ViPNet TIAS 3.7.
Что нового в версии?

Светлана Старовойт
менеджер продуктов

О чем этот вебинар?

План вебинара

1. О чем это вообще? В двух словах о решении ViPNet TDR.
2. Что уже умеет ViPNet TIAS? Краткий обзор ключевых возможностей предыдущих релизов ViPNet TIAS.
3. Что нового будет в ViPNet TIAS 3.7? Новые источники событий и дополнительного контекста.
4. А что в других компонентах? Ключевые фичи последних релизов IDS NS и IDS MC.
5. А что дальше? Планы развития.

О решении ViPNet TDR

Состав решения ViPNet TDR

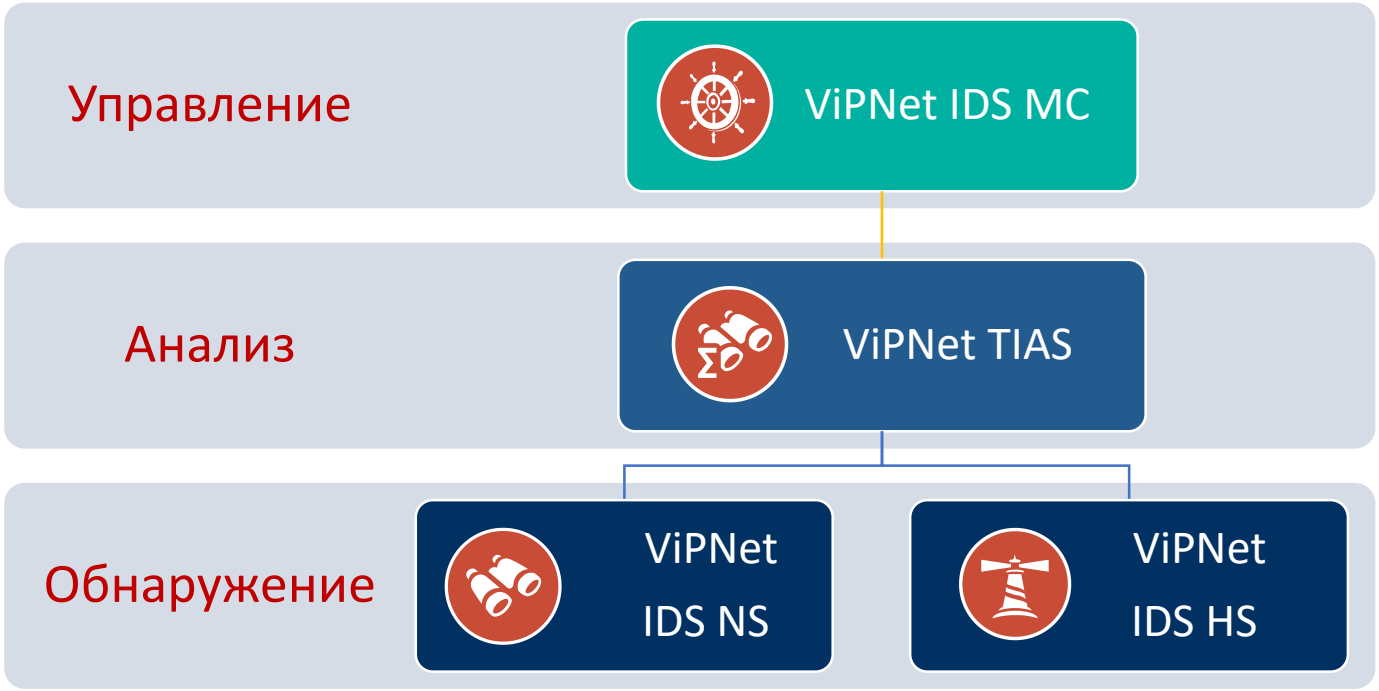
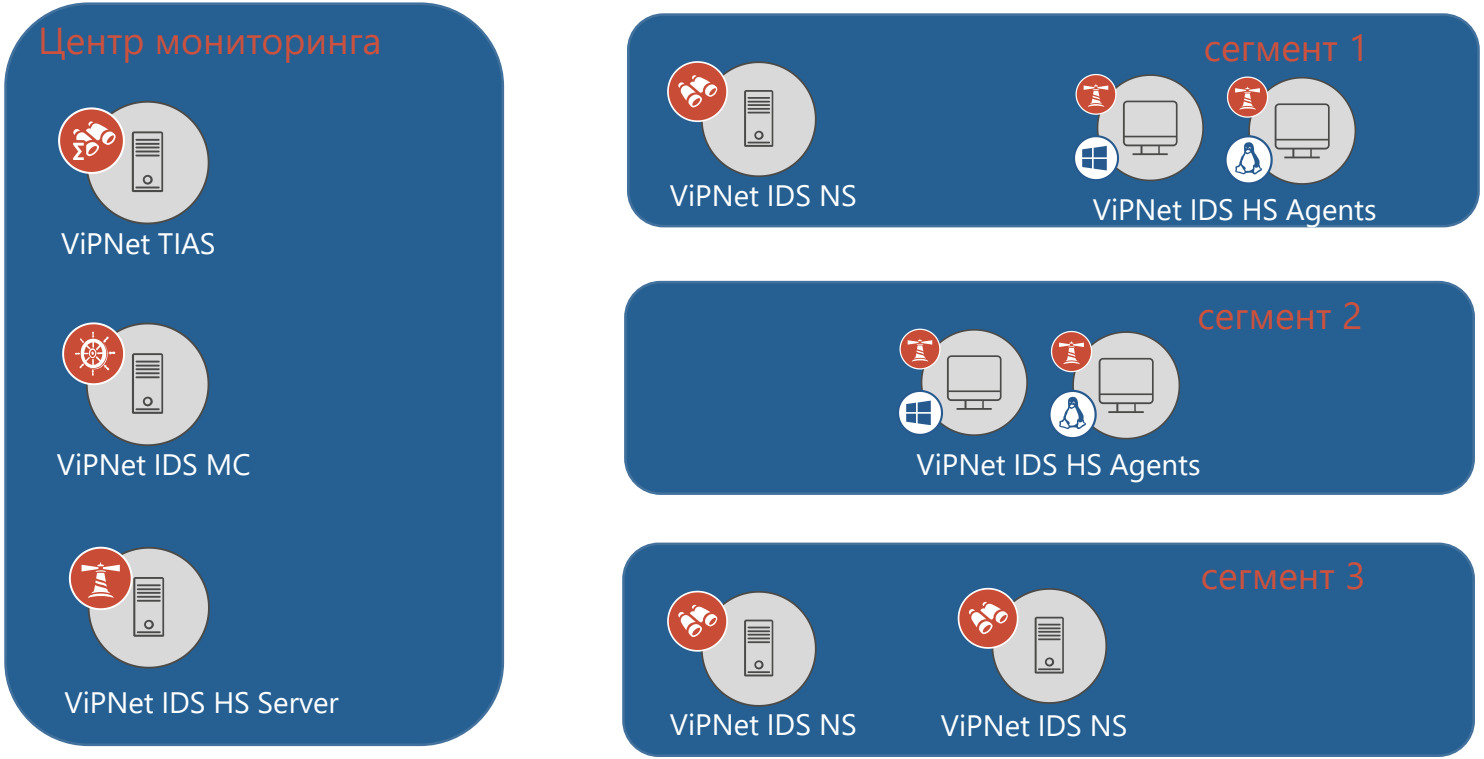


Схема развертывания



Назначение компонентов решения ViPNet TDR

ViPNet IDS MC

- Управлять инфраструктурой сенсоров
- Осуществлять мониторинг состояния сенсоров

ViPNet TIAS

- Анализировать события ИБ от сетевых и хостовых сенсоров и выявлять инциденты ИБ

ViPNet IDS NS

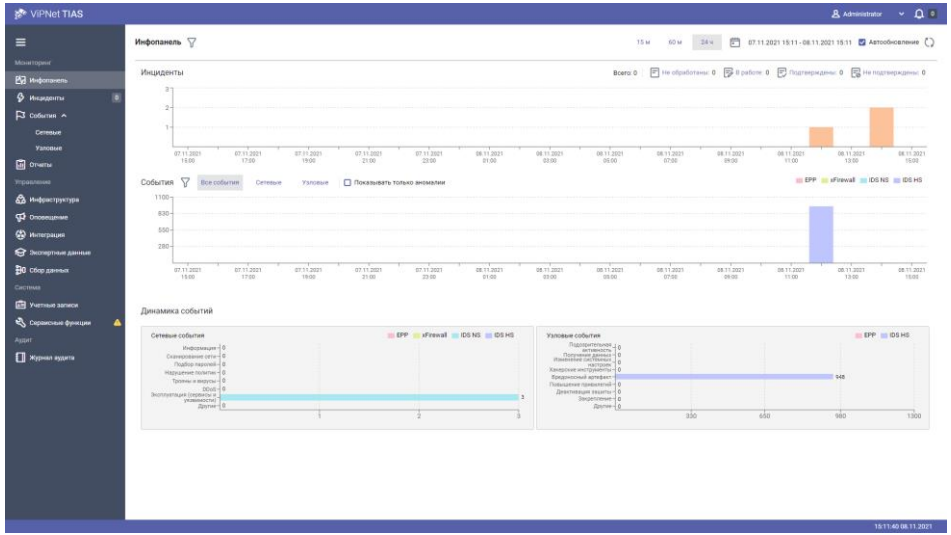
- Выявлять события, связанные с ИБ в сетевом трафике

ViPNet IDS HS

- Выявлять события ИБ и аномалии поведения на конечных узлах

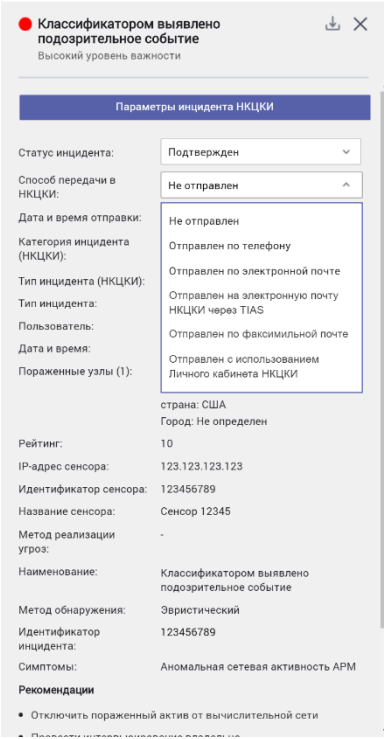
Назначение ViPNet TIAS

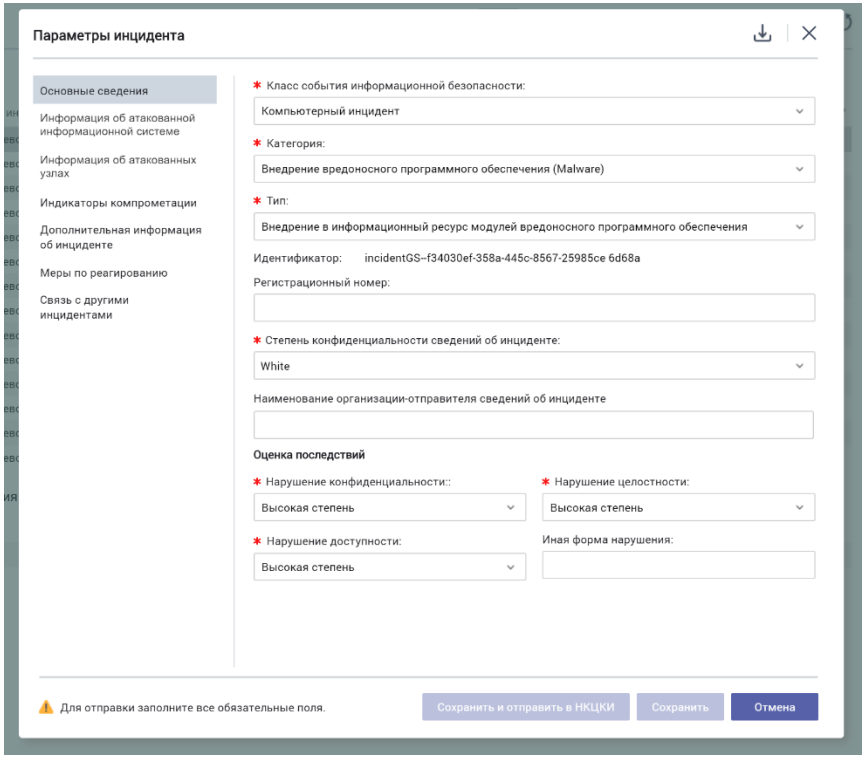
- ✓ анализировать события от сенсоров ViPNet IDS;
- ✓ выявлять инциденты;
- ✓ оповещать об инцидентах;
- ✓ проводить расследования;
- ✓ давать рекомендации;
- ✓ формировать отчеты.



Что уже умеет ViPNet TIAS

Передача инцидентов в НКЦКИ (v 3.5)





Мультиарендный режим работы v 3.6

Роли ViPNet TIAS:

- Системный администратор;
- Администратор TIAS;
- Аудитор;
- Администратор организации;
- Оператор.

Доступ к объектам инфраструктуры ViPNet TIAS:

- для пользователя с ролью администратора организации область действия может быть ограничена одной или несколькими организациями.
- для пользователя с ролью оператора область действия может быть ограничена уровнем сети одной или нескольких организаций.

Иерархия TIAS (v 3.6)

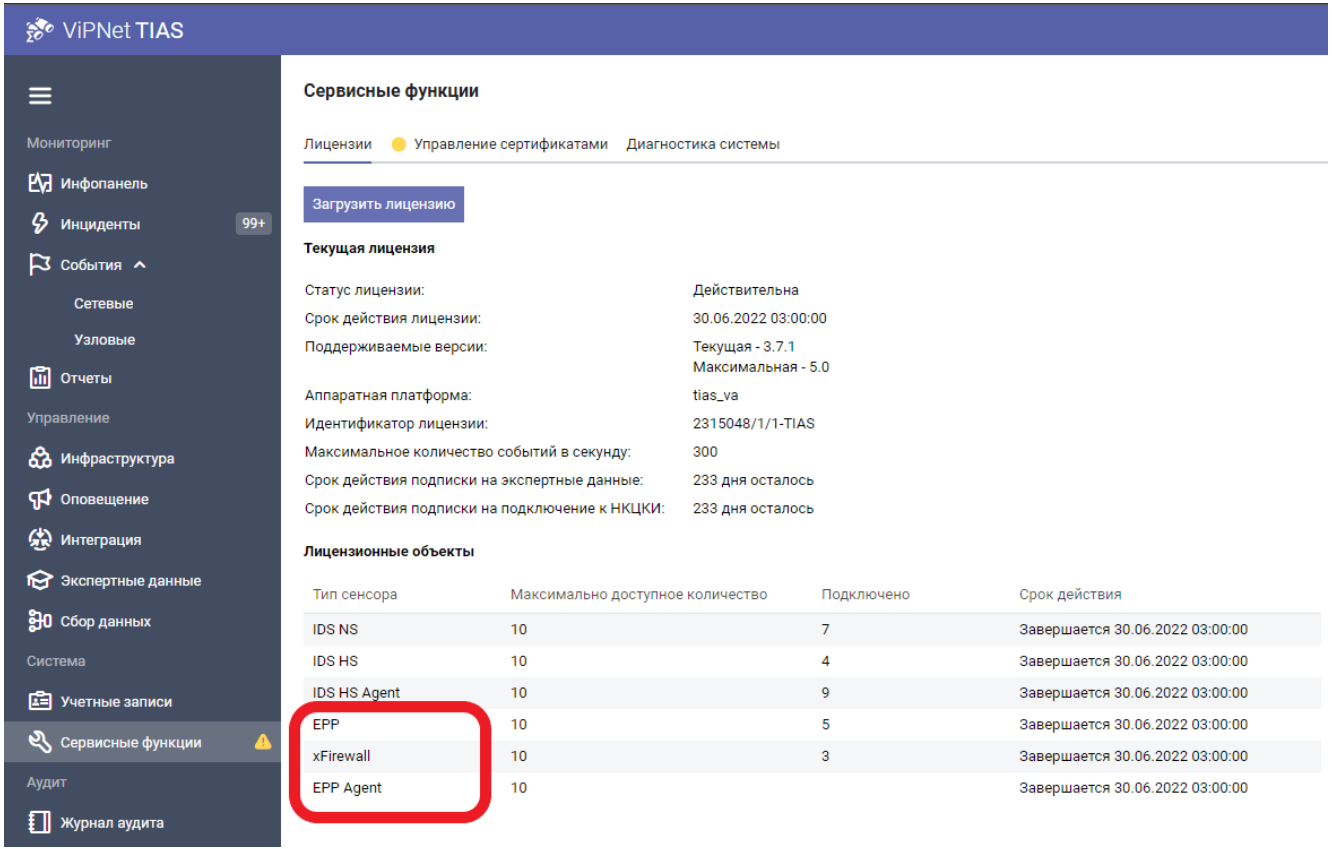
infotecs

ViPNet TIAS 3.7

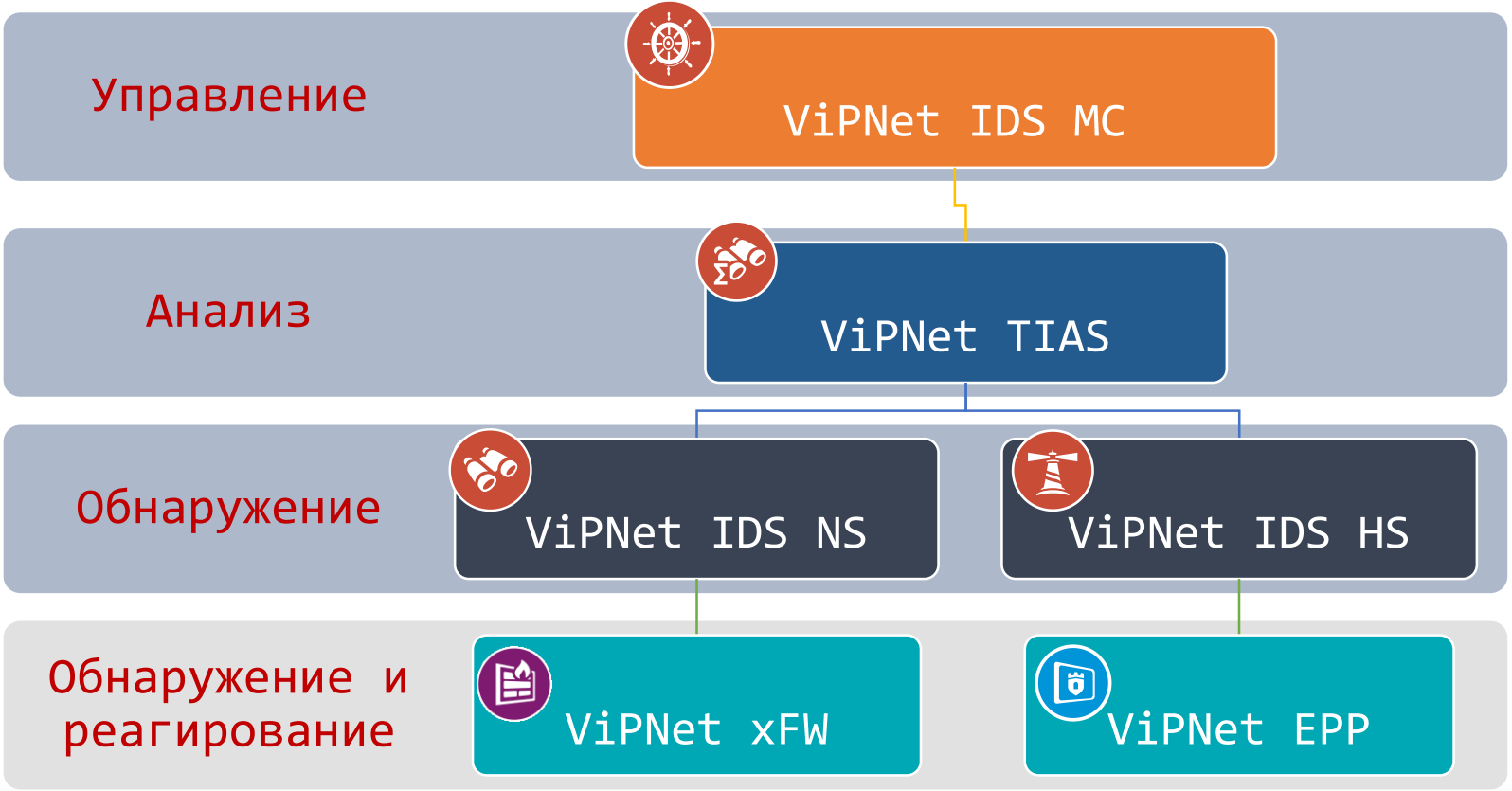
Новое в версии 3.7

1. ViPNet xFW в качестве источника событий;
2. ViPNet EPP в качестве источника событий;
3. Обогащение информации и выявление инцидентов с использованием данных от сканеров уязвимостей;
4. Обогащение информации и выявление инцидентов с использованием данных IoC;
5. Поиск инцидентов по IP-адресу источника/получателя;
6. Использование NTP-сервера для синхронизации времени;
7. Мониторинг состояния TIAS по SNMP;
8. Соответствие новым требованиям ФСБ к СОА класс В.

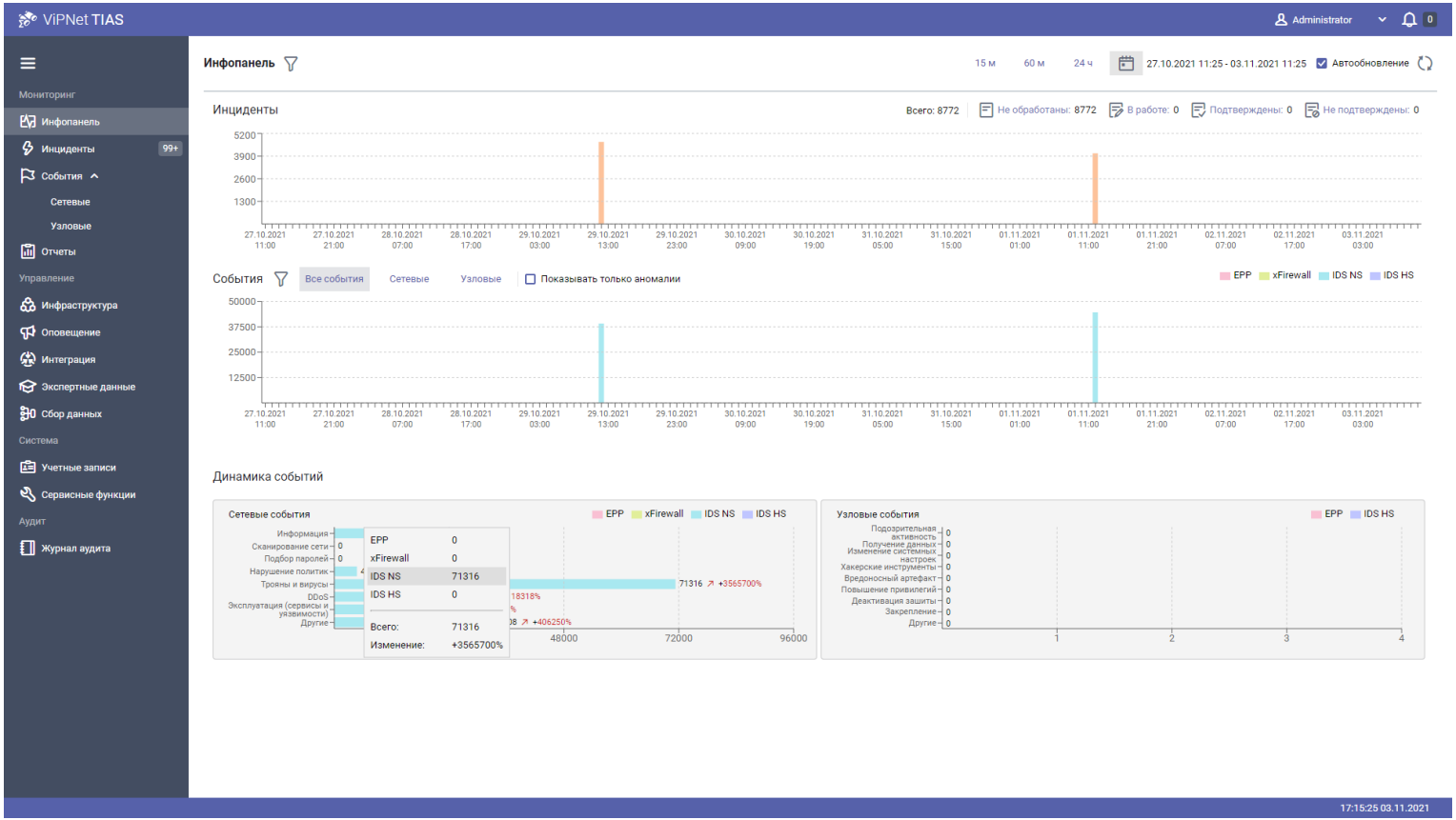
Новые источники событий



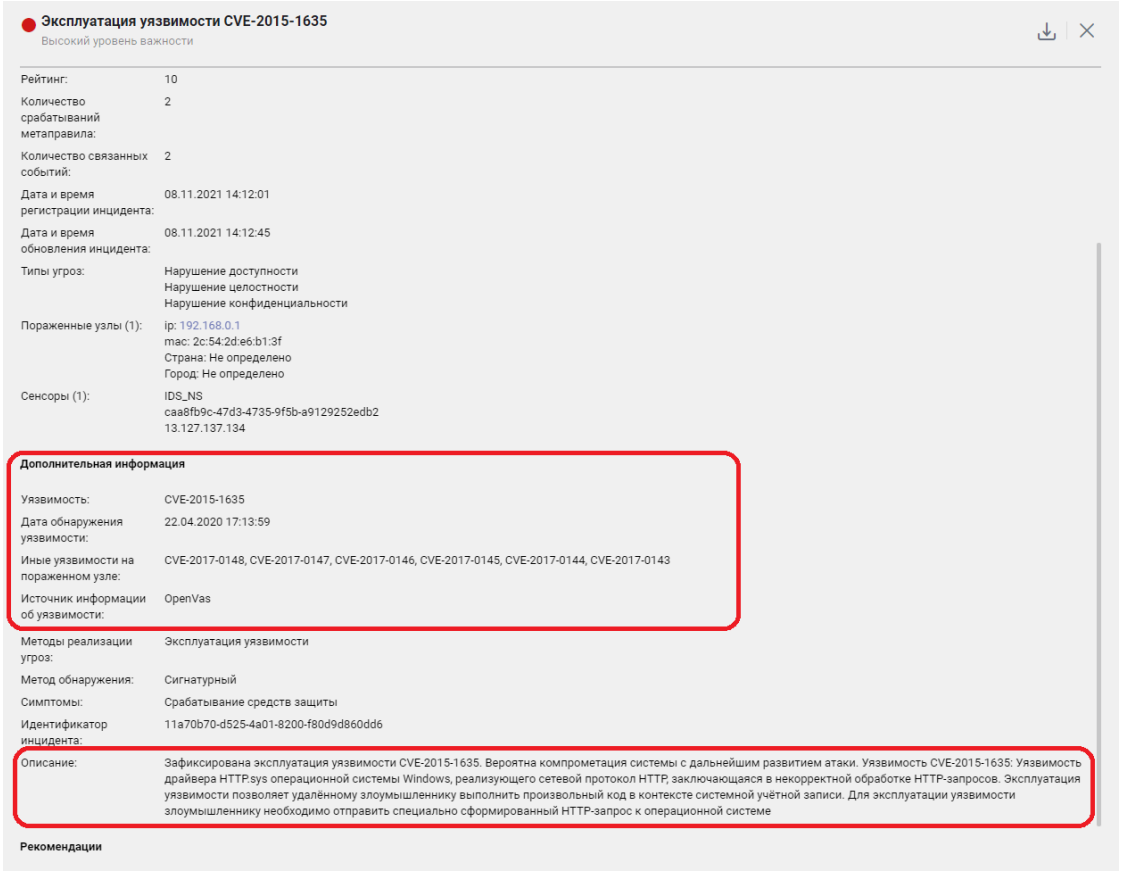
Состав решения ViPNet TDR



Фильтрация по типу источников



Данные от сканеров уязвимостей



Эксплуатация уязвимости CVE-2015-1635
Высокий уровень важности

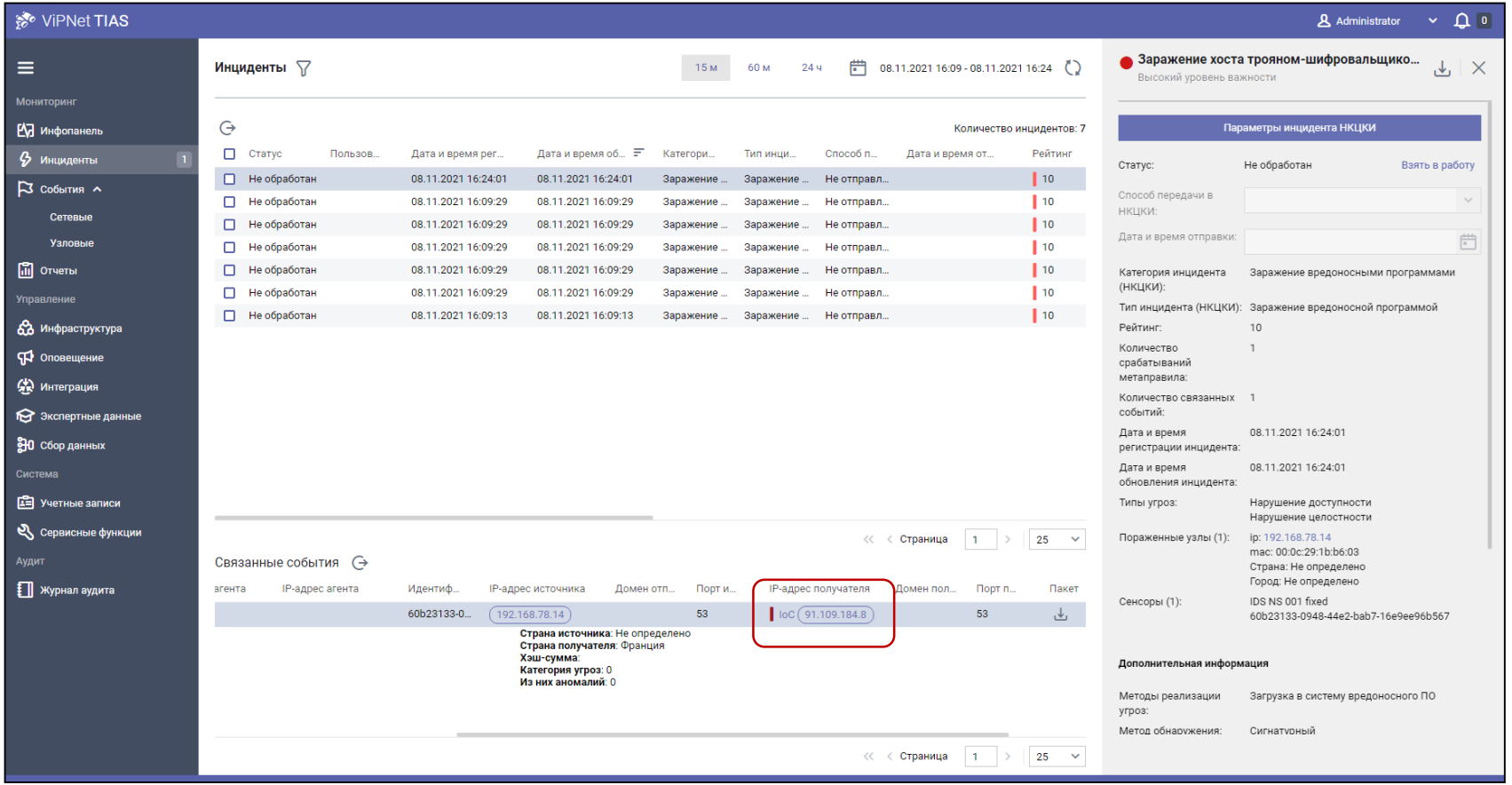
Рейтинг:	10
Количество срабатываний метаправила:	2
Количество связанных событий:	2
Дата и время регистрации инцидента:	08.11.2021 14:12:01
Дата и время обновления инцидента:	08.11.2021 14:12:45
Типы угроз:	Нарушение доступности Нарушение целостности Нарушение конфиденциальности
Пораженные узлы (1):	ip: 192.168.0.1 mac: 2c:54:2d:e6:b1:3f Страна: Не определено Город: Не определено
Сенсоры (1):	IDS_NS caa8fb9c-47d3-4735-9f5b-a9129252edb2 13.127.137.134

Дополнительная информация

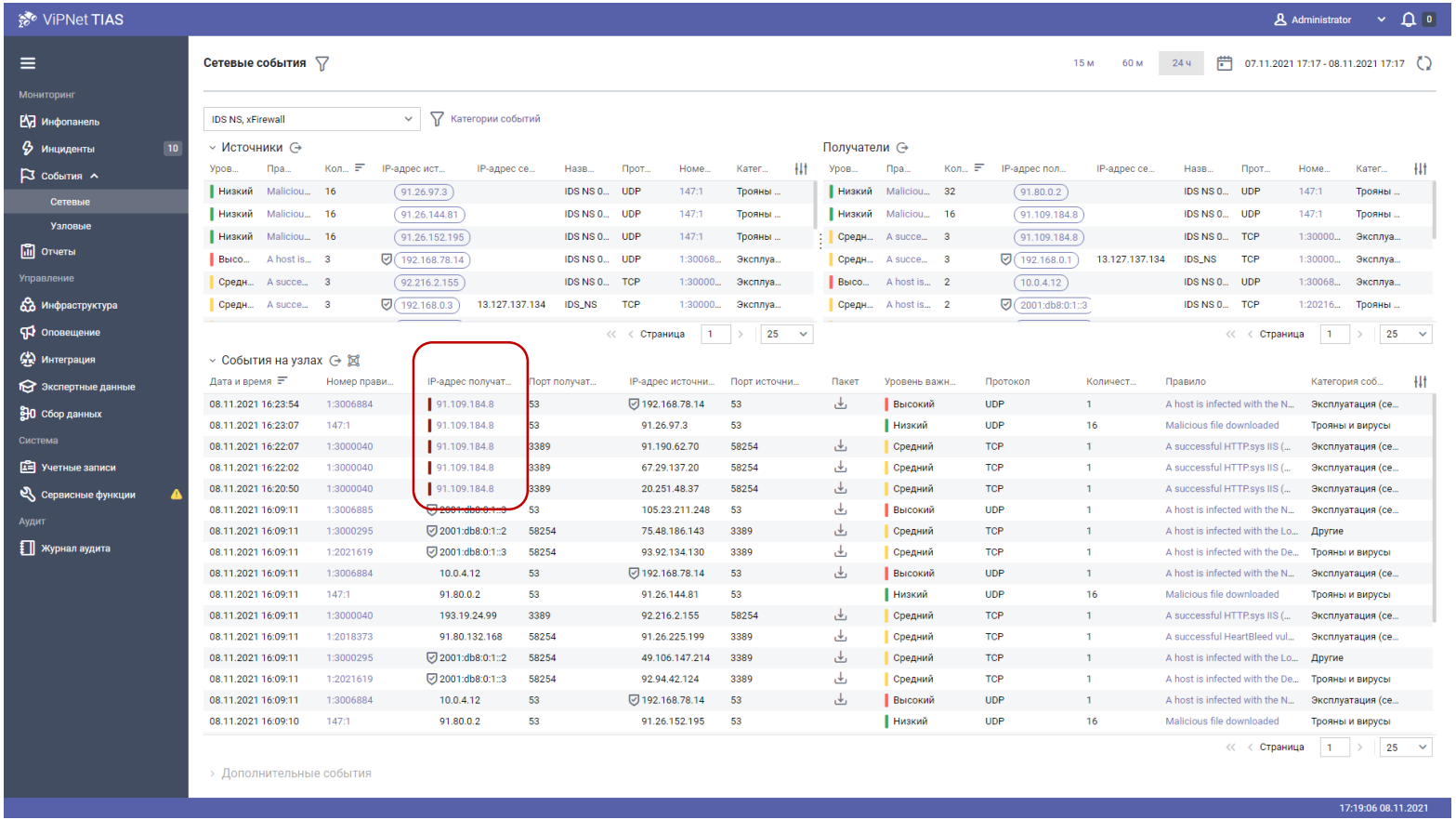
Уязвимость:	CVE-2015-1635
Дата обнаружения уязвимости:	22.04.2020 17:13:59
Иные уязвимости на пораженном узле:	CVE-2017-0148, CVE-2017-0147, CVE-2017-0146, CVE-2017-0145, CVE-2017-0144, CVE-2017-0143
Источник информации об уязвимости:	OpenVas
Методы реализации угроз:	Эксплуатация уязвимости
Метод обнаружения:	Сигнатурный
Симптомы:	Срабатывание средств защиты
Идентификатор инцидента:	11a70b70-d525-4a01-8200-f80d9d860dd6
Описание:	Зафиксирована эксплуатация уязвимости CVE-2015-1635. Вероятна компрометация системы с дальнейшим развитием атаки. Уязвимость CVE-2015-1635: Уязвимость драйвера HTTP.sys операционной системы Windows, реализующего сетевой протокол HTTP, заключающаяся в некорректной обработке HTTP-запросов. Эксплуатация уязвимости позволяет удалённому злоумышленнику выполнить произвольный код в контексте системной учётной записи. Для эксплуатации уязвимости злоумышленнику необходимо отправить специально сформированный HTTP-запрос к операционной системе

Рекомендации

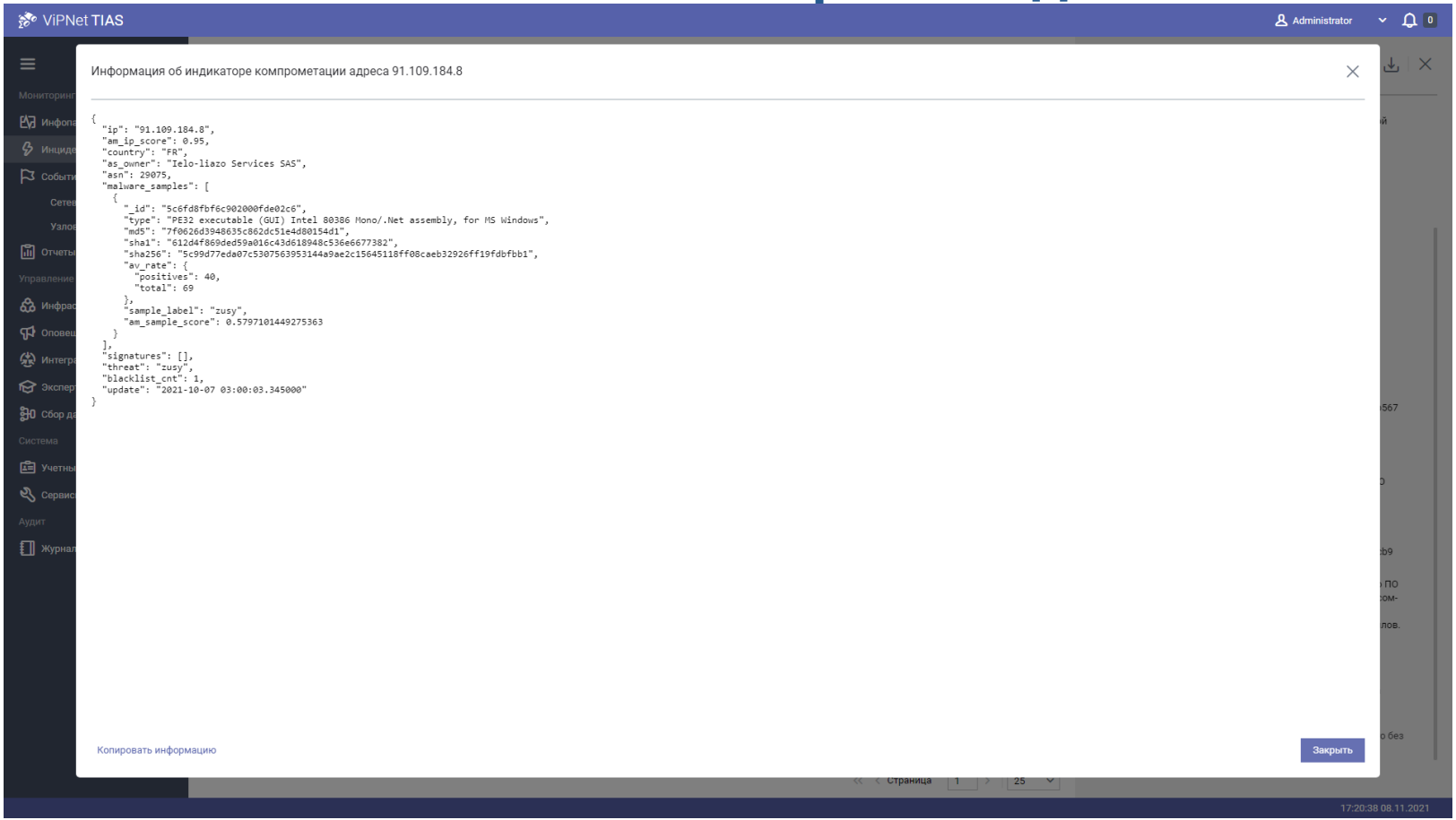
IoC в инциденте



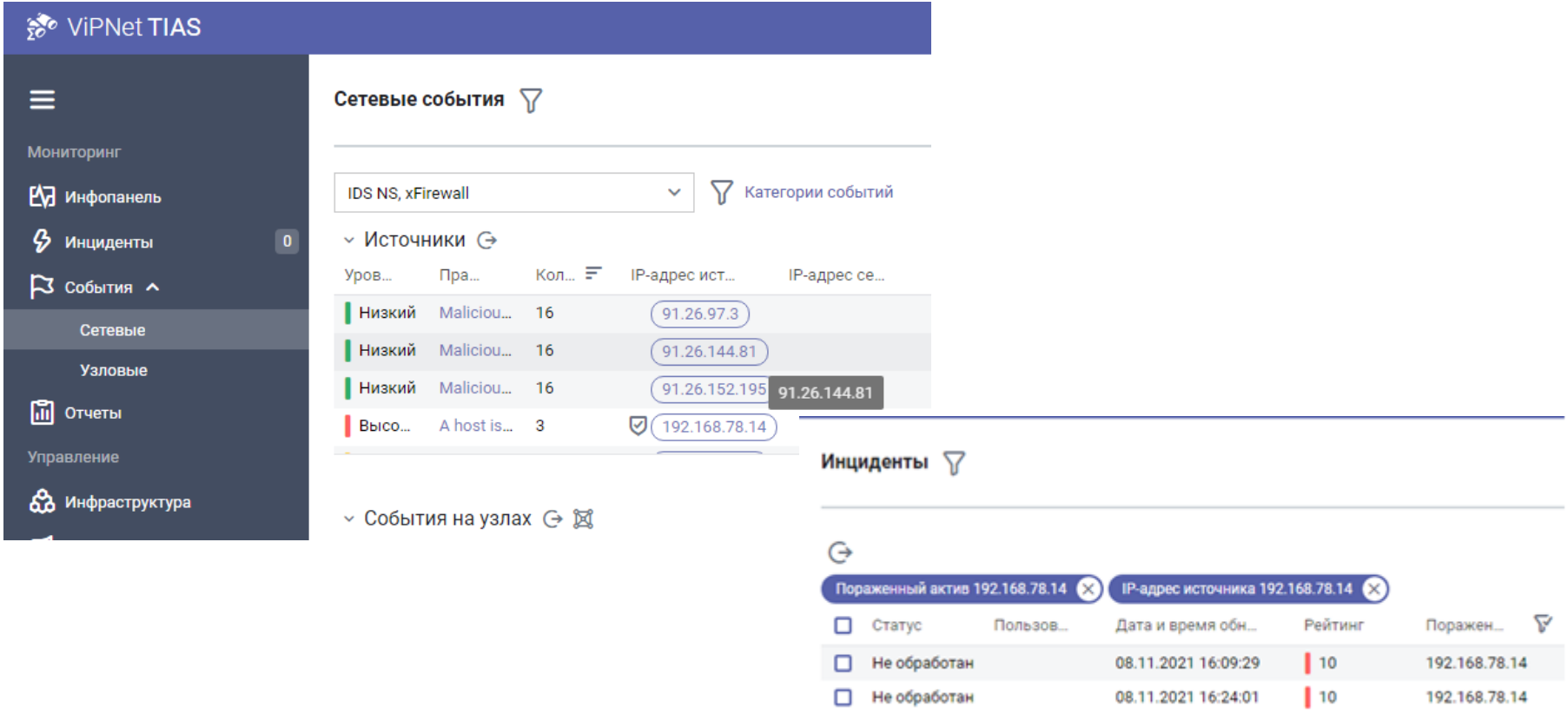
IoC в событиях



Описание IoC в экспертных данных



Поиск инцидентов по IP-адресу



Новое в других компонентах

ViPNet IDS NS v 3.7-3.8

- Синхронизация системного времени с ViPNet IDS MC ;
- Гарантированная доставка сообщений в TIAS;
- Исполнение ViPNet IDS NS 10000;
- Лицензирование исполнений ViPNet IDS NS VA;
- Увеличение производительности за счет технологии DPDK (Data Plane Development Kit);
- Запись сетевой сессии;
- 15 000 пользовательских правил.

ViPNet IDS MC v 1.7-1.8

- передача управления ViPNet IDS MC в ViPNet Prime;
- возможность отправки отчетов для биллинга в ViPNet Prime;
- управление иерархической структурой TIAS;
- расширен список поддерживаемых протоколов для доступа к серверу обновлений через прокси-сервер;
- передача значений HOME_NET адресов с IDS NS в TIAS;
- синхронизация системного времени сенсоров IDS NS со временем ViPNet IDS MC по протоколу NTP;
- Мониторинг состояния TIAS;
- Организация TLS с с двусторонней аутентификацией между сенсорами и TIAS.

Сертификация

Сертифицированные версии

СОА класса В

Система IDS 3 в составе:

- ПАК ViPNet IDS NS 3.6.0
- ПО ViPNet IDS MC 1.6.0
- ПАК ViPNet TIAS 3.5.1

СЗИ

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну, № РОСС RU.0005.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ

№ СФ/СЗИ-0394

Выдан "22" июня 2020 г. Действителен до "30" июня 2023 г.

Настоящий сертификат удостоверяет, что:

1. Средство защиты информации «Система обнаружения компьютерных атак (вторжений) ViPNet IDS 3» (исполнения: ViPNet IDS NS100, ViPNet IDS NS1000, ViPNet IDS NS2000, ViPNet IDS NS VA в комбинации со средством централизованного управления и мониторинга ViPNet IDS MC, средством анализа событий информационной безопасности ViPNet TIAS (исполнения: TIAS 1000, TIAS 2000, TIAS 5000, TIAS VA)), изготовленное в соответствии с техническими условиями ФРКЕ.00211-01 97 01 ТУ,

соответствует требованиям ФСБ России к средствам обнаружения компьютерных атак класса В и может использоваться для обнаружения в автоматическом режиме компьютерных атак (вторжений) на основе анализа [illegible]

СОВ 4 класс, ТДБ 4 уровень

Система IDS 3 в составе:

- ПО ViPNet IDS NS 3.6.0
- ПО ViPNet IDS MC 1.6.0
- ПО ViPNet TIAS 3.5.1

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4329

Внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации 24 ноября 2020 г.

Выдан: 24 ноября 2020 г.
Действителен до: 24 ноября 2025 г.

Настоящий сертификат удостоверяет, что **система обнаружения компьютерных атак (вторжений) ViPNet IDS 3**, разработанная и производимая АО «ИнфоТеКС», является системой обнаружения вторжений, соответствует требованиям по безопасности информации, установленным в документах «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия, «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТ.СОВ.С4.ПЗ» (ФСТЭК России, 2012).

Сертификат выдан на основании технического заключения от 30.09.2020, оформленного по результатам сертификационных испытаний испытательной лабораторией МОУ «ИИФ» (аттестат аккредитации от 18.11.2016 № СЗИ RU.0001.01БИ00.Б012), и экспертного заключения от 27.10.2020, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «ИнфоТеКС»
Адрес: 127287, г. Москва, Старый Петровско-Разумовский проезд, д. 1/23, стр. 1
Телефон: (495) 737-6192

НАЧАЛЬНИК 2 УПРАВЛЕНИЯ ФСТЭК РОССИИ

Д.Шевцов

Сертификация

Соответствие требованиям ФСБ к СОА класса В (по новым требованиям).

Соответствие требованиям ФТЭК СОВ 4 класс, ТДБ 4 уровень

Версии, которые будут сертифицированы в 2022 году:

- ПАК ViPNet IDS NS 3.8.0
- ПО ViPNet IDS MC 1.8.0
- ПАК ViPNet TIAS 3.7.1

Что дальше?

ViPNet TIAS 3.8

- Пользовательские метаправила;
- Дообучение модели на пользовательских данных;
- Ретроспективный анализ.

Интеграция с единой системой управления ViPNet PRIME

- Управление лицензиями;
- Управление организационной структурой и устройствами;
- Управление пользователями и ролями;
- Аутентификация и авторизация пользователей.