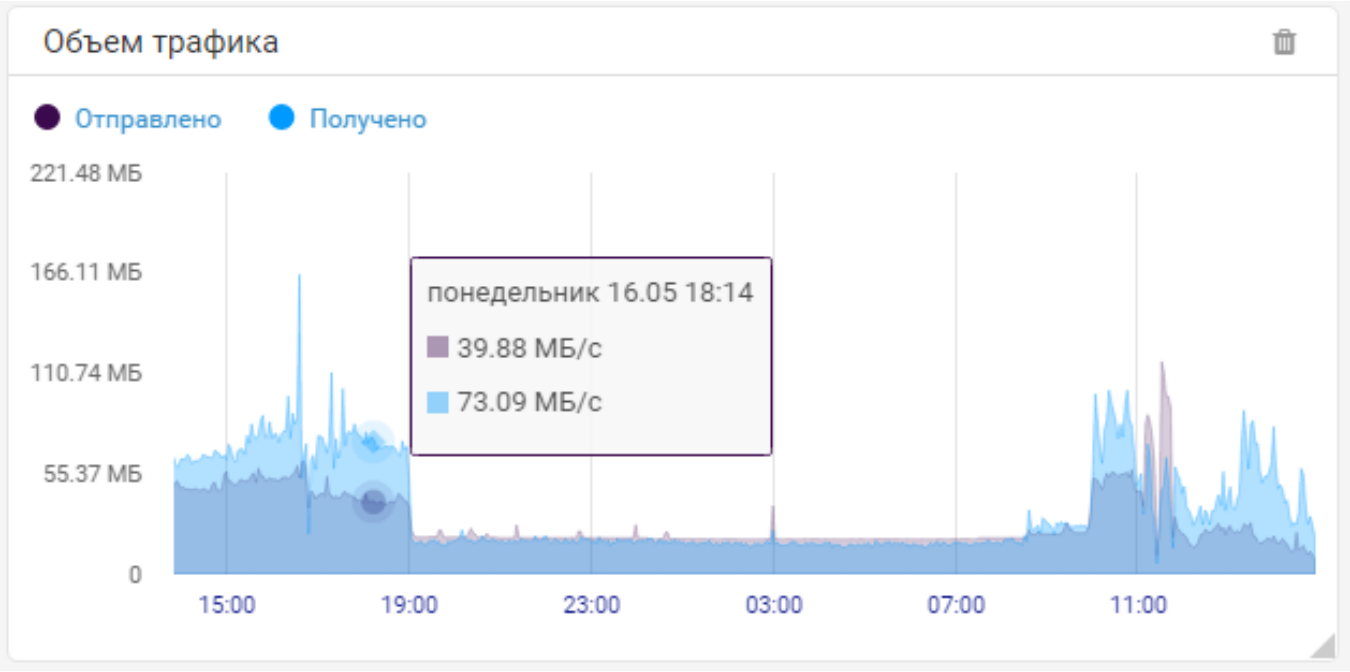

Рисунок 4. Объем передаваемого трафика

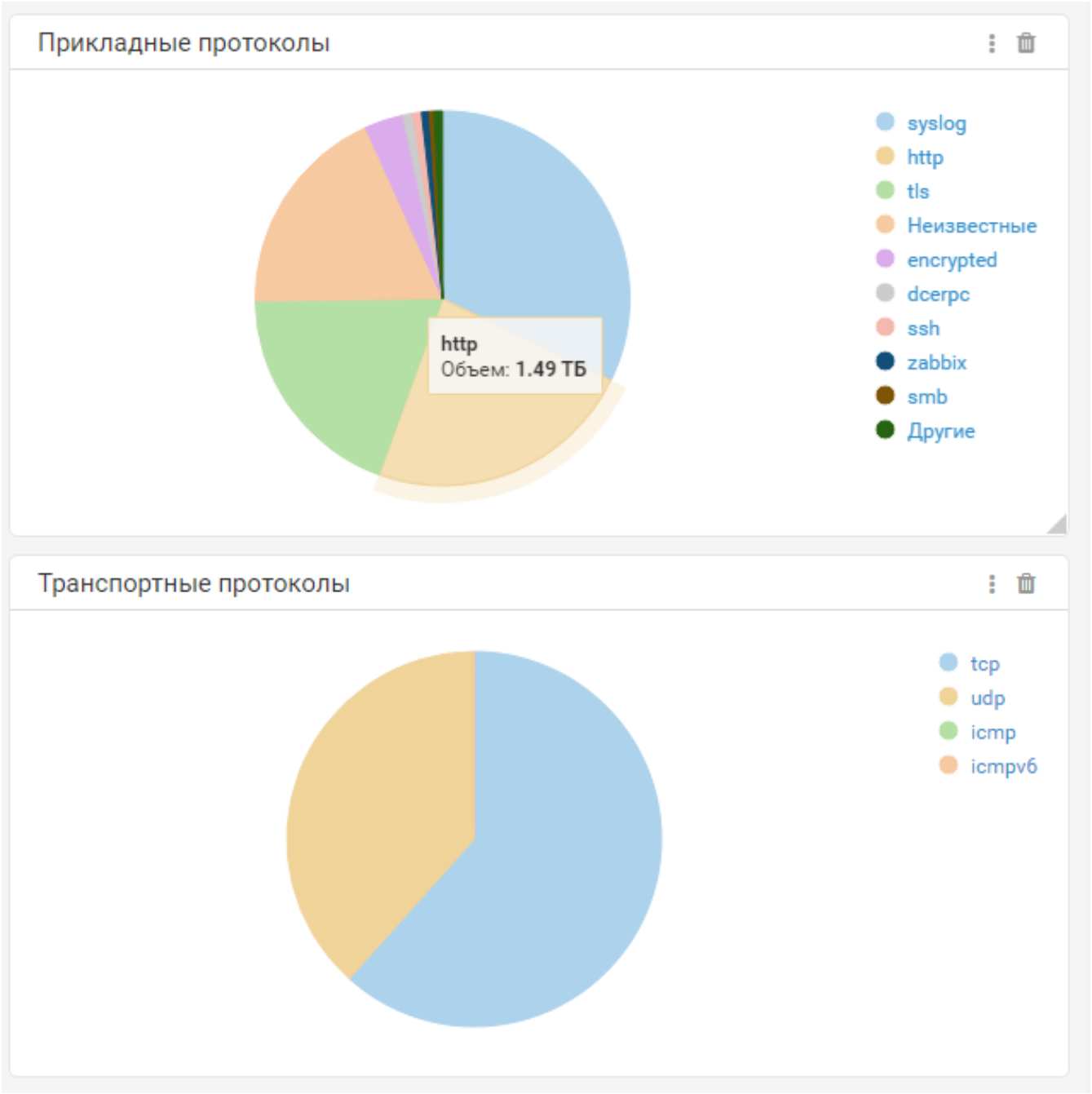

Рисунок 5. Статистика по транспортным и прикладным

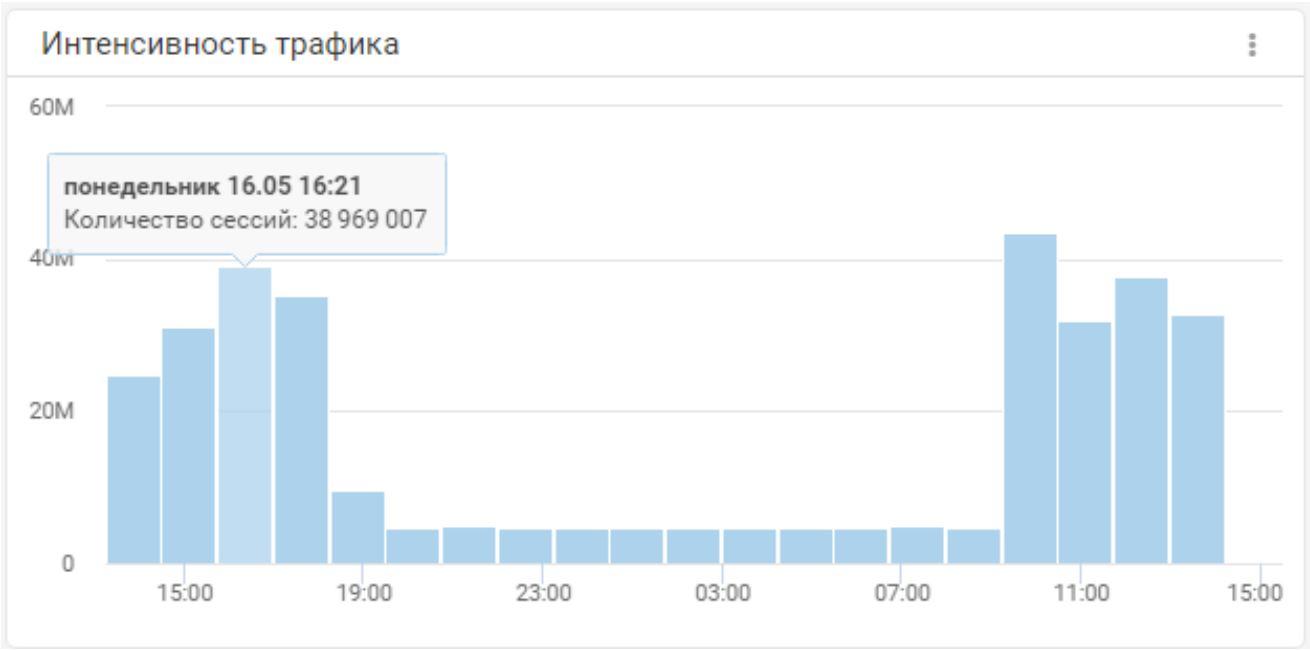

Рисунок 7. Фильтрация сессий с SSH

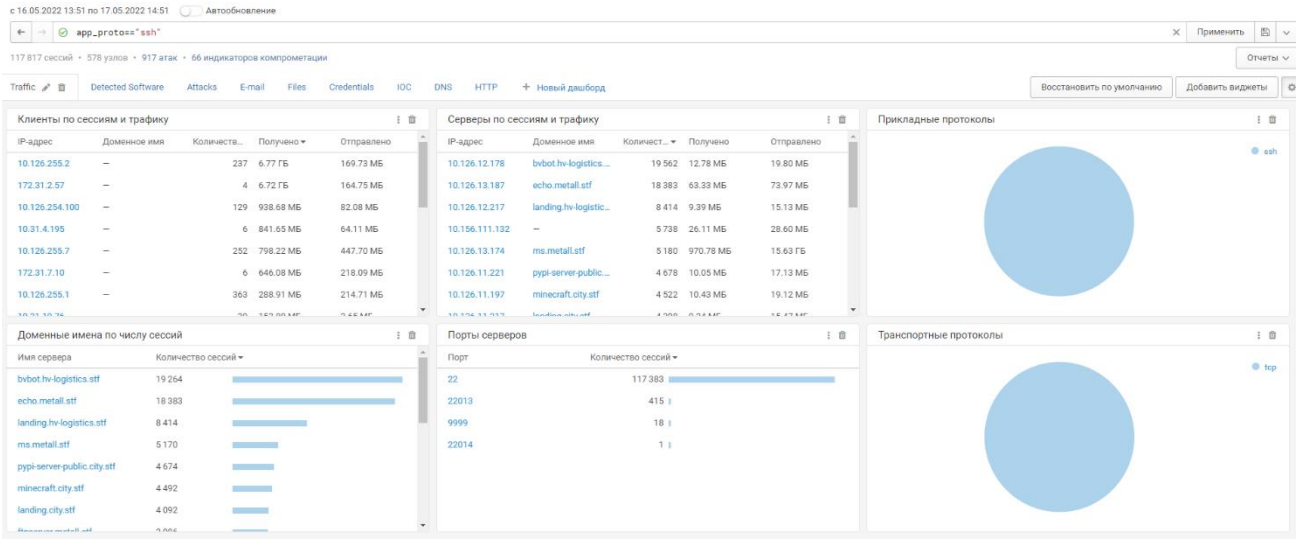

Рисунок 6. Интенсивность трафика по времени

Таким образом, PT NAD помогает определить, какой сетевой узел передает большой поток данных, какой протокол при этом используется и в какой момент это происходит. С помощью этих данных IT-специалисты могут своевременно перенастроить узел или сетевое оборудование, чтобы предотвратить снижение производительности сети.

3. Сбор информации об используемых ОС и ПО

Проблема: пользователи устанавливают стороннее ПО и добавляют свои устройства в корпоративную сеть. Нет механизма, который помог бы контролировать изменения в составе ПО и ОС корпоративной сети.

Решение: PT NAD проводит глубокий анализ (DPI) копии трафика и определяет, какое ПО используется для передачи информации. Продукт показывает, на каких сетевых узлах работает софт и определяет тип ОС.

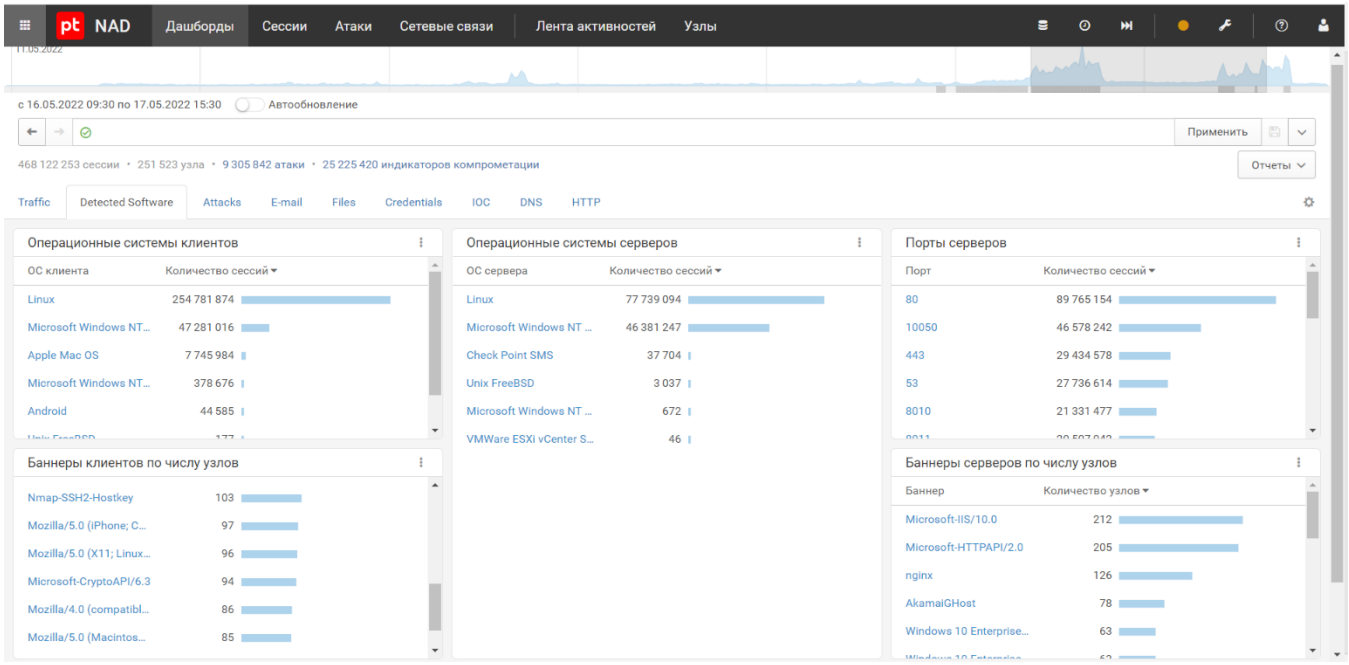

Рисунок 8. Статистика по используемым в сети ОС и ПО

PT NAD помогает IT-специалистам определить сетевые узлы, на которых работает «некорпоративное» ПО, а также быстро определить, какой тип ОС используется, в том числе и на BYOD устройствах. Все это помогает соблюдать IT-регламент компании и постоянно поддерживать в актуальном состоянии информацию о сети.

4. Проверка сетевых связей

Проблема: IT-специалисты перенастроили сетевое оборудование и сегментировали сеть. Необходимо проверить корректность сетевых настроек и определить, могут ли пользователи одного сегмента сети подключаться к другому.

Решение: PT NAD строит график сетевого взаимодействия узлов за выбранный период. Продукт помогает проследить, как выполняется сетевая сегментация, и проконтролировать в режиме реального времени сетевые подключения узлов.

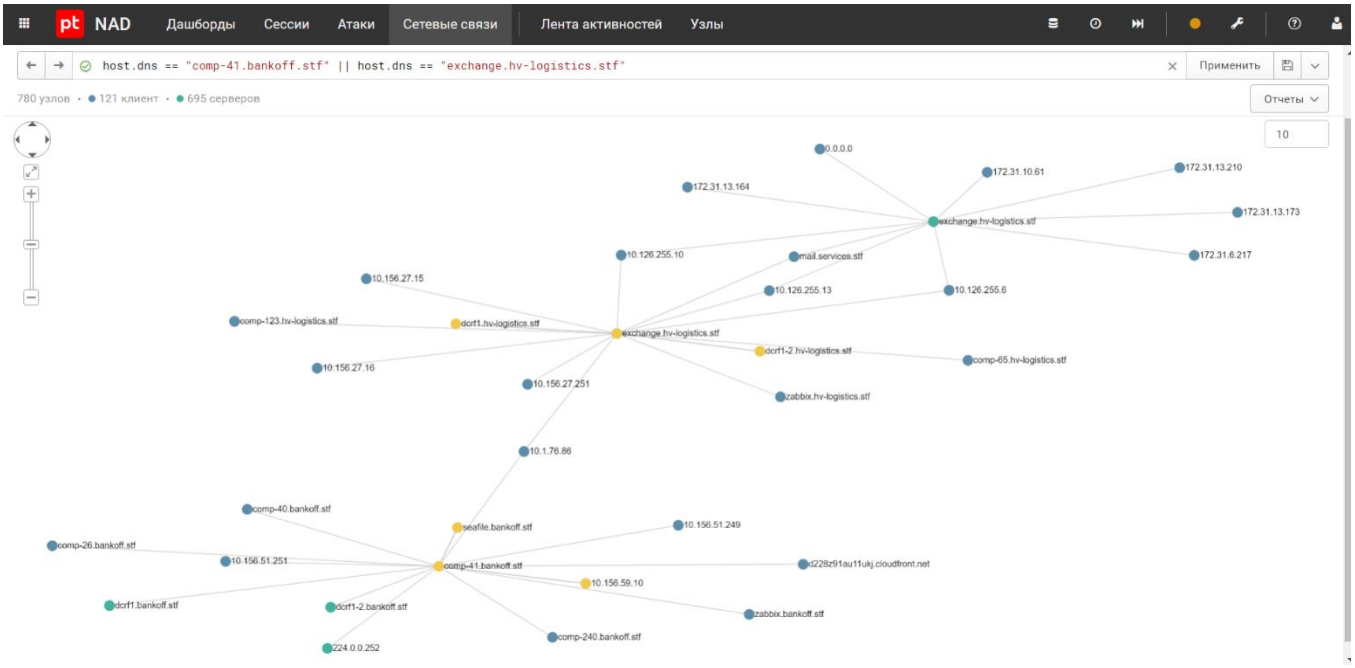

Рисунок 9. Граф сетевого взаимодействия узлов

5. Обнаружение новых сетевых узлов и управление ими

Проблема: у IT-специалистов нет актуальной информации о структуре сети, в том числе о сетевых сегментах. В результате появляются забытые участки сети со своим набором узлов, на которых может быть установлено все что угодно. Пользователи подключают к корпоративной сети собственные устройства: ноутбуки, мобильные устройства. В такой ситуации айтишникам важно своевременно обнаруживать новые сетевые узлы и забытые сегменты сети.

Решение: PT NAD получает данные из копии сетевого трафика и определяет все сетевые узлы в компании. За счет этого продукт может определить shadow IT и сообщить о появлении нового сетевого узла в сети. Внутренний механизм PT NAD не только заметит его, но и определит тип и роль и на основе данных, полученных из трафика, построит сетевой профиль актива.

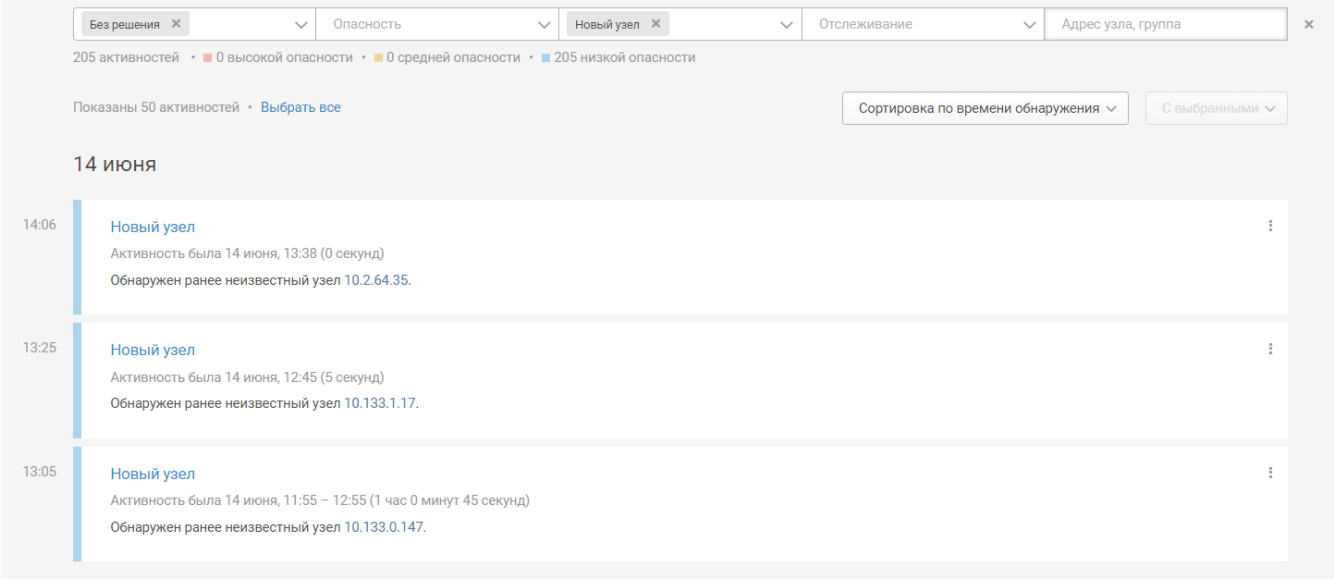

Рисунок 10. Обнаружение новых сетевых узлов

Продукт позволяет поддерживать в актуальном состоянии информацию о внутренних сетевых узлах. Интеграция с другими продуктами Positive Technologies, например с MaxPatrol SIEM, позволит получить максимально подробную модель актива, составленную с учетом 3000 параметров.

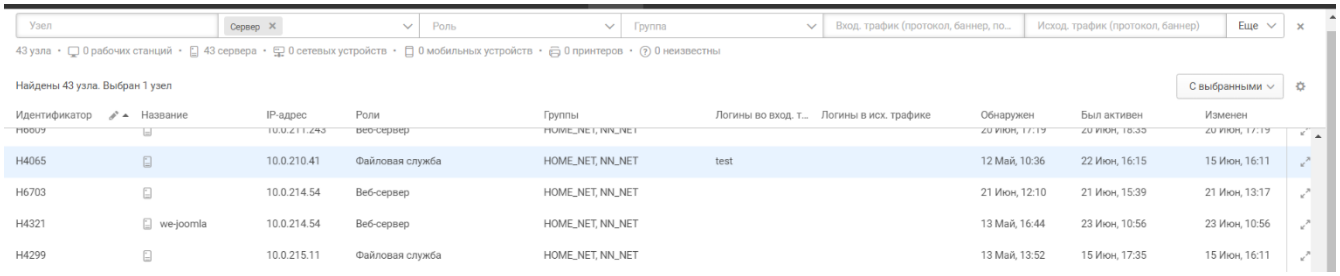

Рисунок 11. Фильтрация по типу сетевого узла

6. Профилирование сетевых узлов

Проблема: поддержание работоспособности и производительности инфраструктуры — обязательная часть операционной деятельности IT-специалистов. Необходимо понимать, что из себя представляет каждый сетевой узел, какую роль он выполняет, и в идеале иметь сетевой профиль узла. Инфраструктура постоянно меняется, сложно профилировать узлы вручную, особенно те, что появляются в сети на короткий промежуток времени. Поэтому нужен инструмент, который автоматически обнаруживает новые узлы, определяет их роль и строит сетевой профиль активов.

Решение: PT NAD умеет определять тип устройства и строить сетевой профиль актива. Это решает проблему ручного анализа каждого сетевого узла. Профиль строится автоматически, предусмотрен механизм ручного переопределения роли сетевого актива. Продукт показывает, когда был обнаружен узел, когда был активен, когда изменен, автоматически определяет доменное имя, используемые на узле логины и пароли, какой трафик был создан.

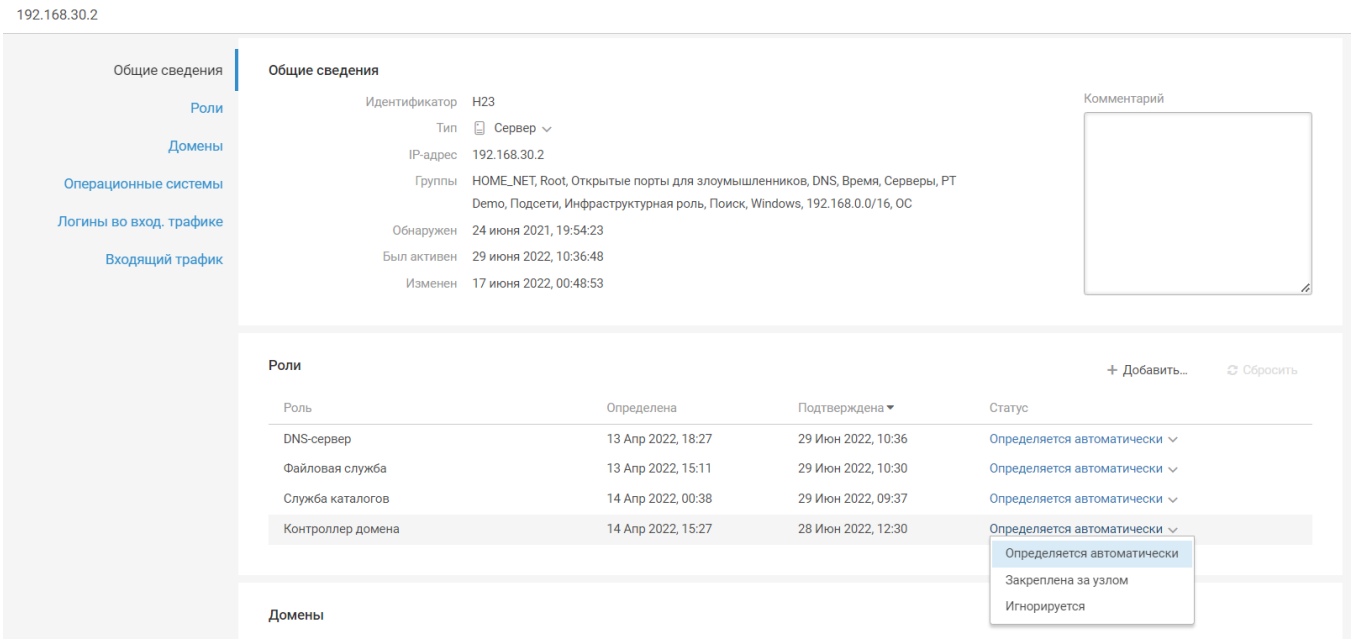

Рисунок 12. Профиль сетевого узла

7. Определение учетных данных пользователей

Проблема: IT-персоналу необходимо контролировать соблюдение парольной политики. Не во всех компаниях это можно организовать стандартными средствами администрирования Windows. Во-первых, не везде используется Windows, во-вторых, пользователи могут воспользоваться собственными узлами для подключения к корпоративным сервисам. Кроме того, необходимо контролировать нецелевое использование сервисов в инфраструктуре. Например, сетевой узел не имеет доступа к сервису, но по какой-то причине пытается использовать учетные данные для входа.

Решение: PT NAD анализирует копию сетевого трафика и за счет технологии DPI обнаруживает передачу учетных данных, объединяет их с источником и сохраняет в профиле сетевого узла. Это дает возможность быстро понять, какой сетевой узел пытается подключиться к сервису, какие учетные данные использует, соответствуют ли они парольной политике.

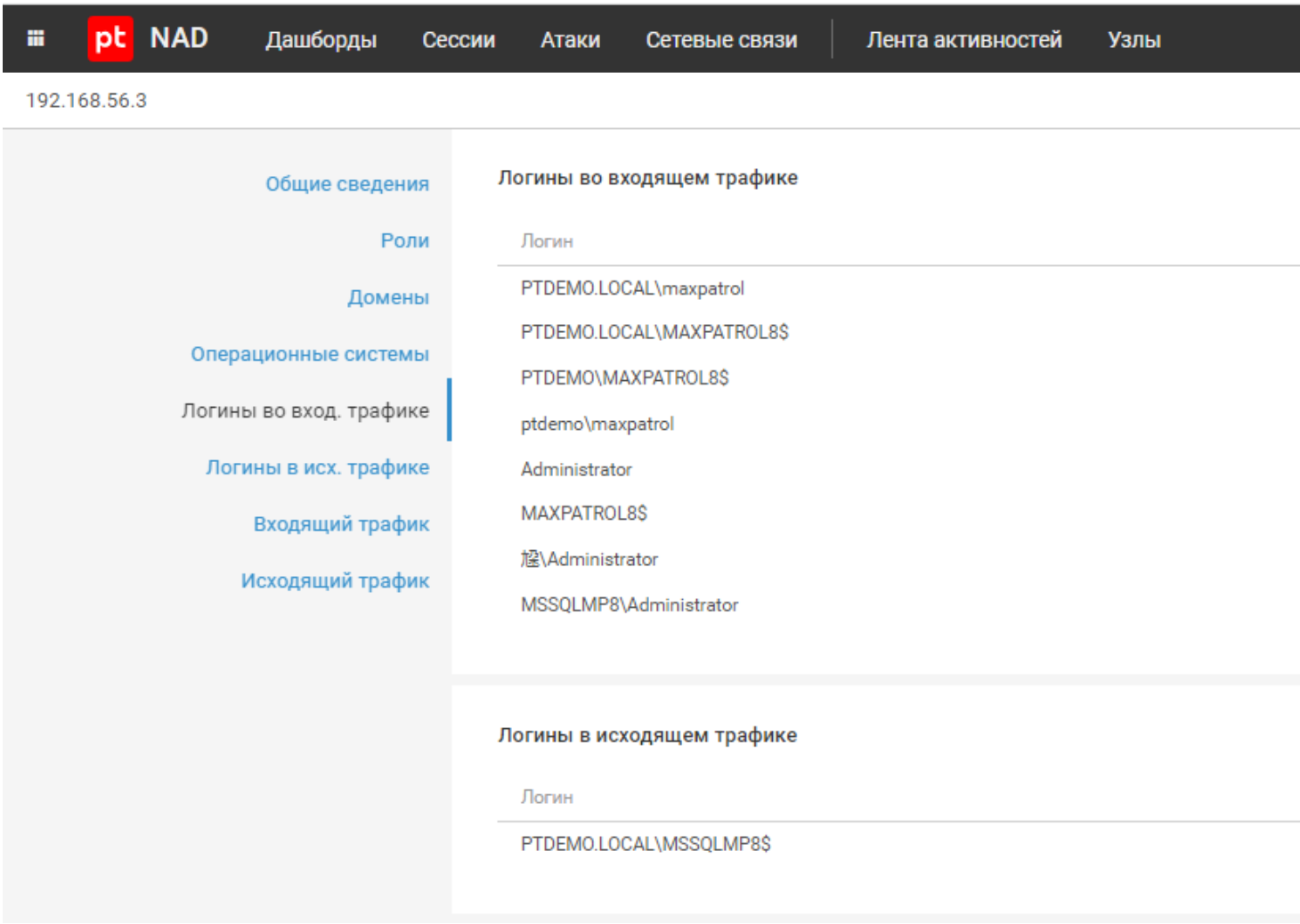

Рисунок 13. Учетные данные, обнаруженные в трафике

8. Обнаружение средств удаленного администрирования

Проблема: Несоблюдение корпоративной политики и использование сотрудниками собственных устройств для подключения к рабочим станциям от имени администратора — проблема IT-отдела. Отсутствуют системы контроля, невозможно определить, какие устройства используют средства удаленного администрирования. В компании есть корпоративный стандарт, согласно которому средствами удаленного администрирования должен пользоваться ограниченный круг лиц без подключения сторонних средств удаленного администрирования. IT-специалисты должны обнаруживать нежелательное использование такого ПО.

Решение: PT NAD определяет ПО, которое предназначено для удаленного администрирования систем. Например, AnyDesk, TeamViewer, RemoteAdmin, Ammyy Admin и другие.

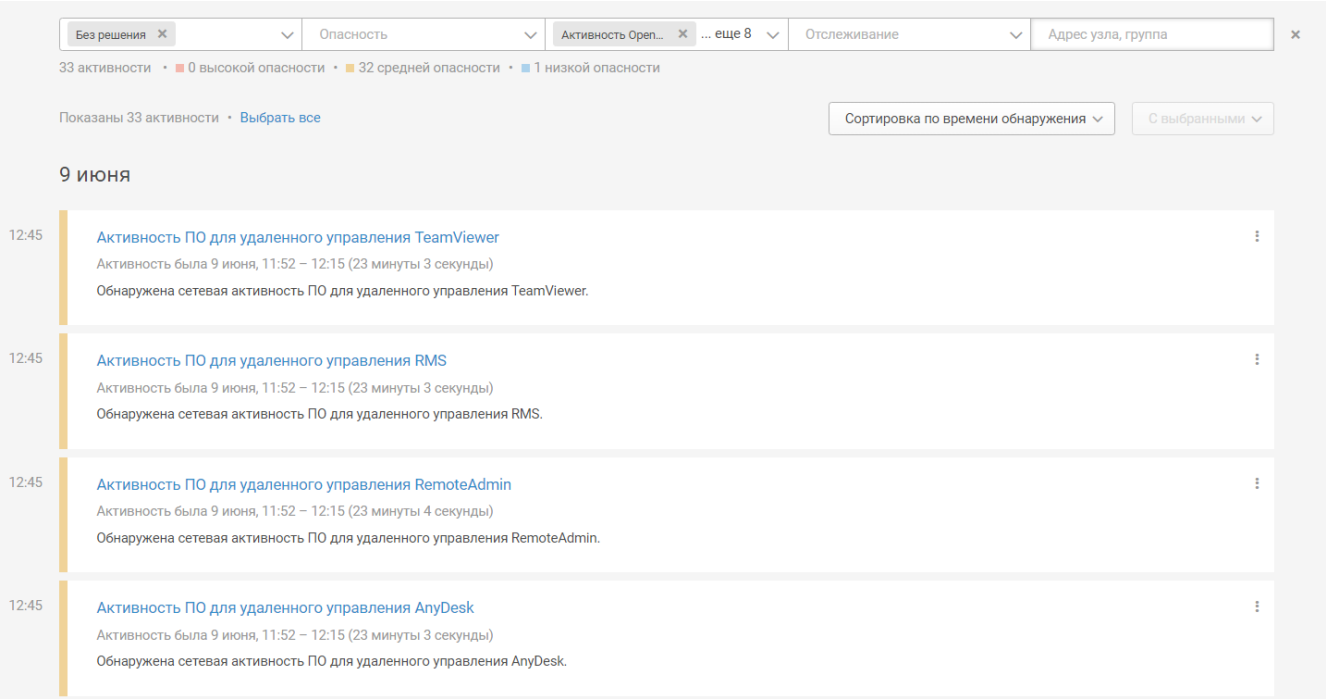

Рисунок 14. Обнаружение средств удаленного администрирования

Нецелевое использование средств удаленного администрирования свидетельствует о неправильной конфигурации сетевых узлов, что, в свою очередь, требует проведения работ со стороны IT-подразделения.

9. Обнаружение использования сторонних сервисов

Проблема: в инфраструктуре установлено большое количество программного обеспечения. Часто пользователи использует собственные домашние компьютеры для подключения к рабочему месту, устанавливают дополнительное ПО, администраторы временно перенастраивают софт и забывают об этом. Необходим механизм или инструмент, который покажет, какие сервисы и ПО используются на сетевых узлах, а главное — какие сетевые узлы подключаются к внутренним активам с использованием некорпоративного программного обеспечения.

Решение: PT NAD контролирует сетевые подключения и может определить, у каких пользователей есть сторонние сервисы, например для подключения к некорпоративному VPN или proxy-серверам. В данной ситуации PT NAD позволяет избежать нарушения корпоративных IT-стандартов и предотвратить инциденты ИБ.

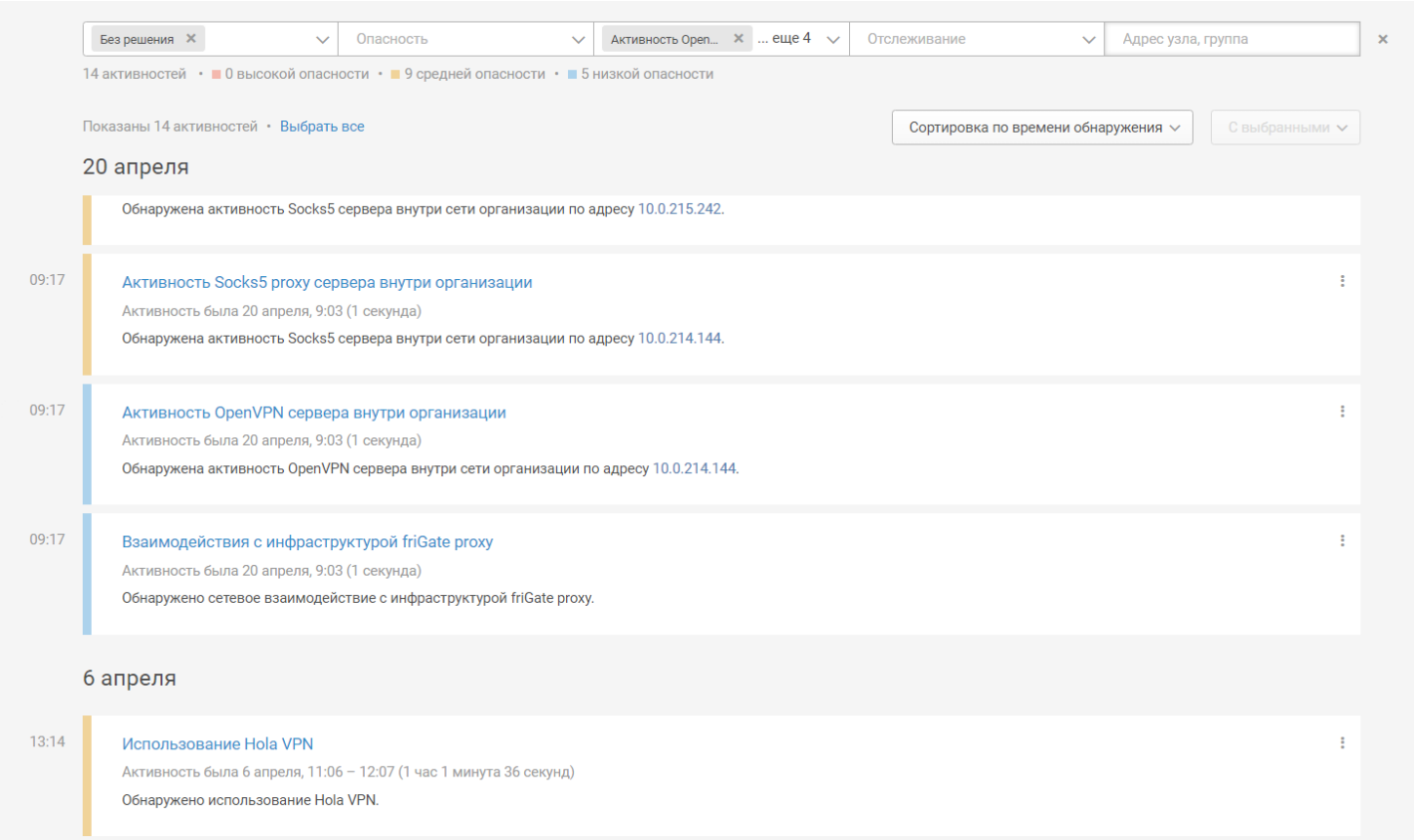

Рисунок 15. Обнаружение сторонних сервисов