ViPNet TIAS

Программно-аппаратный комплекс
ViPNet Threat Intelligence Analytics System

infotecs

www.infotecs.ru

VIPNET TIAS — ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС ДЛЯ АВТОМАТИЧЕСКОГО ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ОСНОВЕ АНАЛИЗА СОБЫТИЙ

ОБЩИЕ СВЕДЕНИЯ

На десятки тысяч событий, регистрируемых сенсорами обнаружения вторжений приходятся единицы реальных инцидентов информационной безопасности.
ViPNet TIAS в автоматическом режиме анализирует весь поток входящих событий от сенсоров, находит взаимосвязи между ними и выявляет действительно значимые угрозы, являющиеся инцидентами информационной безопасности.

Автоматическое выявление инцидентов информационной безопасности в ViPNet TIAS строится на основе комбинирования двух методов:

- Сигнатурный метод анализа, основанный на использовании метаправил выявления инцидентов.
- Математическая модель принятия решений, разработанная на основе статистического анализа угроз с использованием методов машинного обучения.

База метаправил и математическая модель принятия решений разрабатывается и обновляется экспертами компании «Перспективный мониторинг» на основе знаний об угрозах, получаемых в результате анализа инструментов и техник выполнения атак — Threat Intelligence.

ВОЗМОЖНОСТИ

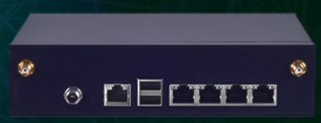
ViPNet TIAS позволяет осуществлять мониторинг угроз информационной безопасности и оперативно реагировать на них в случаях, когда:

- Не хватает квалифицированного персонала.
- Не хватает времени на отработку каждого сообщения о событии информационной безопасности.
- Отсутствуют инструменты, позволяющие автоматизировать процесс анализа событий и расследования причин возникновения угроз.

Дополнительно ViPNet TIAS предоставляет возможности:

- Создавать отчеты по событиям и инцидентам.
- Выгружать информацию об инцидентах во внешние системы, в том числе в систему ГосСОПКА.

ViPNet TIAS 1000



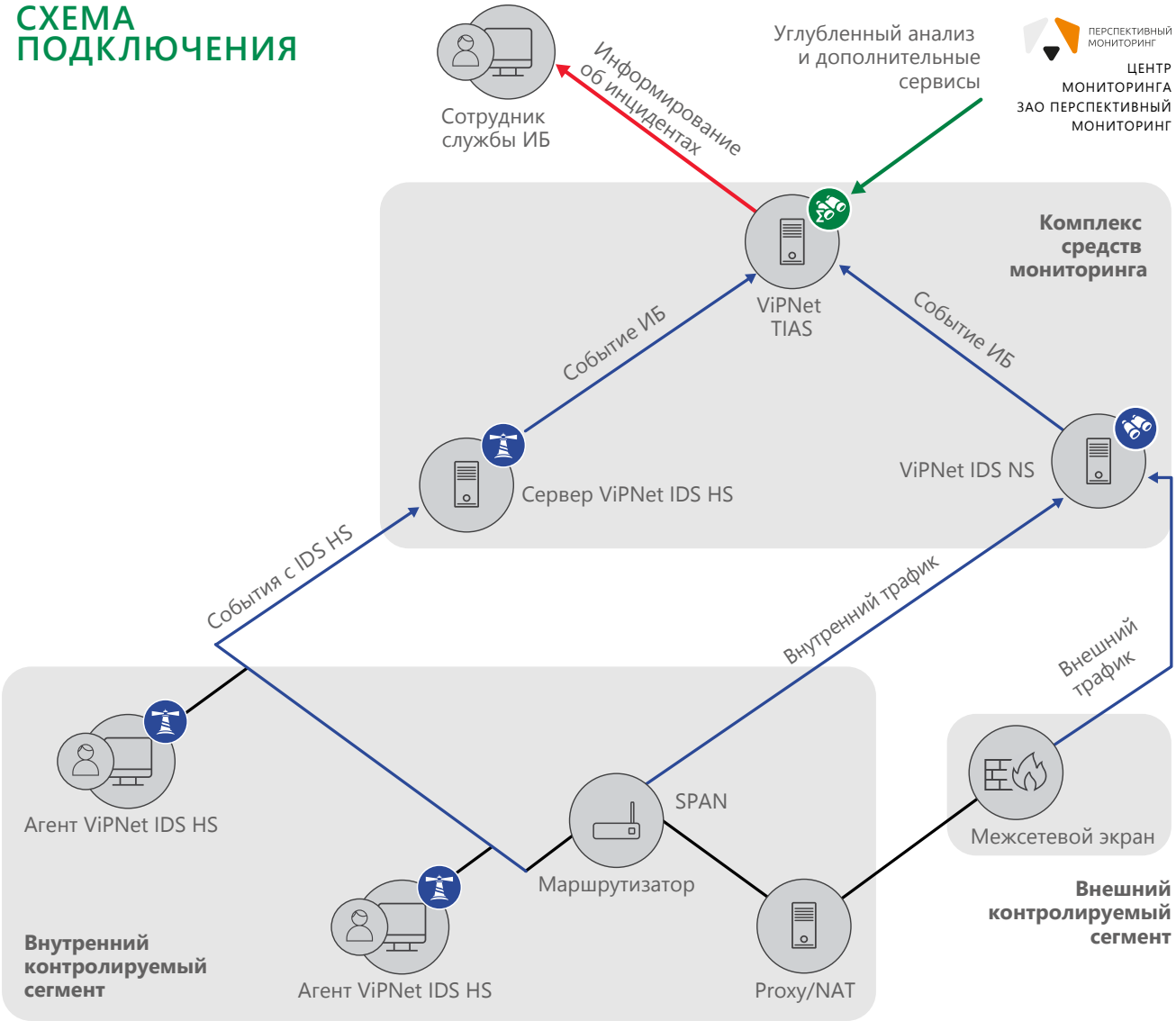
ViPNet TIAS 100

ViPNet TIAS 2000/5000

СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

1. Системы обнаружения вторжений ViPNet IDS сетевого и хостового уровня генерируют события информационной безопасности.
2. ViPNet TIAS автоматически собирает информацию о событиях с подключенных к нему сенсоров ViPNet IDS и серверов ViPNet IDS HS.
3. ViPNet TIAS анализирует события с помощью обученной математической модели и метаправил.
4. В результате анализа одно или несколько нежелательных или неожиданных событий, предполагающих высокую вероятность нарушения работы сети или представляющих угрозу для безопасности, определяются как инцидент информационной безопасности.
5. При обнаружении инцидентов ViPNet TIAS регистрирует данный факт, определяет зависимые события, обогащает их информацией с дополнительных источников и генерирует рекомендации по устранению последствий.
6. ViPNet TIAS с помощью веб-интерфейса и по электронной почте оповещает о произошедшем инциденте.
7. Специалист по информационной безопасности расследует инциденты, устраняет причины и последствия их возникновения в сети.

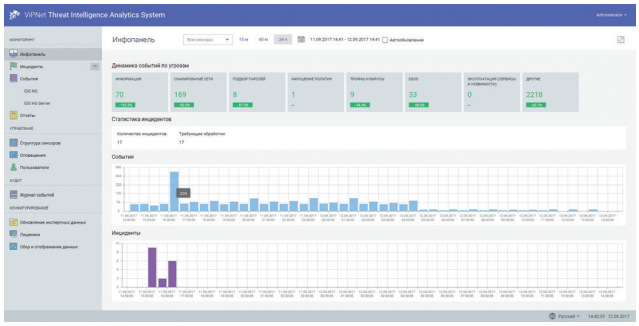
СХЕМА ПОДКЛЮЧЕНИЯ



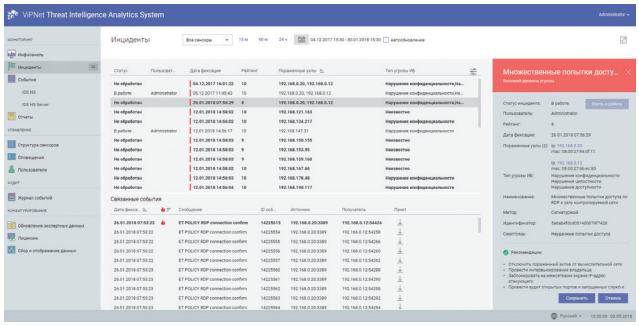
ПРЕИМУЩЕСТВА

- Сокращение среднего времени обнаружения инцидента с 30 до 2 минут по сравнению с ручным анализом событий квалифицированным специалистом.
- Снижение затрат на эксплуатацию системы обнаружения вторжений за счёт сокращения нагрузки на персонал, обслуживающий систему и снижения требований к их квалификации.
- Упрощение реагирования на угрозы информационной безопасности благодаря автоматически формируемым рекомендациям и автоматическому сбору связанных с инцидентом событий.
- Возможность удаленного проведения расследования инцидентов информационной безопасности высококвалифицированными аналитиками компании «Перспективный мониторинг».
- Возможность подключения дополнительных сервисов от компании «Перспективный мониторинг».
- Разворачивание и ввод в эксплуатацию за 1 рабочий день без изменения инфраструктуры заказчика.
- Техническая поддержка специалистами компании «ИнфоТеКС».
- Методологическое сопровождение и консультационные услуги от экспертов компании «Перспективный мониторинг».
- Обучение специалистов в учебном центре «ИнфоТеКС»

Информационная панель ViPNet TIAS



Карточка инцидента



ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

ViPNet TIAS выполняет следующие функции:

- производит сбор событий из источников обнаружения вторжений (ViPNet IDS);
- анализирует поступающие события и автоматически выявляет инциденты информационной безопасности;
- оповещает об инцидентах через веб-интерфейс и по электронной почте;
- предоставляет графический интерфейс для мониторинга угроз информационной безопасности в режиме реального времени;
- предоставляет графический интерфейс для анализа при расследовании инцидентов;
- предоставляет инструменты для самостоятельного анализа событий и выявления инцидентов;
- позволяет создавать отчеты о событиях и выявленных инцидентах.

МОДЕЛЬНЫЙ РЯД

	ПАК ViPNet TIAS 100	ПАК ViPNet TIAS 1000	ПАК ViPNet TIAS 2000	ПАК ViPNet TIAS 5000
Производительность	до 300 событий ИБ за 1 секунду до 5 Гб информации в сутки до 1 IDS NS до 1 IDS HS (100 агентов) Нет модуля отчётности	до 1000 событий ИБ за 1 секунду до 15 Гб информации в сутки до 10 IDS NS до 1 IDS HS (1000 агентов)	до 2000 событий ИБ за 1 секунду до 30 Гб информации в сутки до 20 IDS NS до 2 IDS HS (2000 агентов)	до 5000 событий ИБ за 1 секунду до 50 Гб информации в сутки до 50 IDS NS до 5 IDS HS (5000 агентов)
Форм-фактор	Desktop	1U	1U	1U
Размер	185.4 x 44 x 137.1	380*430*43.4	383*444*44	383*444*44
Платформа	Lanner NCA-1210	Asus RS100-E8-PI2	Asus RS400-E8-PS2-F	Asus RS400-E8-PS2-F
ЦПУ	Intel® Atom™ processor C2558	Intel Core i3-4360	2x Intel Xeon E5-2609v4	2x Intel Xeon E5-2620v3
RAM	16Gb DDR4	16Gb DDR4	32Gb DDR4	64Gb DDR4
HDD	500Gb	1Tb	1Tb (RAID1)	2Tb (RAID1)
LAN	4x RJ45 1G	4x RJ45 1G	4x RJ45 1G 2x SFP+ 10G	4x RJ45 1G 2x SFP+ 10G
БП (Вт)	36W Power Adaptek	250Вт (AcBel FSB009)	1x500 (Delta DPS-500AB-5 B)	1x500 (Delta DPS-500AB-5 B)

СЕРТИФИКАЦИЯ

Ведутся работы по сертификации продукта:

- по требованиям ФСТЭК на отсутствие НДВ (4 уровень) и на соответствие ТУ;
- в составе ViPNet IDS 3 на соответствие требованиям ФСТЭК к системам обнаружения вторжений;
- в составе ViPNet IDS 3 на соответствие требованиям ФСБ к системам обнаружения атак.

СМЕЖНЫЕ ПРОДУКТЫ

- ViPNet IDS NS и ViPNet IDS HS — передают события информационной безопасности для анализа в VIPNet TIAS.
- ViPNet IDS MC — управление обновлениями экспертных данных и структурой сенсоров

infotecs

ОАО «ИнфоТеКС», 127287, Москва, Старый ПетровскоРазумовский проезд, 1/23, стр. 1

+7 495 7376192, 8 800 2500260 (бесплатный звонок по России)

+7 495 7377278

soft@infotecs.ru, hotline@infotecs.ru

www.infotecs.ru

ViPNet Virtual Private Network

infotecs.ru/f21

Ваше впечатление от листовки: