



ViPNet TIAS 3.6

Новые возможности

Светлана Старовойт



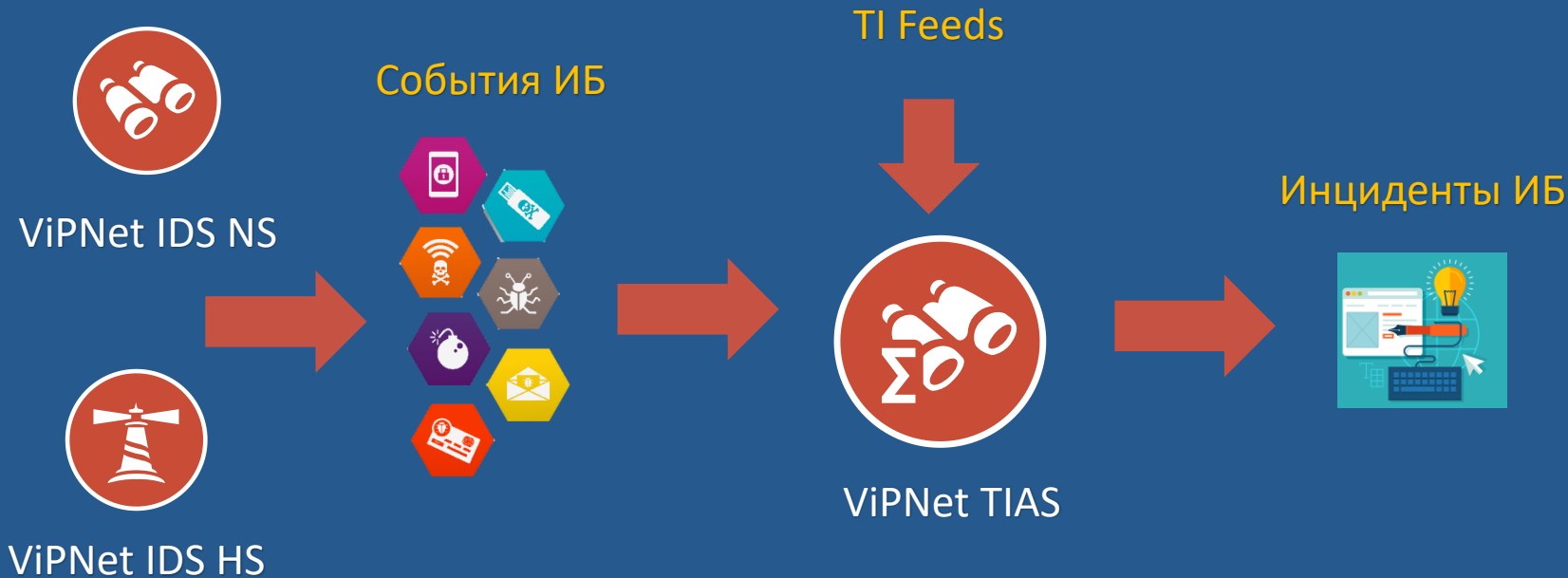
О чем этот вебинар?

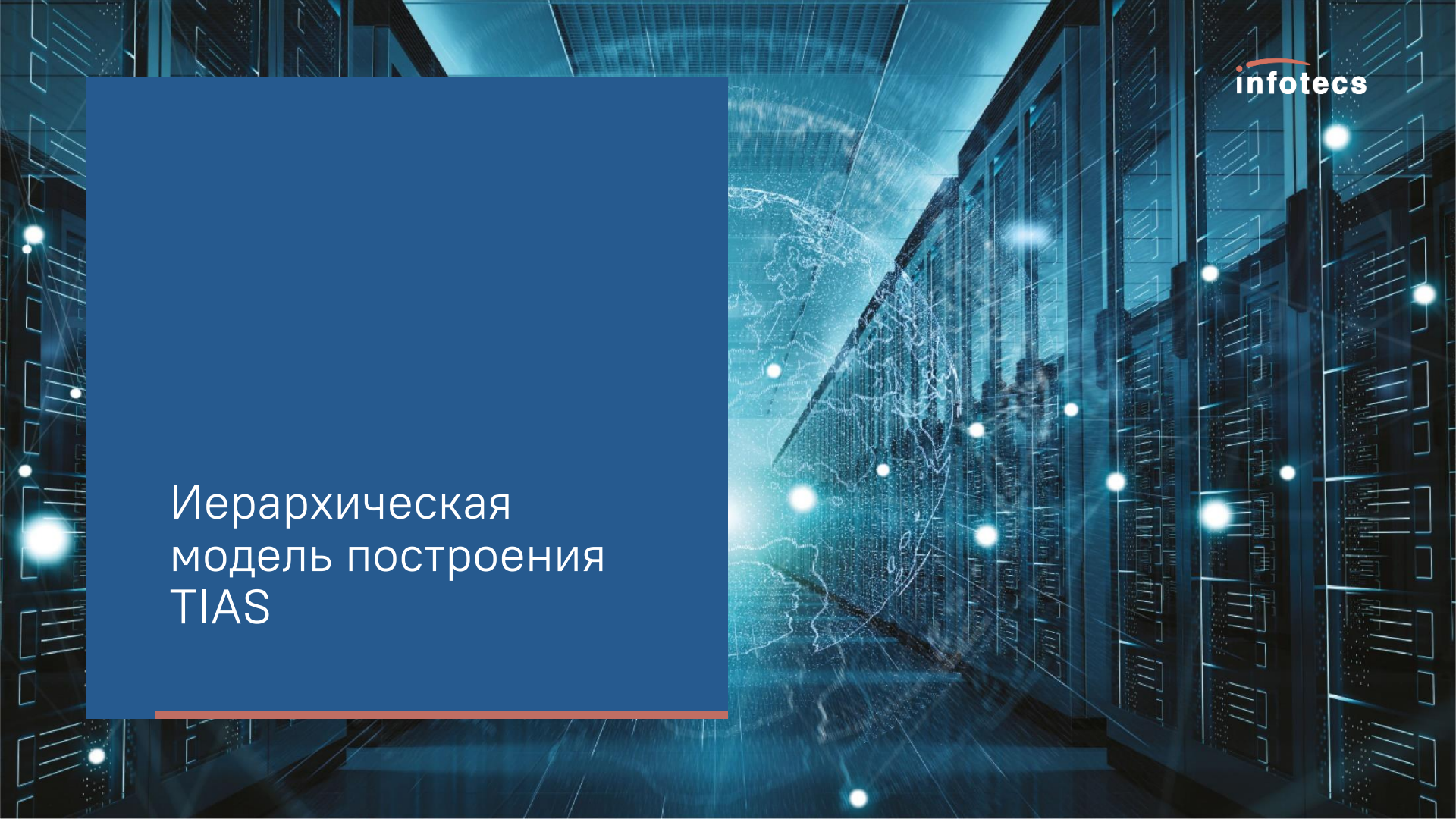
Новое в версии ViPNet TIAS 3.6



- Иерархическая схема построения TIAS
 - Мультиарендный режим доступа в TIAS
 - Новые алгоритмы выявления инцидентов
 - Гарантированная доставка событий по защищенному каналу
- и другие возможности

Что такое ViPNet TIAS?



The background of the slide is a dark blue, futuristic server room. On the right side, there are rows of server racks with glowing blue lights. The left side is dominated by a large, semi-transparent blue rectangle containing white text. The overall scene is overlaid with a complex digital network of white lines and nodes, resembling a data flow or a neural network, which is most prominent in the center and right areas of the image.

Иерархическая модель построения TIAS

Кому и зачем это нужно?



Режим подчиненного TIAS

Весь функционал TIAS Standalone

+ передача в головной TIAS:

- инцидентов и связанных событий
- агрегированной информации о событиях для инфопанели



- ✓ Не требует специфической лицензии
- ✓ Режим работы и головной TIAS задается в IDS MC
- ✓ На любом варианте исполнения TIAS

Режим головного TIAS



- Сбор и хранение информации обо всех инцидентах
- Работа с инцидентами и связанными событиями
- Передача инцидентов в НКЦКИ (настраивается для каждой организации)
- Отображение онлайн дэшбордов по событиям
- Оповещение об инцидентах и передача инцидентов во внешние системы
- Отчеты

Доступ к Web UI подчиненных TIAS

Успешная эксплуатация уязвимости в HTTP.sys IIS (MS-15-034)

Высокий уровень важности

Параметры инцидента НКЦКИ

Статус инцидента: **Не обработан** Взять в работу

Способ передачи в НКЦКИ:

Дата и время отправки:

Категория инцидента (НКЦКИ): **Попытка несанкционированного доступа**

Тип инцидента (НКЦКИ): **Попытка эксплуатации уязвимости**

Подчиненный TIAS: **slave_192.168.80.45**

Идентификатор TIAS: 5e52b03c-6931-4104-92e4-4baf0b1b345b

Рейтинг: 10

Количество срабатываний метаправила: 1

Количество связанных событий: 1

ViPNet TIAS

Инциденты

67e9cfc9-cf09-4617-89d7-462f363c21c1

<input type="checkbox"/>	Статус	Пользователь	Дата и время обновления...	Рейтинг
<input type="checkbox"/>	Не обрабо...		12.11.2020 17:56:25	10

Режим головного TIAS



- Требуется специальная лицензия на головной TIAS
- Управление структурой и режим работы TIAS задается в IDS MC
- Работает на TIAS 2000 и TIAS 5000

Мультиарендный режим работы

Сервис на базе решения

Сервис-провайдер



ViPNet TIAS



ViPNet IDS MC



ViPNet IDS HS Server

Клиент 1



ViPNet IDS NS



ViPNet IDS HS Agents

Клиент 2



ViPNet IDS HS Agents

Клиент 3



ViPNet IDS NS



ViPNet IDS NS

- мультиарендный доступ к IDS MC и TIAS
- мастер подключения организации
- активация и настройка сенсоров из IDS MC
- распределение и учет лицензий по организациям

Виды услуг

- Мониторинг угроз ИБ в сетевом трафике клиента и автоматическое выявление инцидентов на основе анализа трафика
 - оповещение по e-mail
 - в режиме 24x7
 - сетевой сенсор ViPNet IDS NS.

- Мониторинг угроз ИБ на рабочих станциях пользователей
 - оповещение по e-mail
 - в режиме 24x7
 - сенсоры ViPNet IDS HS agent.

- Проведение расследований по инцидентам и рекомендации по реагированию
 - квалифицированными аналитиками ИБ сервис-провайдера
 - с привлечением аналитиков Перспективного мониторинга

- Предоставление отчетов по выявленным угрозам и инцидентам

- Настройка и обслуживание сенсоров

- Доступ конечного клиента к web-консоли ViPNet TIAS

Разграничение доступа в TIAS

Учетные записи

Область действия | Новая учетная запись

ФМС г. Томск

Имя учетной записи	Роли
Administrator	Администратор TIAS
Ivanov	Администратор, Оператор
TestUser	Аудитор, Оператор
TestUserAdministratorTias	Администратор TIAS
TestUserAuditor	Аудитор

Ivanov

Имя учетной записи: Ivanov

Задайте пароль вручную или сгенерируйте его автоматически.

Пароль: Сгенерировать

Не менее 12 и не более 31 символа.

Роли

Администратор

ФМС г. Томск


Оператор

Городская муниципальная поликлиника №25 г. Томск
Центральная районная больница город Томск

Специальные роли

Аудитор

Администратор TIAS

The background of the slide is a futuristic data center. It features rows of server racks on the right side, illuminated with blue light. The floor is highly reflective, mirroring the lights and the server racks. In the center and left, there are abstract digital patterns, including a glowing globe and various lines and dots, suggesting data flow and network connectivity. The overall color palette is dominated by dark blues and teals, with bright white and light blue highlights from the lights and reflections.

Новые алгоритмы выявления инцидентов

Агрегация инцидентов

Сеть 1

Название сети: Сеть 1

Обнаружение инцидентов

Частота заведения повторных инцидентов (часы): 6

Множественные попытки использования DNS контролируемого ресурса ...

Средний уровень важности

Параметры инцидента НКЦКИ

Статус инцидента: Не обработан [Взять в работу](#)

Способ передачи в НКЦКИ: Не отправлен

Дата и время отправки:

Категория инцидента (НКЦКИ): Нарушение доступа

Тип инцидента (НКЦКИ): Распределенное воздействие с целью нарушения доступа

Рейтинг: 5

Количество срабатываний метасправил: 2

Количество связанных событий: 2

Дата и время регистрации инцидента: 27.11.2020 22:34:07

Дата и время обновления инцидента: 27.11.2020 22:45:10

Тип угрозы: Иное
Нарушение доступности

Пораженные узлы (1): ip: 24.200.1.24
mac: 68:05:ca:15:f3:20
Страна: Канада
Город: Монреаль

Сенсоры (1): VIPNet IDS NS VA 1291861570
eef00ebb-9112-4d87-9576-628502a9a9de

Корреляция событий с разных источников

The screenshot displays the VIPNet TIAS interface with the following components:

- Left Sidebar:** Navigation menu including Мониторинг, Инциденты (994), События, Сетевые Угрозы, Отчеты, Управление (Инфраструктура, Оповещение, Интеграция, Экспертные данные, Сбор данных), Система (Учетные записи, Сервисные функции), and Аудит (Журнал аудита).
- Main Panel - Incidents:** A table titled "Инциденты" with 5083 total incidents. The table has columns for Status, Date/Time, Rating, Affected Hosts, and Name. The first row is highlighted in blue.
- Main Panel - Correlated Events:** A table titled "Связанные события" showing related events with columns for Date/Time, Level, Rule, Sensor Type, ID, IP Address, Port, and IP Address of the collector. One row is highlighted with a red box.
- Right Panel - Incident Details:** A detailed view of an incident titled "Классификатором выявлено подозрительное событие". It includes fields for (НКЦИ), Type, Rating (10), Number of related events (0), Date and time of registration (23.11.2020 14:15:44), Date and time of update (23.11.2020 14:15:44), Type of threat, Affected Hosts (IP: 37.110.48.7, MAC: 88:5a:92:84:ae:51, Country: Russia, City: Moscow), Sensors (IDS NS Sensor), and Additional Information (Method of realization: heuristic, Method of detection: heuristic, Symptoms: anomalous network activity, etc.).

Статус	Дата и время обновл...	Рейтинг	Пораженные узлы	Наименование
Не обработан	23.11.2020 14:15:44	9	36.110.48.4	Классификатором выявлено подозрительное с...
Не обработан	23.11.2020 14:15:44	10	37.110.48.7	Классификатором выявлено подозрительное с...
Не обработан	23.11.2020 14:16:55	9	3.200.1.6	Классификатором выявлено подозрительное с...
Не обработан	23.11.2020 14:15:44	9	1.200.1.8	Классификатором выявлено подозрительное с...
Не обработан	23.11.2020 14:15:19	10	3.200.1.9	Классификатором выявлено подозрительное с...
Не обработан	23.11.2020 14:15:20	9	37.110.48.5	Классификатором выявлено подозрительное с...
Не обработан	23.11.2020 14:15:45	10	35.110.48.9	Классификатором выявлено подозрительное с...
Не обработан	23.11.2020 14:15:44	10	3.200.1.4	Классификатором выявлено подозрительное с...
Не обработан	23.11.2020 14:15:45	9	2.200.1.5	Классификатором выявлено подозрительное с...
Не обработан	23.11.2020 14:16:09	10	37.110.48.3	Классификатором выявлено подозрительное с...
Не обработан	23.11.2020 14:15:20	9	1.200.1.9	Классификатором выявлено подозрительное с...
Не обработан	23.11.2020 14:15:44	9	2.200.1.1	Классификатором выявлено подозрительное с...
Не обработан	23.11.2020 14:15:19	9	36.110.48.9	Классификатором выявлено подозрительное с...

Дата и время	Урове...	Правило	Тип сенсора	Идент...	IP-адрес...	Порт и...	IP-адрес получ...
23.11.2020 14:12:43	Критичн...	ET CHAT Skype VOIP Checking Version (Startup) 5...	VIPNet IDS NS	bb6b99e0...	37.110.48.7	56879	2.200.1.8
23.11.2020 14:12:43	Высокий	ET POLICY POSSIBLE Web Crawl using Wget 494	VIPNet IDS NS	bb6b99e0...	37.110.48.7	39372	1.200.1.8
23.11.2020 14:12:43	Критичн...	ET INFO Session Traversal Utilities for NAT (STUN...	VIPNet IDS NS	bb6b99e0...	37.110.48.7	63732	1.200.1.4
23.11.2020 14:12:43	Критичн...	ET CHAT Skype VOIP Checking Version (Startup) 4...	VIPNet IDS NS	bb6b99e0...	37.110.48.7	56879	1.200.1.2
23.11.2020 14:12:43	Высокий	ET POLICY curl User-Agent Outbound 462	VIPNet IDS NS	bb6b99e0...	37.110.48.7	33606	3.200.1.1
23.11.2020 14:12:43	Высокий	SNMP public access udp 440	VIPNet IDS NS	bb6b99e0...	37.110.48.7	27294	1.200.1.6
23.11.2020 14:12:43	Критичн...	ET POLICY PE EXE or DLL Windows file download...	VIPNet IDS HS	bb6b99e0...	37.110.48.7	80	2.200.1.3
23.11.2020 14:12:43	Критичн...	ET POLICY PE EXE or DLL Windows file download...	VIPNet IDS HS	bb6b99e0...	37.110.48.7	80	1.200.1.8
23.11.2020 14:12:43	Критичн...	ET CHAT Skype VOIP Checking Version (Startup) 2...	VIPNet IDS NS	bb6b99e0...	37.110.48.7	56879	3.200.1.6
23.11.2020 14:12:43	Критичн...	ET INFO Session Traversal Utilities for NAT (STUN...	VIPNet IDS NS	bb6b99e0...	37.110.48.7	63732	3.200.1.2

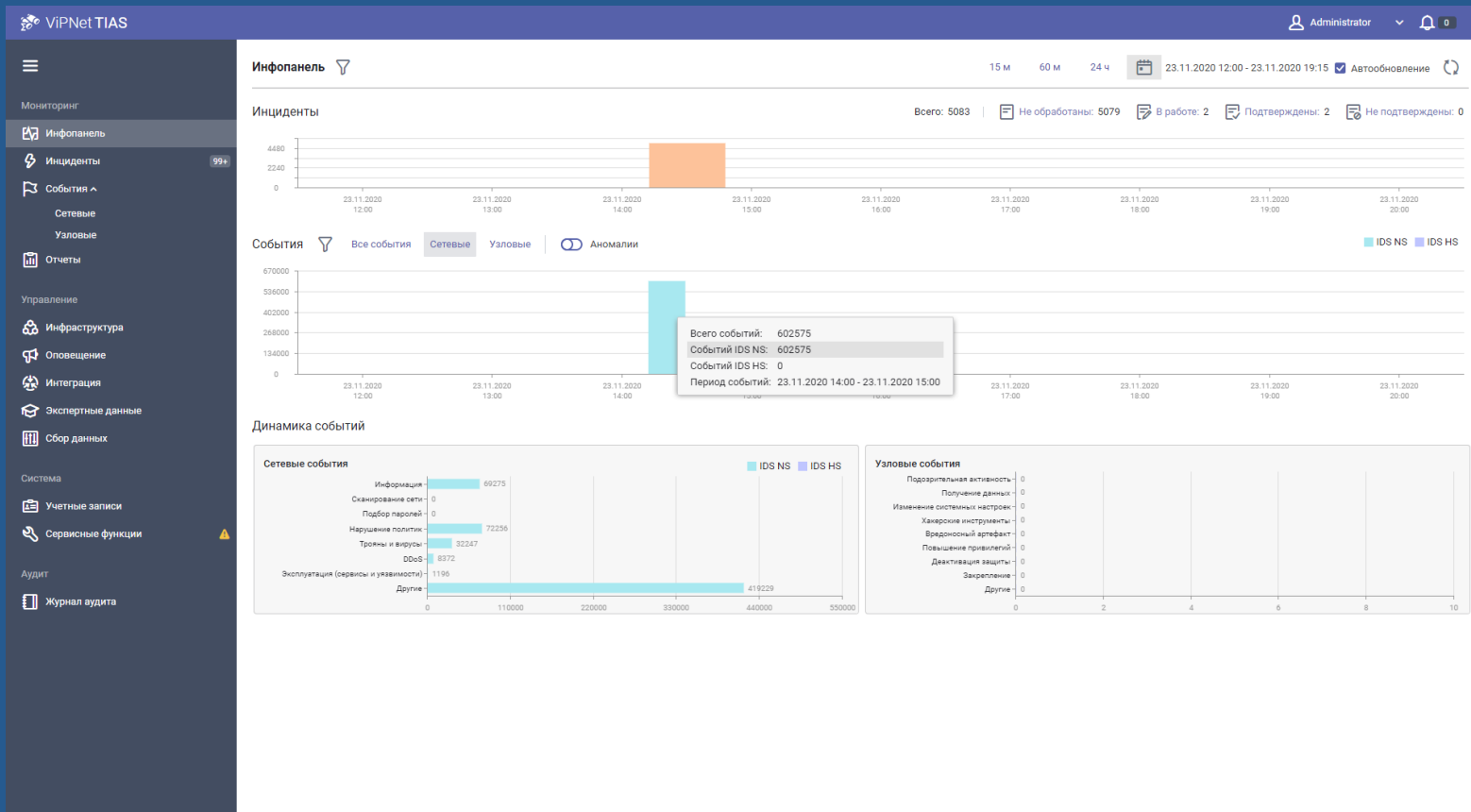
Классификатором выявлено подозрительное событие
Высокий уровень важности

(НКЦИ): ...
Тип инцидента (НКЦИ): Другие
Рейтинг: 10
Количество сработавшей метавправила: 0
Количество связанных событий: 100
Дата и время регистрации инцидента: 23.11.2020 14:15:44
Дата и время обновления инцидента: 23.11.2020 14:15:44
Тип угрозы:
Пораженные узлы (1): ip: 37.110.48.7
mac: 88:5a:92:84:ae:51
Страна: Россия
Город: Москва
Сенсоры (1): IDS NS Sensor
bb6b99e0-1ba7-49b3-6180-2694dcb38540
192.168.78.85

Дополнительная информация
Методы реализации угрозы:
Метод обнаружения: Эвристический
Симптомы: Аномальная сетевая активность AFM
Идентификатор инцидента: 02f1f0e5-ec57-47a5-8317-02eed51449ac
Наименование: Классификатором выявлено подозрительное событие
Описание:
Рекомендации:
• Отключить пораженный компьютер от сети
• Провести интервьюирование владельца
• Осуществить антивирусную проверку
• Передать обнаруженные вредоносные ПО в ЦМ для анализа
• Удалить обнаруженные вредоносные ПО
• Провести анализ сетевой активности узла

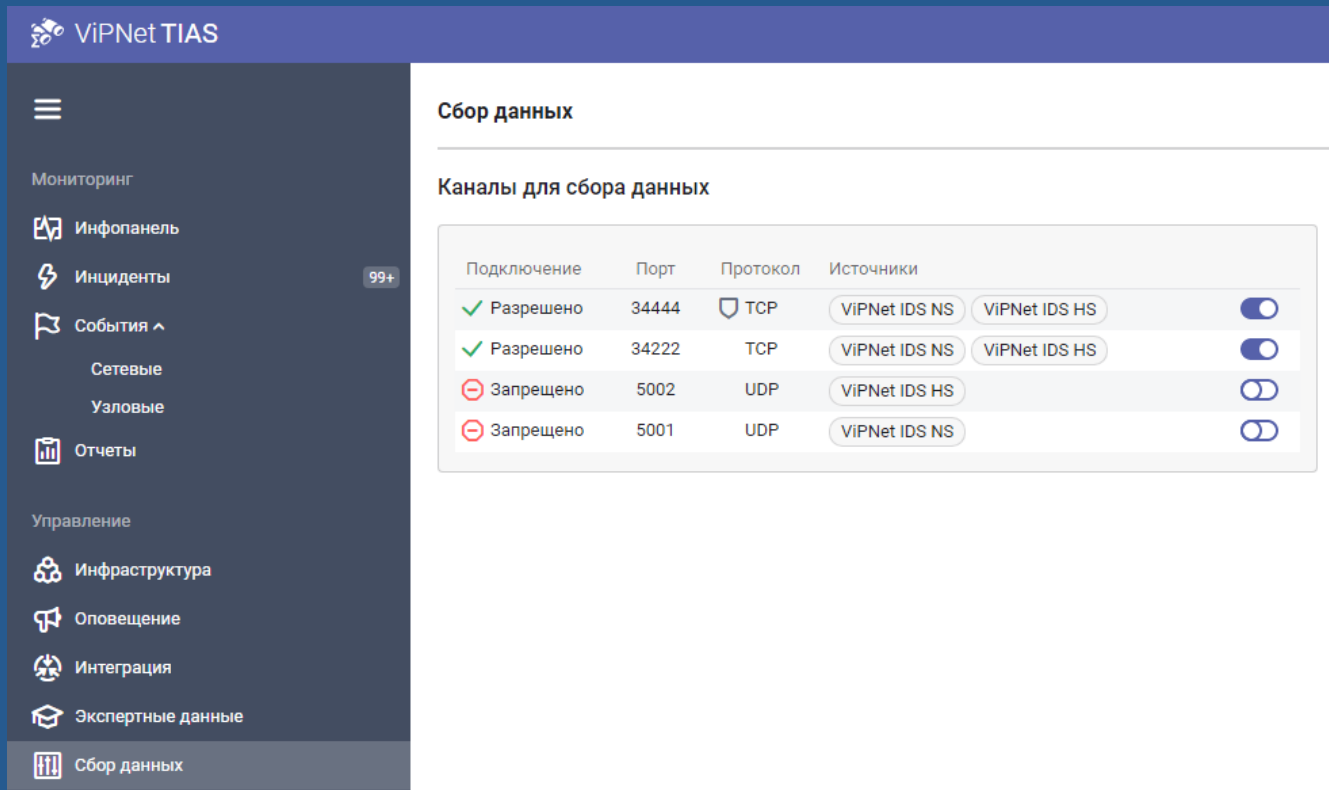
17:17:02 23.11.2020

Общая инфопанель событий и инцидентов



И другие полезные
доработки

Гарантированная доставка и защита канала передачи событий



ViPNet TIAS

Мониторинг

- Инфопанель
- Инциденты 99+
- События ^
 - Сетевые
 - Узловые
- Отчеты

Управление

- Инфраструктура
- Оповещение
- Интеграция
- Экспертные данные
- Сбор данных**

Сбор данных

Каналы для сбора данных

Подключение	Порт	Протокол	Источники	
✓ Разрешено	34444	TCP	ViPNet IDS NS ViPNet IDS HS	<input checked="" type="checkbox"/>
✓ Разрешено	34222	TCP	ViPNet IDS NS ViPNet IDS HS	<input checked="" type="checkbox"/>
⊖ Запрещено	5002	UDP	ViPNet IDS HS	<input type="checkbox"/>
⊖ Запрещено	5001	UDP	ViPNet IDS NS	<input type="checkbox"/>

Управление сертификатами и лицензией через Web GUI

Сервисные функции

VIPNet TIAS Лицензии **Управление сертификатами** Диагностика системы

Сертификаты

⚠ Для защиты подключения между веб-браузером и VIPNet TIAS необходимо установить публичный или собственный транспортный сертификат.

Публичный транспортный сертификат ⓘ

Действителен по: 23.07.2021 09:38:58
Адреса: Test SMP\ (Основной)
smp.itcs
*.smp.itcs

Установить Обновить Данные сертификата

Собственный транспортный сертификат ⓘ

Действителен по: 25.11.2030 22:14:45
Адреса: 192.168.78.149 (Основной)
tias-local.com

Установить Перевыпустить Данные сертификата

Корневой самоподписанный сертификат ⓘ

Действителен по: 25.11.2030 22:14:39
Страна: US
Организация: Amazon

Выгрузить Перевыпустить Данные сертификата

Сервисные функции

VIPNet TIAS Лицензии **Управление сертификатами** Диагностика системы

[Загрузить лицензию](#)

Текущая лицензия

Статус лицензии: Действительна
Срок действия лицензии: 11.06.2021 03:00:00
Поддерживаемые версии: Текущая - 3.6.1
Максимальная - 5.0

Аппаратная платформа: tias_va
Идентификатор лицензии: 1739267/1/1-TIAS
Максимальное количество событий в секунду: 30300
Срок действия подписки на экспертные данные: 190 дней осталось
Срок действия подписки на подключение к НКЦКИ: 190 дней осталось

Лицензионные объекты

Тип сенсора	Максимально доступное количество	Подключено	Срок действия
VIPNet IDS NS	500	1	Завершается 11.06.2021
VIPNet IDS HS	500		Завершается 11.06.2021
VIPNet IDS HS Agent	500		Завершается 11.06.2021

Другие улучшения



- Загрузка и выгрузка данных по протоколу SFTP
- Установка часового пояса местоположения ViPNet TIAS
- Расширенный набор параметров мониторинга TIAS в ViPNet IDS MC.

Передача в ViPNet IDS MC следующих данных:

- Системное время
- Версия ПО и наименование исполнения ViPNet TIAS
- Дата окончания действия лицензии
- Дата и время установки и выпуска установленных экспертных данных
- Отчет для биллинга об узлах защищаемой сети в каждой обслуживаемой организации.

Основные отличия IDS NS 3 версии

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 4329

Внесен в государственной 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 (вторичный) ViPNet IDS 3, разработанная и произведенная АО «ИнфоТекс», является системой обнаружения вторжений, соответствует требованиям по безопасности информации, установленным в документе «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, 2013) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты. ИТС.ОВ.С4.П3» (ФСТЭК России, 2012).

Сертификат выдан на основании технического заключения от 30.09.2020, оформленного по результатам сертификационных испытаний испытательной лабораторией МСУ «ИИФ» (аттестат аккредитации от 18.11.2016 № СИИ RU.0001.01БИ00.012), а экспертного заключения от 27.10.2020, оформленного органом по сертификации ФГУ «ТРИНИ ПТЗи ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СИИ RU.0001.01БИ00.A002).

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

Примечание: сертифицированной продукции, указанной в настоящем сертификате соответствия, не обеспечена техническая информация, раскрывающая ее качество и/или в государственном реестре средств защиты информации по требованиям безопасности информации.

- Централизованное управление и мониторинг с помощью ViPNet IDS MC
- Новый модуль Malware detection
- Возможность анализа до 10 Гбит трафика
- Сертифицированная версия IDS NS VA
- Управление правилами с помощью профилей
- Синхронизация системного времени ViPNet IDS NS
- Возможность удаленного подключения к консоли по протоколу SSH
- Возможность настройки передаваемых в CEF параметров сообщений
- Обнаружение сетевых атак на протокол IPv6
- Расширение функционала по обнаружению атак типа ARP-spoofing

Что дальше?



- ViPNet xFW и EPP в качестве источников
- Выявление инцидентов с использованием репутационных списков адресов
- Обогащение информации об инцидентах данными от сканеров уязвимостей
- Ретроспективный анализ событий
- Новые алгоритмы машинного обучения

Ответы на вопросы!

Контакты

Светлана Старовойт

Старший менеджер
отдела развития продуктов

E-mail:
starovoytsg@infotecs.ru

The logo for 'infotecs' features a small orange dot above the letter 'i', followed by a curved orange line that arches over the letters 'f' and 'o'. The word 'infotecs' is written in a bold, white, lowercase sans-serif font.

infotecs

A vertical orange line that acts as a separator between the logo and the text.

Спасибо
за внимание!