udv|group

Что нового?

UDV NTA 1.1

2025

ОГЛАВЛЕНИЕ

НОВЫЕ ВОЗМОЖНОСТИ

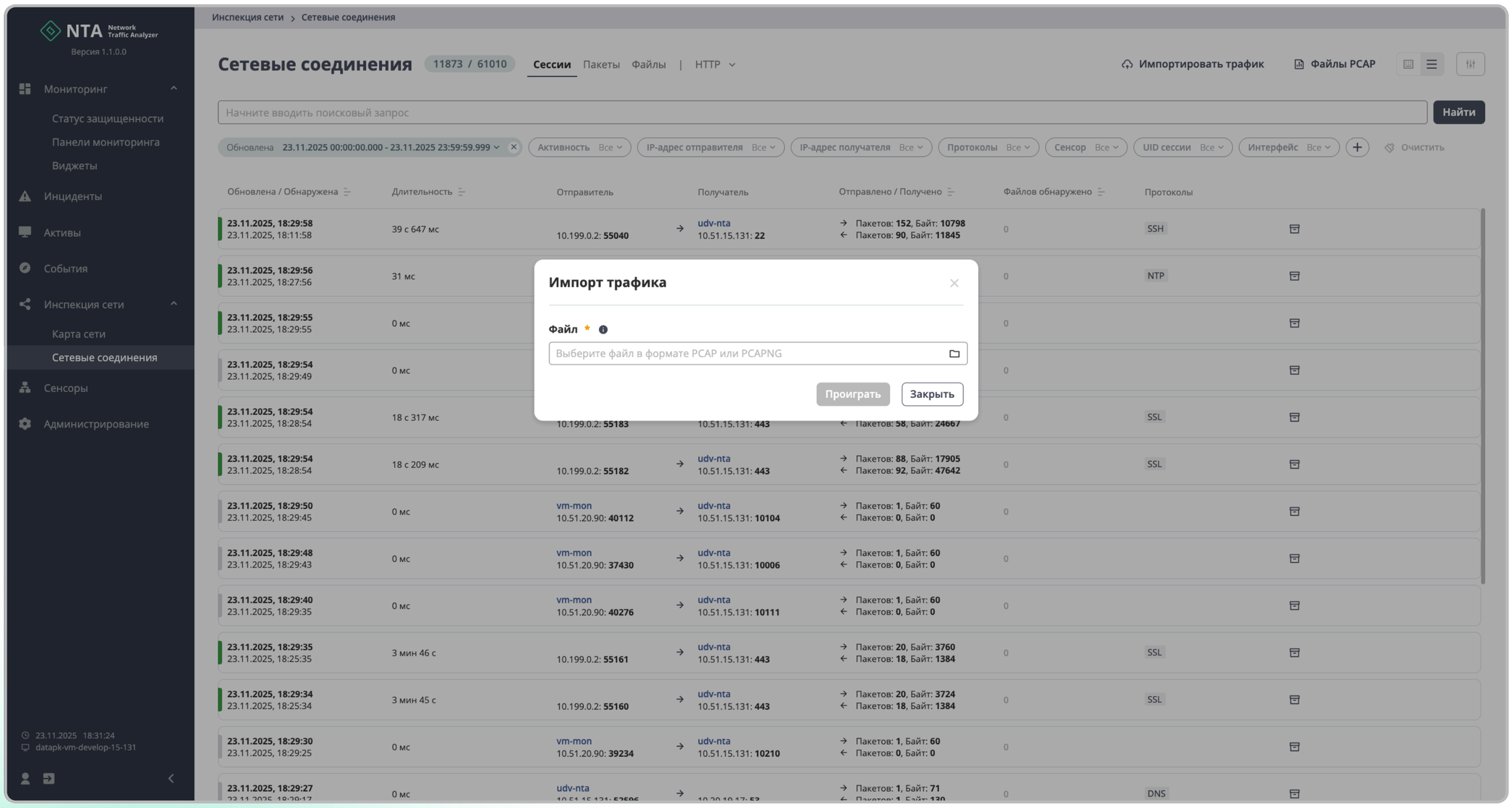
Экспертные знания при ретроспективном анализе сетевого трафика

В релизе UDV NTA 1.1 добавлена возможность импорта копии сетевого трафика для детального пост-анализа.

Ретроспективный анализ сырой копии сетевого трафика поможет аналитикам ИБ повторно проанализировать подозрительный трафик по обновленным пакетам экспертизы и выявить сложные угрозы, которые могли остаться незамеченными. Что в свою очередь позволит выявить и локализовать закрепившегося в инфраструктуре злоумышленника и снизить риск нанесения ущерба.

Также новая функциональность позволяет снизить затраты на приобретение дополнительных сенсоров для удаленных малоактивных сегментов. Теперь сетевой трафик можно накапливать и проводить точечный анализ по необходимости.

Специалистам SOC и консультантам по ИБ ретроспективный анализ поможет провести быстрый аудит сетевого трафика заказчика на наличие уязвимых протоколов, сетевых аномалий и злоумышленников в инфраструктуре без затрат на интеграцию.



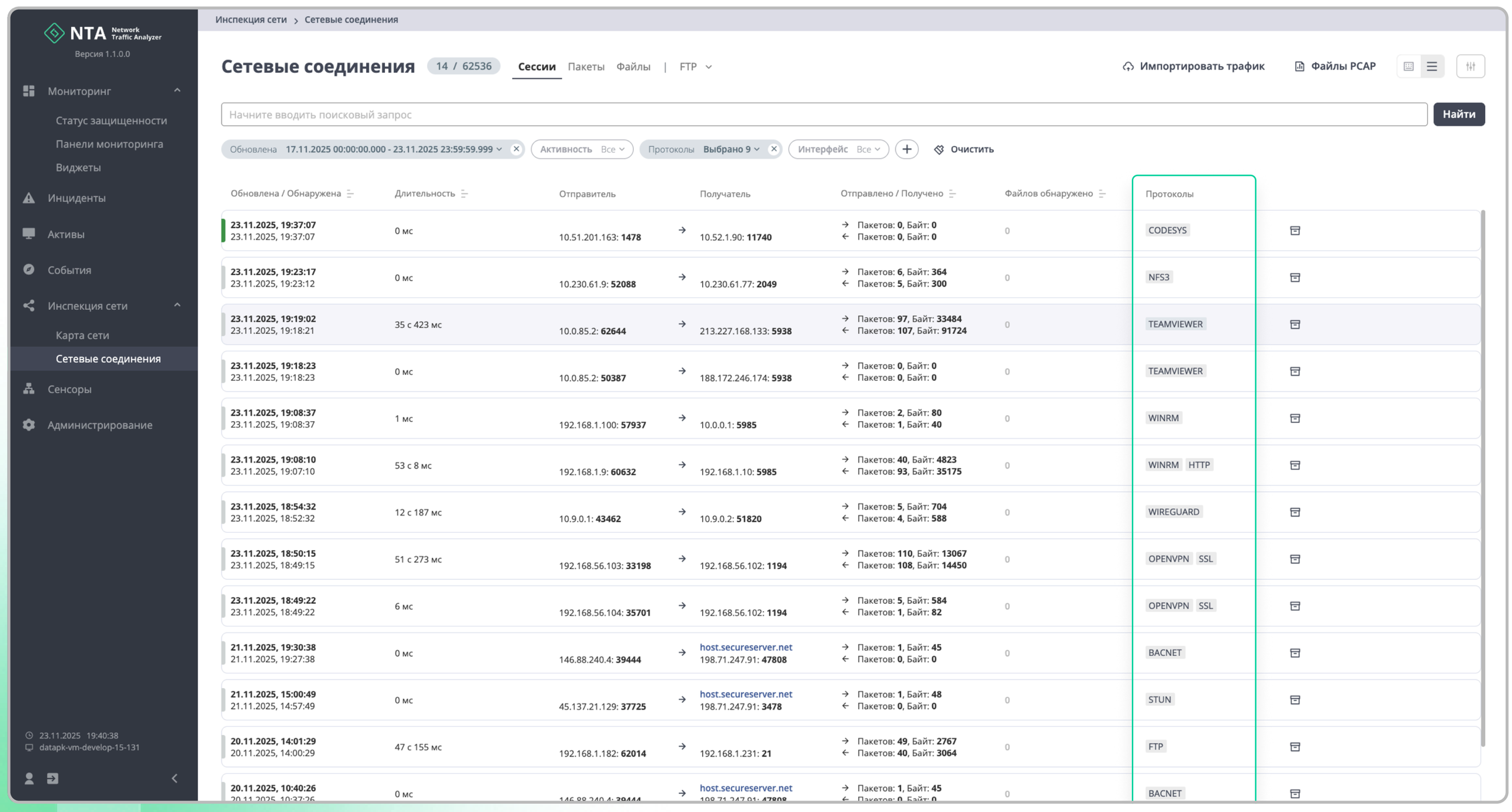
Импорт трафика

Расширена поддержка протоколов уровня приложений

Глубокий разбор сетевого трафика до уровня приложений помогает как аналитику ИБ, так и сетевому инженеру получить более широкую видимость действий в сети, что сокращает время на принятие решений при возникновении сетевых аномалий.

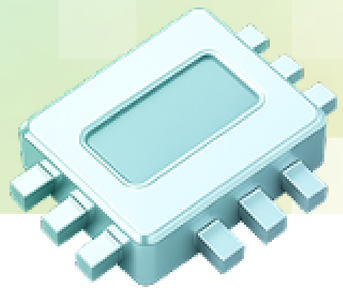
В новой версии добавлен разбор критичных для бизнеса протоколов приложений:

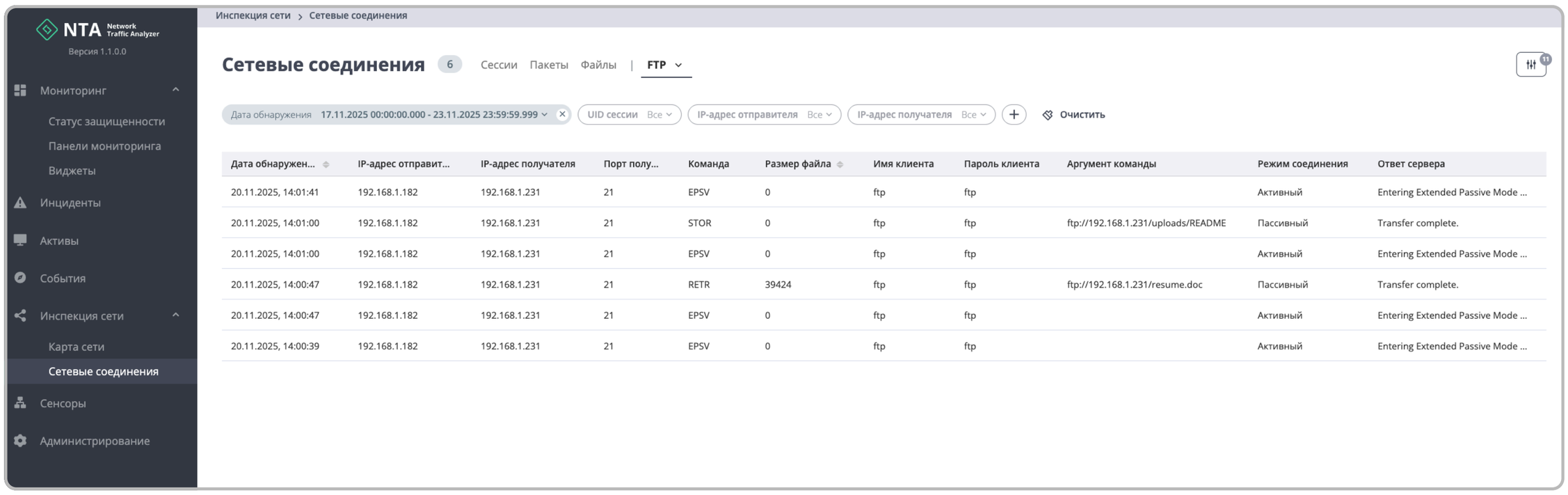
- VPN (OpenVPN, IPSec, WireGuard, Tailscale, STUN) — для выявления несанкционированного туннелирования, использования некорпоративных приложений и удалённых подключений к инфраструктуре;
- WinRM, TeamViewer, Radmin, Dameware, X11, KSC — протоколы удаленного управления помогут своевременно обратить внимание на излишне настроенный или нелегитимный доступ;
- BitTorrent — поддержка P2P позволяет выявлять горизонтальное перемещение внутри корпоративных сетей;
- NFS — для отслеживания перемещения файлов в Unix/Linux-системах;
- FTP — теперь доступен детализированный разбор: можно видеть не только передаваемые файлы, но и выполняемые действия, корректность ответов сервера и передачу учётных данных в открытом виде. Проверка соответствия политикам ИБ и выявление атак на протокол стали проще;
- CodeSYS, ProfiNet, BACNet, Omron, GE, BSAP, Vnet/IP — наличие в корпоративной сети промышленных протоколов укажет на некорректное сегментирование и потенциальный риск атаки через слабозащищённые подсистемы.



Отображение новых поддерживаемых протоколов в списке сетевых соединений

НОВЫЕ ВОЗМОЖНОСТИ





Дата обнаружен...	IP-адрес отправит...	IP-адрес получателя	Порт полу...	Команда	Размер файла	Имя клиента	Пароль клиента	Аргумент команды	Режим соединения	Ответ сервера
20.11.2025, 14:01:41	192.168.1.182	192.168.1.231	21	EPSV	0	ftp	ftp		Активный	Entering Extended Passive Mode ...
20.11.2025, 14:01:00	192.168.1.182	192.168.1.231	21	STOR	0	ftp	ftp	ftp://192.168.1.231/uploads/README	Пассивный	Transfer complete.
20.11.2025, 14:01:00	192.168.1.182	192.168.1.231	21	EPSV	0	ftp	ftp		Активный	Entering Extended Passive Mode ...
20.11.2025, 14:00:47	192.168.1.182	192.168.1.231	21	RETR	39424	ftp	ftp	ftp://192.168.1.231/resume.doc	Пассивный	Transfer complete.
20.11.2025, 14:00:47	192.168.1.182	192.168.1.231	21	EPSV	0	ftp	ftp		Активный	Entering Extended Passive Mode ...
20.11.2025, 14:00:39	192.168.1.182	192.168.1.231	21	EPSV	0	ftp	ftp		Активный	Entering Extended Passive Mode ...

Пример глубокого разбора протокола FTP

Поддержка пользовательских протоколов

UDV NTA — единственное на рынке РФ решение для анализа сетевого трафика с возможностью глубокой инспекции пакетов любого протокола уровня приложения.

Поддержка пользовательских протоколов позволит сетевым инженерам и экспертам по ИБ получить полную видимость сетевой активности, даже если UDV NTA не поддерживал протокол «из коробки».

Новая функциональность обеспечит более плотную интеграцию с используемой инфраструктурой и предоставит возможность быстро отследить сетевую активность устройств, использующих редкие или специализированные приложения, с целью выявления нарушения политики ИБ или вредоносной активности.

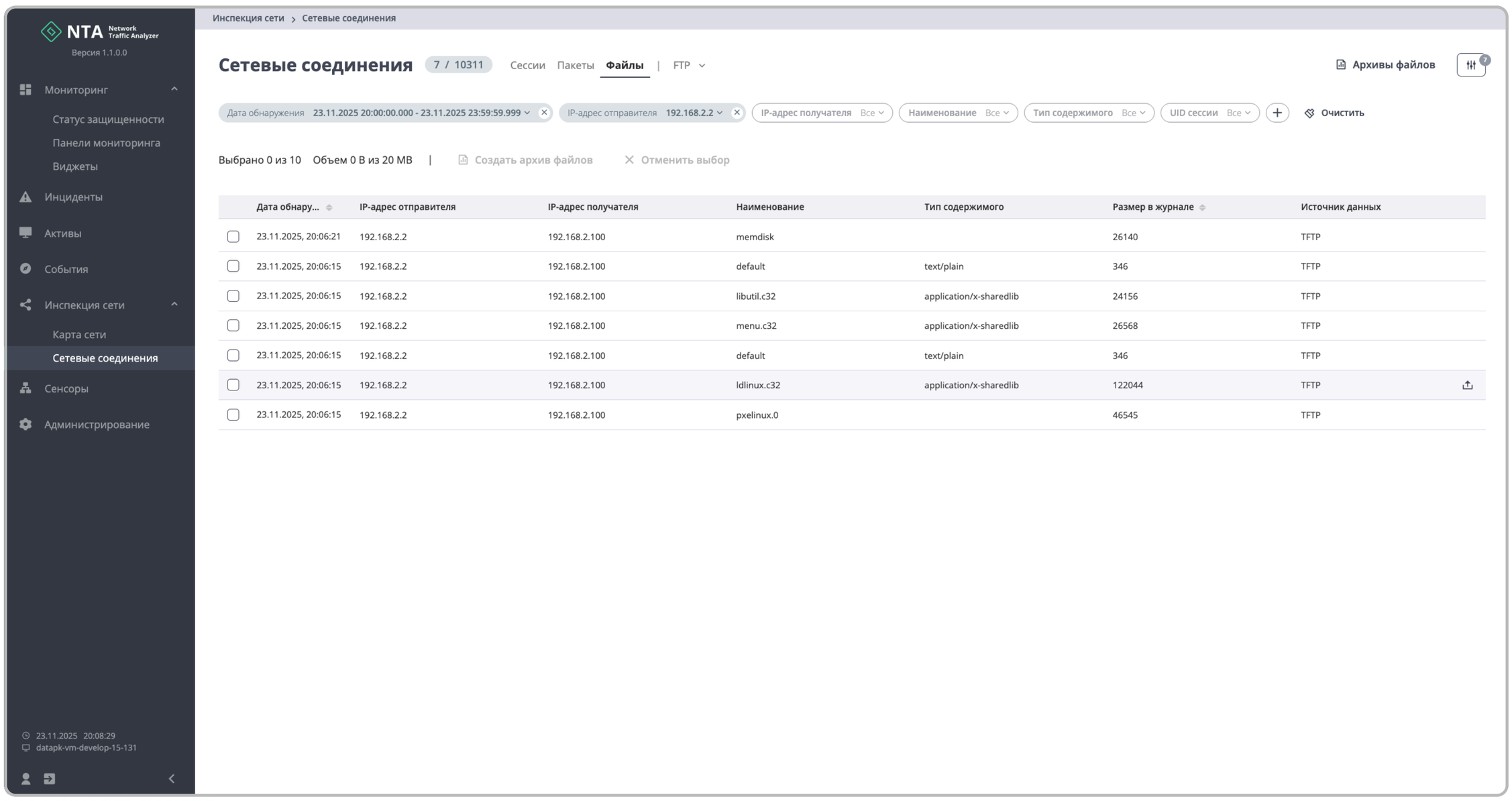
НОВЫЕ ВОЗМОЖНОСТИ

Больше файлов для анализа

В предыдущем релизе было добавлено обнаружение незащищенного протокола TFTP, который позволяет передавать файлы без необходимости аутентификации в открытом виде, в первую очередь для выявления техники атаки «Предзагрузка операционной системы по сети» (T1542.005 MITRE ATT&CK).

В UDV NTA 1.1 мы добавили разбор файлов по этому протоколу, что позволяет точно определить передавался ли файл с операционной системой, для однозначного подтверждения наличия инцидента ИБ.

Также для нового протокола NFS добавлен детальный анализ передаваемых файлов в Unix/Linux-средах, доля которых растет в связи с переходом на импортозамещенные операционные системы.



Инспекция файлов, переданных по протоколу TFTP

НОВЫЕ ВОЗМОЖНОСТИ

Расширение перечня выявляемых сетевых атак

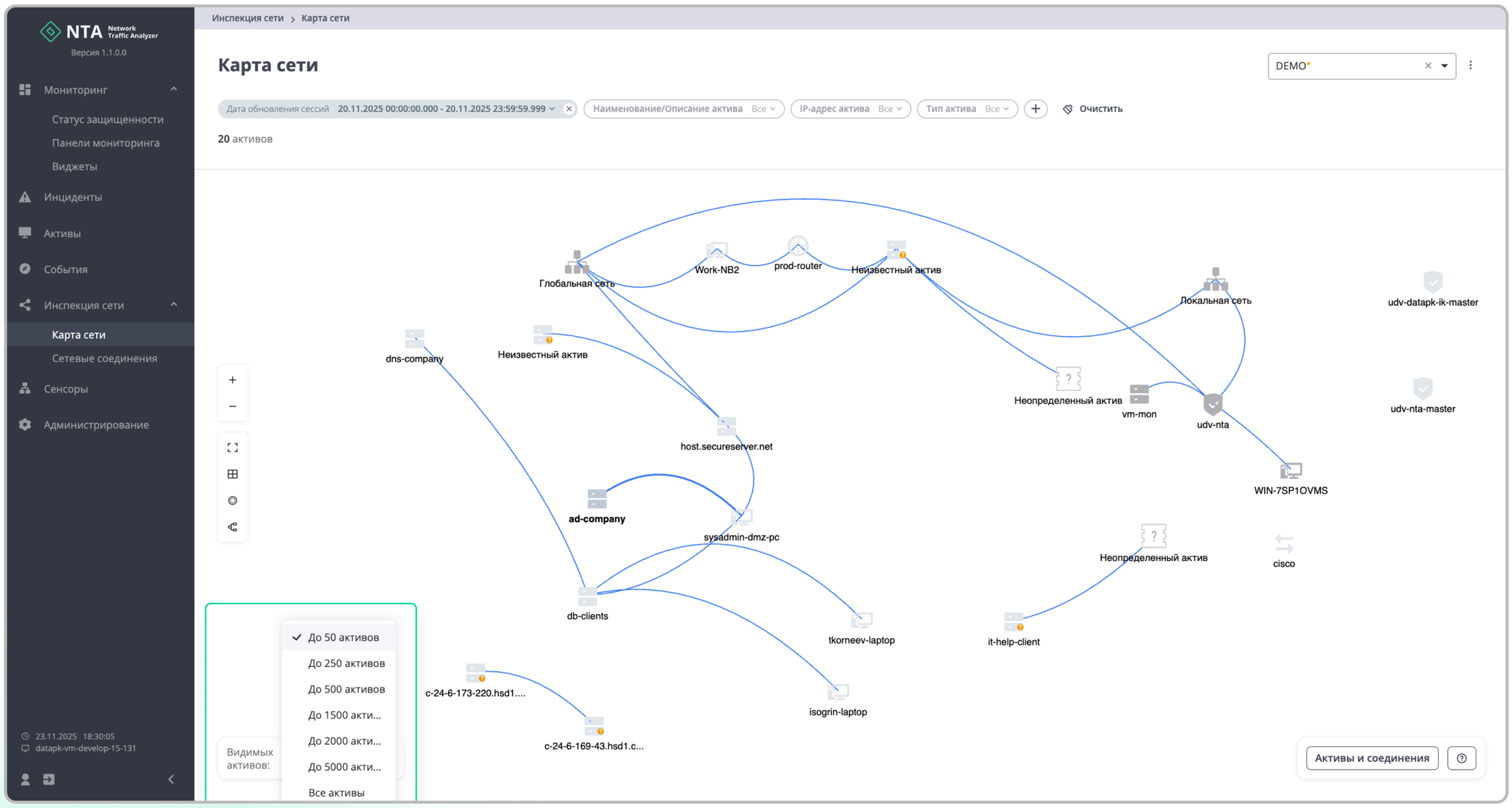
Глубокий разбор протокола передачи файлов FTP теперь позволяет фиксировать атаки типа bruteforce и оперативно сигнализировать об их наличии.

Также добавлена поддержка обнаружения атаки Zerologon — критической уязвимости в протоколе контроллера домена Windows, позволяющей злоумышленнику без аутентификации получить права администратора домена. Теперь продукт своевременно оповестит аналитика об эксплуатации этой уязвимости.

Улучшение пользовательского опыта при использовании карты сети

Карта сети получила обновлённый, более интуитивный интерфейс. Поиск узлов и выявление подозрительной активности теперь занимают меньше времени.

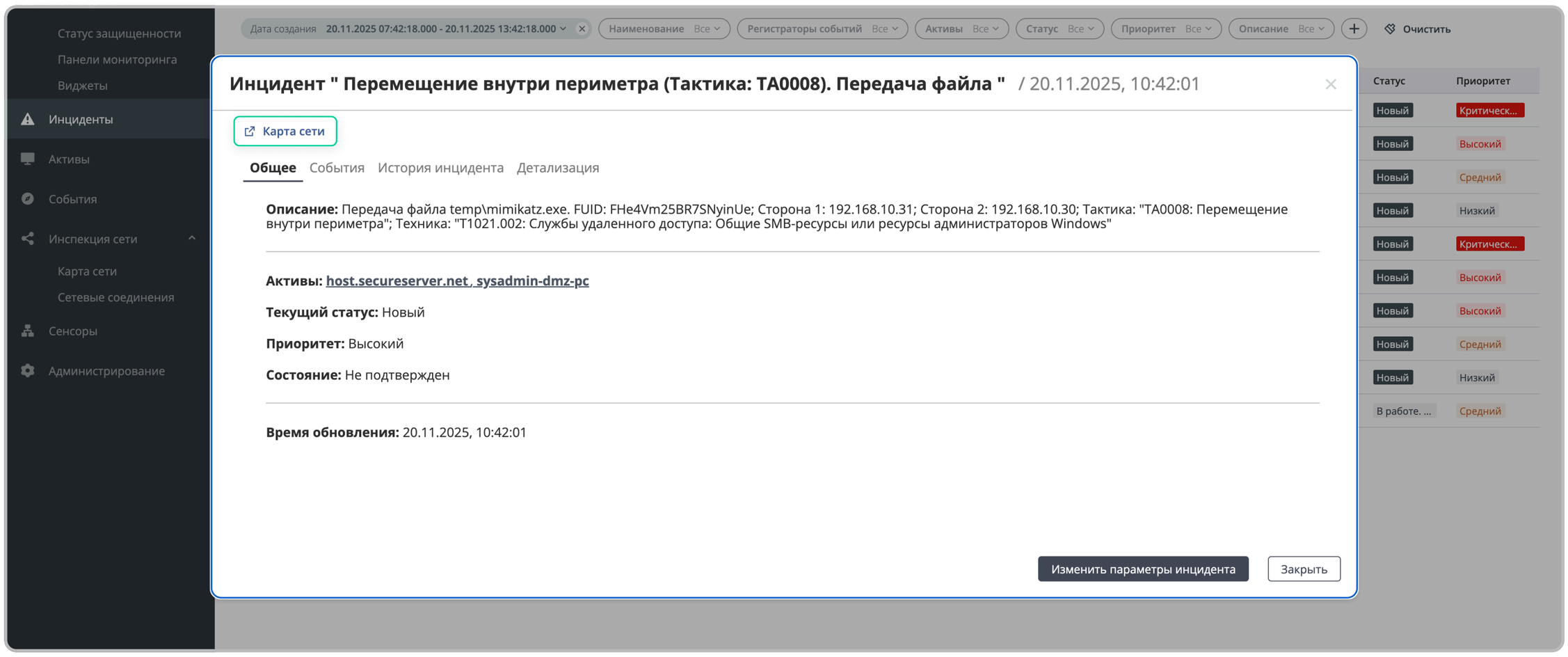
Для удобства работы с крупными сетями появилась возможность регулирования объёма отображаемых элементов.



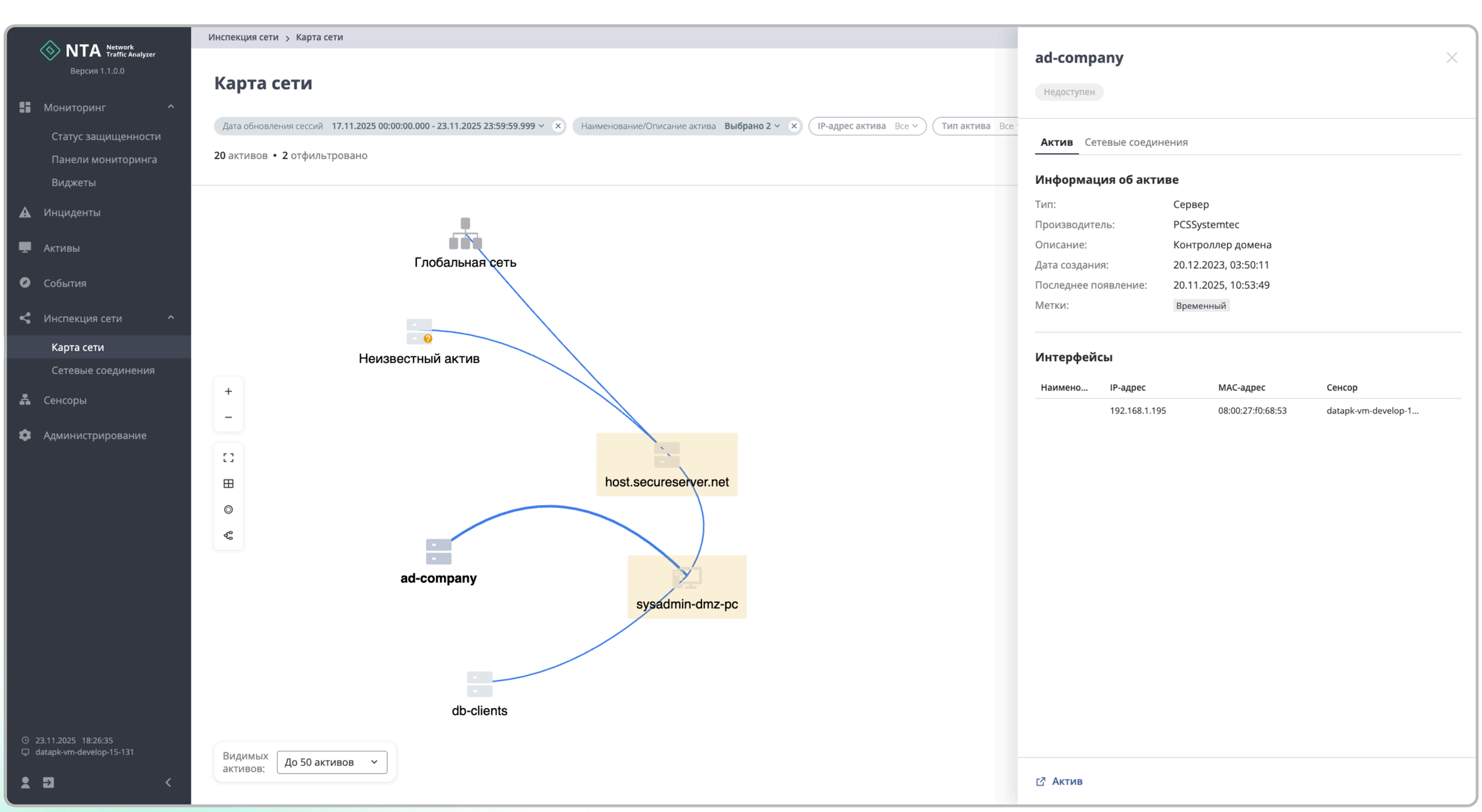
Выбор по количеству видимых на карте сети активов - для удобства анализа крупных сетей

НОВЫЕ ВОЗМОЖНОСТИ

Добавлен контекстный переход от инцидента к карте сети, что позволяет мгновенно видеть взаимодействия между узлами, вовлечёнными в инцидент, и быстрее локализовывать атаку.



Переход к карте сети с карточки инцидента

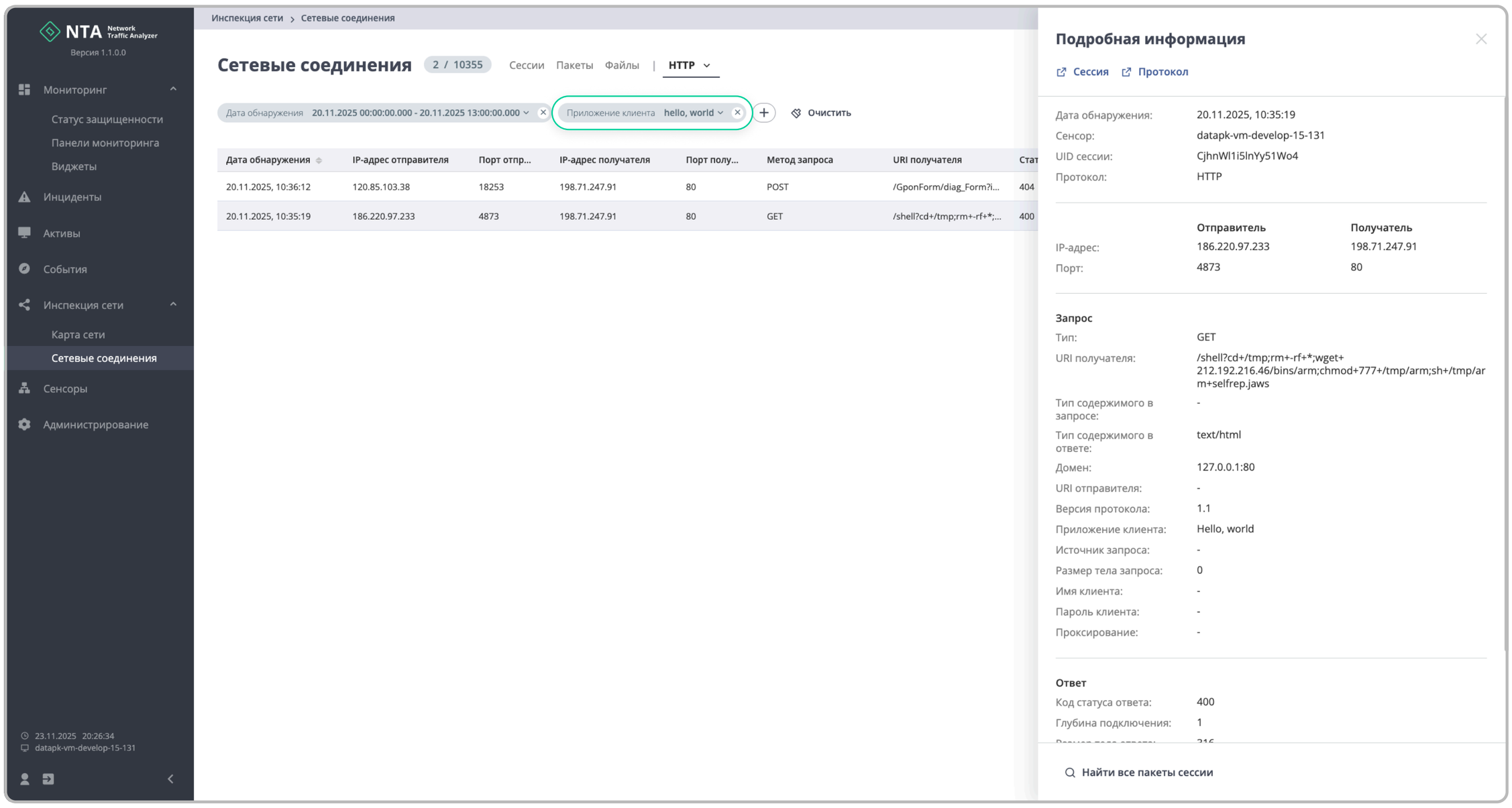


Фрагмент карты сети с отображением узлов, задействованных в инциденте.
В окне справа показана информация об активах, с которыми взаимодействует рассматриваемый узел, и о его сетевых соединениях.

НОВЫЕ ВОЗМОЖНОСТИ

Новые поля для поиска угроз

Возможность поиска по полям IP для извлеченных файлов и полю User-agent протокола HTTP позволит аналитикам ИБ быстрее находить связи между активностями сетевых узлов, а также получать дополнительную информацию (использование утилит сканирования, взлома, используемые приложения и операционная система).



Фильтрация по полю «Приложение клиента» для поиска потенциально зловредных утилит

Закажите пилотный проект или персональную демонстрацию наших решений

Контакты
commercial@udv.group
8-800-511-65-51

Сайт
udv.group

Телеграм
@udv_group

Адрес
620100, г. Екатеринбург,
ул. Сибирский тракт, 12,
строение 7, этаж 4 udv.group

udv|group