

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 фишки последних релизов IDS NS и IDS MC.
5. А что дальше? Планы развития.



0 решении ViPNet TDR

Состав решения ViPNet TDR

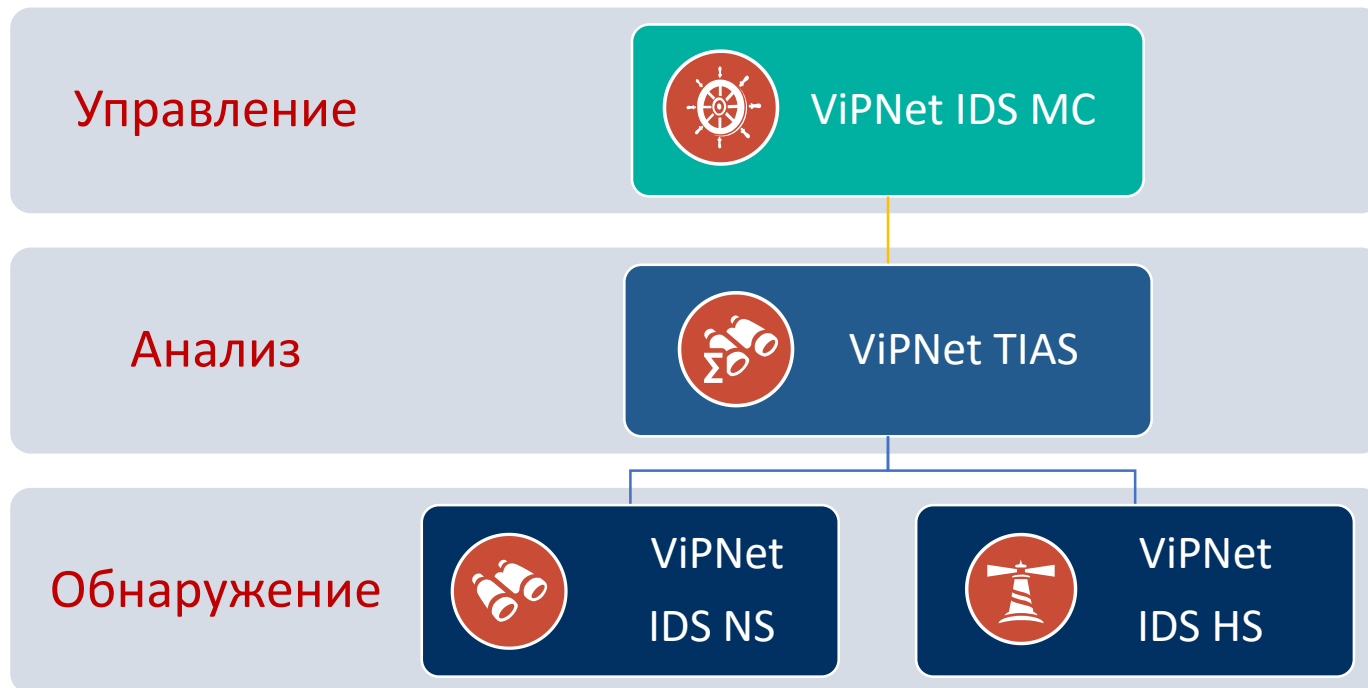


Схема развертывания

Центр мониторинга



ViPNet TIAS



ViPNet IDS MC



ViPNet IDS HS Server



ViPNet IDS NS



ViPNet IDS HS Agents

сегмент 1



ViPNet IDS HS Agents

сегмент 2



ViPNet IDS NS



ViPNet IDS NS

сегмент 3

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

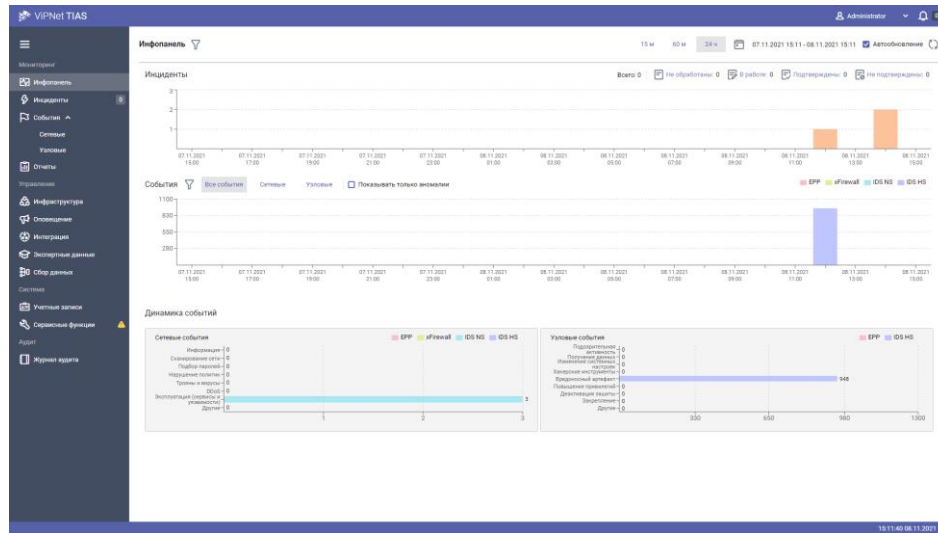


ViPNet IDS HS

- 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)

Классификатором выявлено подозрительное событие
Высокий уровень важности

Параметры инцидента НКЦКИ

Статус инцидента:

Способ передачи в НКЦКИ:

Дата и время отправки:

Категория инцидента (НКЦКИ):

Тип инцидента (НКЦКИ):

Тип инцидента:

Пользователь:

Дата и время:

Пораженные узлы (1):

страна: США
Город: Не определен

Рейтинг: 10

IP-адрес сенсора: 123.123.123.123

Идентификатор сенсора: 123456789

Название сенсора: Сенсор 12345

Метод реализации угрозы: -

Наименование: Классификатором выявлено подозрительное событие

Метод обнаружения: Звристический

Идентификатор инцидента: 123456789

Симптомы: Аномальная сетевая активность APM

Рекомендации

- Отключить пораженный актив от вычислительной сети

Параметры инцидента

Основные сведения

Информация об атакованной информационной системе:

Информация об атакованных узлах:

Индикаторы компрометации:
Дополнительная информация об инциденте:

Меры по реагированию:
Связь с другими инцидентами:

*** Класс события информационной безопасности:**

*** Категория:**

*** Тип:**

Идентификатор: incidentGS-f34030ef-358a-445c-8567-25985ce 6d68a

Регистрационный номер:

*** Степень конфиденциальности сведений об инциденте:**

Наименование организации-отправителя сведений об инциденте:

Оценка последствий

*** Нарушение конфиденциальности:**

*** Нарушение целостности:**

*** Нарушение доступности:**

Иная форма нарушения:

⚠ Для отправки заполните все обязательные поля.

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 ТІАС (v 3.6)





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

ViPNet TIAS

Меню

- Мониторинг
 - Инфопанель
 - Инциденты 99+
 - События ^
 - Сетевые
 - Узловые
 - Отчеты
- Управление
 - Инфраструктура
 - Оповещение
 - Интеграция
 - Экспертные данные
 - Сбор данных
- Система
 - Учетные записи
 - Сервисные функции ⚠
- Аудит
 - Журнал аудита

Сервисные функции

Лицензии ● Управление сертификатами Диагностика системы

[Загрузить лицензию](#)

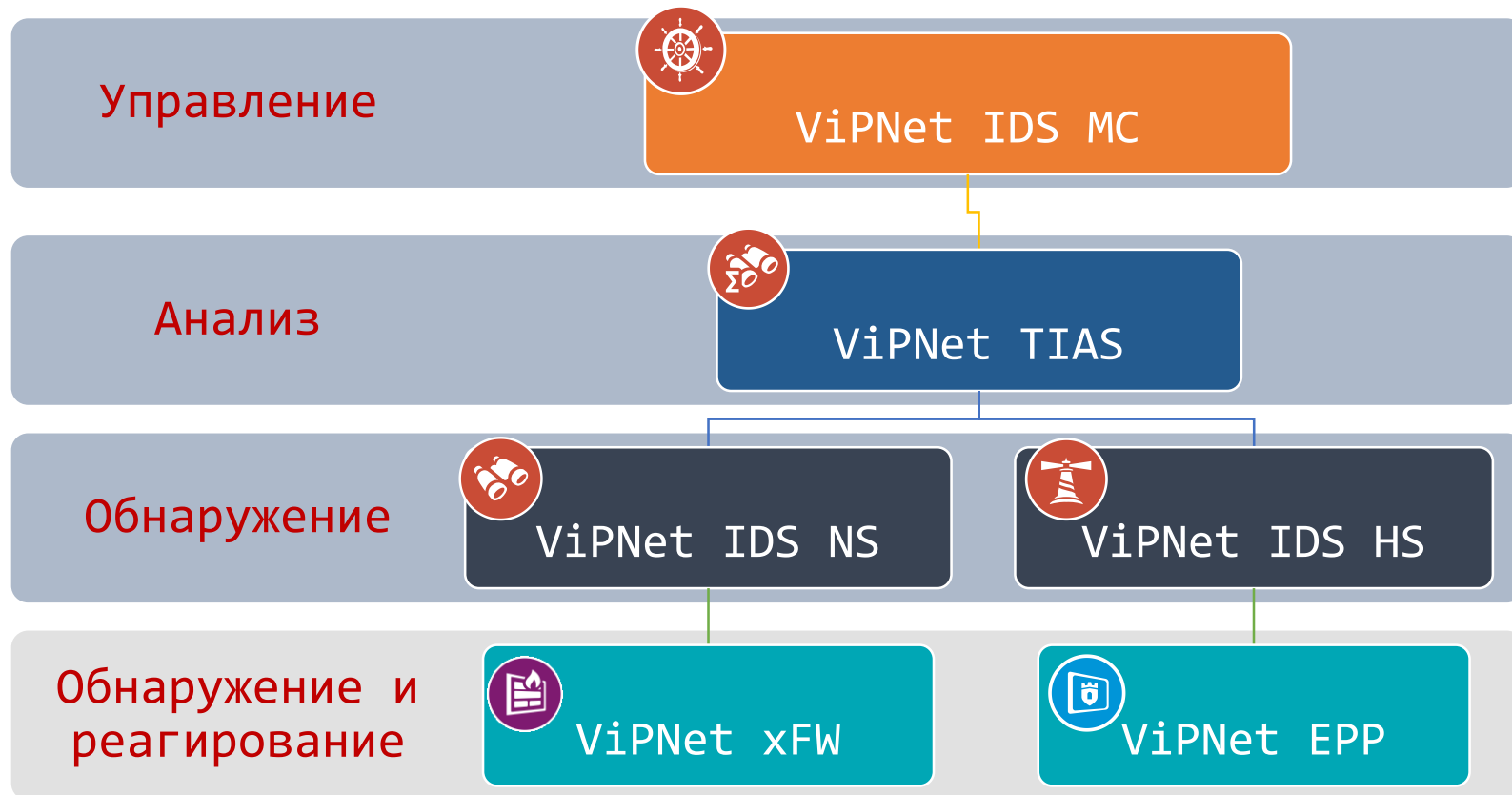
Текущая лицензия

Статус лицензии:	Действительна
Срок действия лицензии:	30.06.2022 03:00:00
Поддерживаемые версии:	Текущая - 3.7.1 Максимальная - 5.0
Аппаратная платформа:	tias_va
Идентификатор лицензии:	2315048/1/1-TIAS
Максимальное количество событий в секунду:	300
Срок действия подписки на экспертные данные:	233 дня осталось
Срок действия подписки на подключение к НКЦКИ:	233 дня осталось

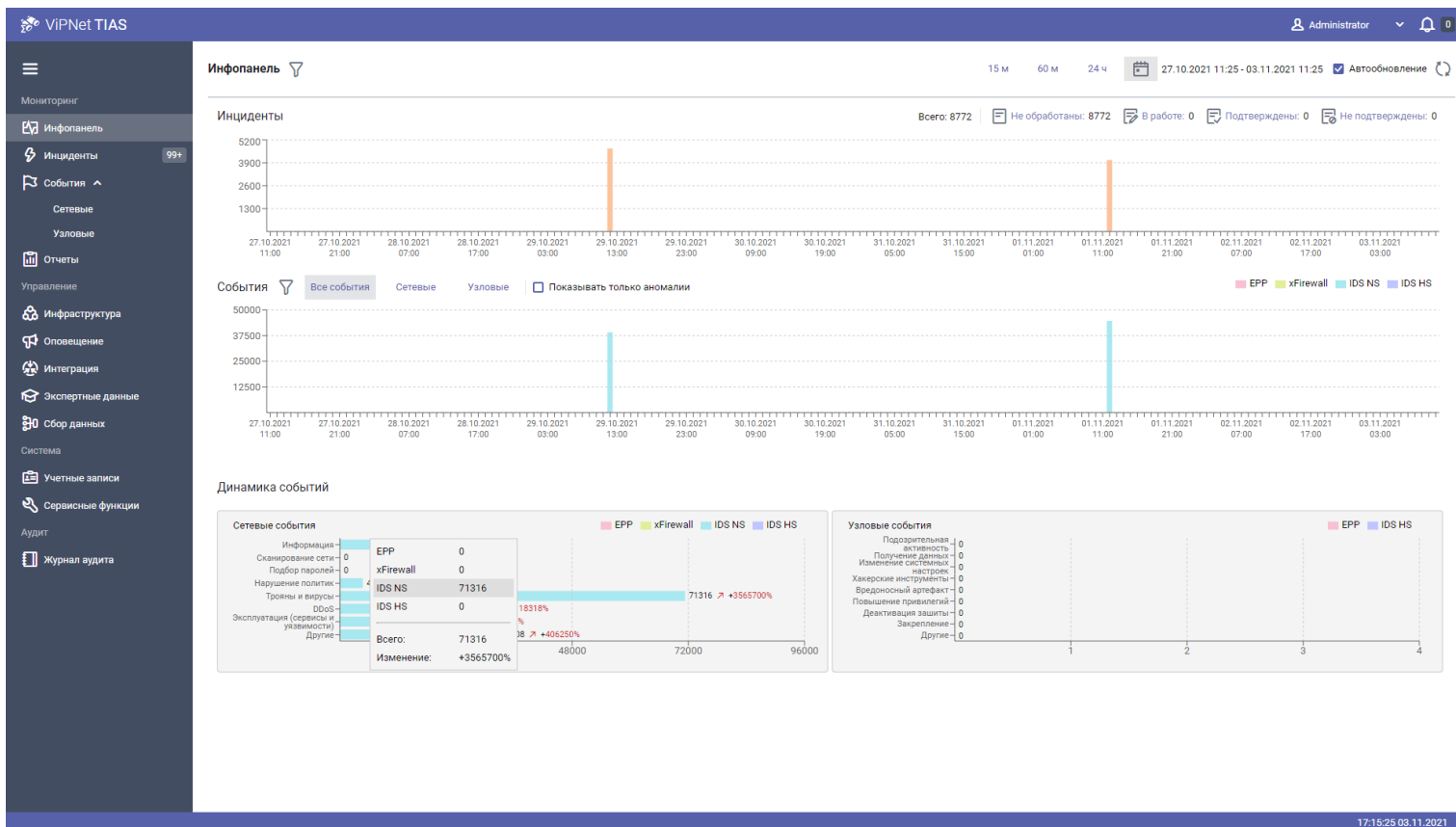
Лицензионные объекты

Тип сенсора	Максимально доступное количество	Подключено	Срок действия
IDS NS	10	7	Завершается 30.06.2022 03:00:00
IDS HS	10	4	Завершается 30.06.2022 03:00:00
IDS HS Agent	10	9	Завершается 30.06.2022 03:00:00
EPP	10	5	Завершается 30.06.2022 03:00:00
xFirewall	10	3	Завершается 30.06.2022 03:00:00
EPP Agent	10		Завершается 30.06.2022 03:00:00

Состав решения ViPNet TDR



Фильтрация по типу источников



Данные от сканеров уязвимостей

● Эксплуатация уязвимости CVE-2015-1635

Высокий уровень важности

Рейтинг: 10

Количество сработавших метаправил: 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

VIPNet TIAS Administrator 0

Инциденты 15 м 60 м 24 ч 08.11.2021 16:09 - 08.11.2021 16:24

Количество инцидентов: 7

Статус	Пользов...	Дата и время рег...	Дата и время об...	Кategori...	Тип инци...	Способ п...	Дата и время от...	Рейтинг
<input type="checkbox"/>	Не обработан	08.11.2021 16:24:01	08.11.2021 16:24:01	Заражение ...	Заражение ...	Не отправл...		10
<input type="checkbox"/>	Не обработан	08.11.2021 16:09:29	08.11.2021 16:09:29	Заражение ...	Заражение ...	Не отправл...		10
<input type="checkbox"/>	Не обработан	08.11.2021 16:09:29	08.11.2021 16:09:29	Заражение ...	Заражение ...	Не отправл...		10
<input type="checkbox"/>	Не обработан	08.11.2021 16:09:29	08.11.2021 16:09:29	Заражение ...	Заражение ...	Не отправл...		10
<input type="checkbox"/>	Не обработан	08.11.2021 16:09:29	08.11.2021 16:09:29	Заражение ...	Заражение ...	Не отправл...		10
<input type="checkbox"/>	Не обработан	08.11.2021 16:09:13	08.11.2021 16:09:13	Заражение ...	Заражение ...	Не отправл...		10

Связанные события

агента	IP-адрес агента	Идентиф...	IP-адрес источника	Домен отп...	Порт и...	IP-адрес получателя	Домен пол...	Порт п...	Пакет
	60b23133-0...	192.168.78.14			53	IoC 91.109.184.8		53	

Страна источника: Не определено
Страна получателя: Франция
Хэш-сумма
Категория угрозы: 0
Из них аномалий: 0

Страница 1 25

Заражение хоста трояном-шифровальщиком...
Высокий уровень важности

Параметры инцидента НКЦКИ

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

Способ передачи в НКЦКИ:

Дата и время отправки:

Категория инцидента (НКЦКИ): Заражение вредоносными программами

Тип инцидента (НКЦКИ): Заражение вредоносной программой

Рейтинг: 10

Количество срабатываний метаправила: 1

Количество связанных событий: 1

Дата и время регистрации инцидента: 08.11.2021 16:24:01

Дата и время обновления инцидента: 08.11.2021 16:24:01

Типы угроз: Нарушение доступности
Нарушение целостности

Пораженные узлы (1): ip: 192.168.78.14
mac: 00:0c:29:1b:b6:03
Страна: Не определено
Город: Не определено

Сенсоры (1): IDS NS 001 fixed
60b23133-0948-44e2-bab7-16e9ee96b567

Дополнительная информация

Методы реализации: Загрузка в систему вредоносного ПО
угроз:

Метод обновления: Сигнационный

IoC в событиях

VIPNet TIAS Administrator 0

Сетевые события

15 м 60 м 24 ч 07.11.2021 17:17 - 08.11.2021 17:17

IDS NS, xFirewall Категории событий

Источники

Уров...	Пра...	Кол...	IP-адрес ист...	IP-адрес се...	Назв...	Прот...	Номе...	Катер...
Низкий	Malicio...	16	91.26.97.3		IDS NS 0...	UDP	147:1	Трояны ...
Низкий	Malicio...	16	91.26.144.81		IDS NS 0...	UDP	147:1	Трояны ...
Низкий	Malicio...	16	91.26.152.195		IDS NS 0...	UDP	147:1	Трояны ...
Высо...	A host is...	3	192.168.78.14		IDS NS 0...	UDP	1:30068...	Эксплу...
Средн...	A succe...	3	92.216.2.155		IDS NS 0...	TCP	1:30000...	Эксплу...
Средн...	A succe...	3	192.168.0.3	13.127.137.134	IDS_NS	TCP	1:30000...	Эксплу...

Получатели

Уров...	Пра...	Кол...	IP-адрес пол...	IP-адрес се...	Назв...	Прот...	Номе...	Катер...
Низкий	Malicio...	32	91.80.0.2		IDS NS 0...	UDP	147:1	Трояны ...
Низкий	Malicio...	16	91.109.184.8		IDS NS 0...	UDP	147:1	Трояны ...
Средн...	A succe...	3	91.109.184.8		IDS NS 0...	TCP	1:30000...	Эксплу...
Средн...	A succe...	3	192.168.0.1	13.127.137.134	IDS_NS	TCP	1:30000...	Эксплу...
Высо...	A host is...	2	10.0.4.12		IDS NS 0...	UDP	1:30068...	Эксплу...
Средн...	A host is...	2	2001:db8:0:1:3		IDS NS 0...	TCP	1:20216...	Трояны ...

События на узлах

Дата и время	Номер прави...	IP-адрес получат...	Порт получат...	IP-адрес источни...	Порт источни...	Пакет	Уровень важн...	Протокол	Количес...	Правило	Категория соб...
08.11.2021 16:23:54	1:3006884	91.109.184.8	53	192.168.78.14	53	↓	Высокий	UDP	1	A host is infected with the N...	Эксплуатация (се...
08.11.2021 16:23:07	147:1	91.109.184.8	53	91.26.97.3	53	↓	Низкий	UDP	16	Malicious file downloaded	Трояны и вирусы
08.11.2021 16:22:07	1:3000040	91.109.184.8	3389	91.190.62.70	58254	↓	Средний	TCP	1	A successful HTTPsays IIS (...	Эксплуатация (се...
08.11.2021 16:22:02	1:3000040	91.109.184.8	3389	67.29.137.20	58254	↓	Средний	TCP	1	A successful HTTPsays IIS (...	Эксплуатация (се...
08.11.2021 16:20:50	1:3000040	91.109.184.8	3389	20.251.48.37	58254	↓	Средний	TCP	1	A successful HTTPsays IIS (...	Эксплуатация (се...
08.11.2021 16:09:11	1:3006885	2001:db8:0:1:3	53	105.23.211.248	53	↓	Высокий	UDP	1	A host is infected with the N...	Эксплуатация (се...
08.11.2021 16:09:11	1:3000295	2001:db8:0:1:2	58254	75.48.186.143	3389	↓	Средний	TCP	1	A host is infected with the Lo...	Другие
08.11.2021 16:09:11	1:2021619	2001:db8:0:1:3	58254	93.92.134.130	3389	↓	Средний	TCP	1	A host is infected with the De...	Трояны и вирусы
08.11.2021 16:09:11	1:3006884	10.0.4.12	53	192.168.78.14	53	↓	Высокий	UDP	1	A host is infected with the N...	Эксплуатация (се...
08.11.2021 16:09:11	147:1	91.80.0.2	53	91.26.144.81	53	↓	Низкий	UDP	16	Malicious file downloaded	Трояны и вирусы
08.11.2021 16:09:11	1:3000040	193.19.24.99	3389	92.216.2.155	58254	↓	Средний	TCP	1	A successful HTTPsays IIS (...	Эксплуатация (се...
08.11.2021 16:09:11	1:2018373	91.80.132.168	58254	91.26.225.199	3389	↓	Средний	TCP	1	A successful HeartBleed vul...	Эксплуатация (се...
08.11.2021 16:09:11	1:3000295	2001:db8:0:1:2	58254	49.106.147.214	3389	↓	Средний	TCP	1	A host is infected with the Lo...	Другие
08.11.2021 16:09:11	1:2021619	2001:db8:0:1:3	58254	92.94.42.124	3389	↓	Средний	TCP	1	A host is infected with the De...	Трояны и вирусы
08.11.2021 16:09:11	1:3006884	10.0.4.12	53	192.168.78.14	53	↓	Высокий	UDP	1	A host is infected with the N...	Эксплуатация (се...
08.11.2021 16:09:10	147:1	91.80.0.2	53	91.26.152.195	53	↓	Низкий	UDP	16	Malicious file downloaded	Трояны и вирусы

Дополнительные события

17:19:06 08.11.2021

Описание IoC в экспертных данных

Информация об индикаторе компрометации адреса 91.109.184.8

```
{
  "ip": "91.109.184.8",
  "am_ip_score": 0.95,
  "country": "FR",
  "as_owner": "Telo-liazo Services SAS",
  "asn": 29075,
  "malware_samples": [
    {
      "id": "5c6fd8fbfc902000fde02c6",
      "type": "PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows",
      "md5": "7f0e26d394863c862dc51e4d80154d1",
      "sha1": "612d4f869ded59a016c43d618948c536e677382",
      "sha256": "5c99d77eda07c5307563953144a9ae2c15645118ff08caeb32926ff19fdbfb1",
      "av_ret": {
        "positives": 40,
        "total": 69
      },
      "sample_label": "zusy",
      "am_sample_score": 0.5797101449275363
    }
  ],
  "signatures": [],
  "threat": "zusy",
  "blacklist_cnt": 1,
  "update": "2021-10-07 03:00:03.345000"
}
```

Копировать информацию

Закрыть

Страница 1 из 25

17:20:38 08.11.2021

Поиск инцидентов по IP-адресу

ViPNet TIAS



Мониторинг

Инфопанель

Инциденты 0

События ^

Сетевые

Узловые

Отчеты

Управление

Инфраструктура

Сетевые события

IDS NS, xFirewall



Категории событий

Источники ↻

Уров... Пра... Кол... IP-адрес ист... IP-адрес се...

Низкий	Maliciou...	16	91.26.97.3	
Низкий	Maliciou...	16	91.26.144.81	
Низкий	Maliciou...	16	91.26.152.195	91.26.144.81
Высо...	A host is...	3	192.168.78.14	

Инциденты



Пораженный актив 192.168.78.14

IP-адрес источника 192.168.78.14

<input type="checkbox"/> Статус	Пользов...	Дата и время обн...	Рейтинг	Поражен...
<input type="checkbox"/> Не обработан		08.11.2021 16:09:29	10	192.168.78.14
<input type="checkbox"/> Не обработан		08.11.2021 16:24:01	10	192.168.78.14



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.



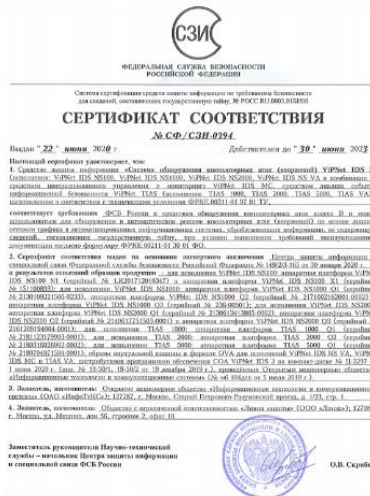
Сертификация

Сертифицированные версии

COA класса B

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



COB 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



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?



- 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.