

техно infotecs
2019 Фест

ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

12
09 2019

ViPNet IDS NS -
классический сетевой
сенсор с
отечественной базой
решающих правил



ViPNet IDS NS

ViPNet IDS

Details

Appliance

Virtual appliance

Intrusion detection system

IDS 100

IDS 1000

IDS 2000

IDS VA

Signature and Heuristic analysis

Events notification

Collection intrusion information

SIEM Integration



ViPNet IDS Network Sensor

- ✓ **Сигнатурный и эвристический методы анализа**
 - анализ заголовков протоколов и содержимого сетевых пакетов на основе правил
 - отслеживание отклонений отдельных параметров сетевого трафика от эталонной модели

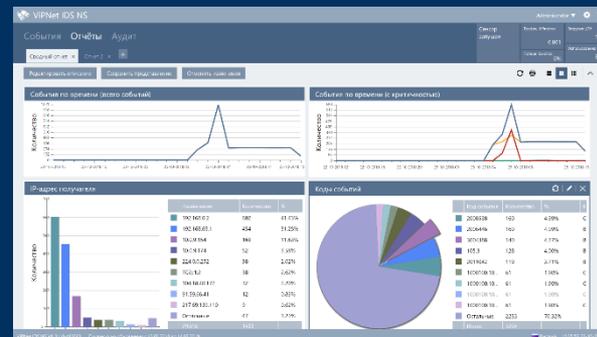
✓ **Отображение**

- дашборды в режиме реального времени
- таблицы с возможностью поиска
- отчеты и графики

✓ **Оповещение**

- web-интерфейс,
- e-mail,
- Syslog

✓ **Служебные функции**



События | Отчеты | Аудит

Живой мониторинг | Поиск событий | Сигнатурный анализ файлов

Выберите фильтр

11 131 526	8 877 602	1 793 928	459 996
Всего событий за год	Высокая критичность	Средняя критичность	Низкая критичность

Критичность	Дата/время	Код события	Кол.	Описание	Класс
Средняя	2018-10-23 14:54:4...	1000100.1000180	1	AD LOW VALUE OF DATA AND UNE...	bad-unknown
Средняя	2018-10-23 14:54:4...	1000100.1000178	1	AD LOW VALUE OF UNKNOWN FLA...	bad-unknown
Средняя	2018-10-23 14:54:4...	1000100.1000176	1	AD LOW VALUE OF DATA TCP/IP UPL...	bad-unknown
Средняя	2018-10-23 14:54:4...	1000100.1000174	1	AD LOW VALUE OF DATA TCP/IP DO...	bad-unknown
Средняя	2018-10-23 14:54:4...	1000100.1000172	1	AD LOW VALUE OF ACK TCP/IP FLAG...	bad-unknown
Средняя	2018-10-23 14:54:4...	1000100.1000170	1	AD LOW VALUE OF ACK TCP/IP FLAG...	bad-unknown
Средняя	2018-10-23 14:54:4...	1000100.1000168	1	AD LOW VALUE OF FIN TCP/IP FLAG...	bad-unknown
Средняя	2018-10-23 14:54:4...	1000100.1000166	1	AD LOW VALUE OF FIN TCP/IP FLAG...	bad-unknown
Средняя	2018-10-23 14:54:4...	1000100.1000164	1	AD LOW VALUE OF SYN TCP/IP FLAG...	bad-unknown
Средняя	2018-10-23 14:54:4...	1000100.1000162	1	AD LOW VALUE OF SYN TCP/IP FLAG...	bad-unknown

ViPNet IDS NS VA 3.1.0-413063 | Подписка на обновление с 13.03.2018 до 14.03.2019

Производительность ViPNet IDS NS 3

Исполнение	IDS100	IDS1000	IDS2000
IDS, 1518 byte UDP, 0.1 % attack (Mbps)	140	950	6 000
IDS, 1518 byte TCP, 0.1 % attack (Mbps)	140	950	6 000
IDS, 64 byte UDP, 0.1 % attack (Packets Per Second))	76 000	780 000	870 000

Откуда сигнатуры



Сигнатуры от ЗАО «ПМ»

почти 10 тыс. собственных сигнатур



220 тыс. хешей вредоносных



Страна происхождения - Россия



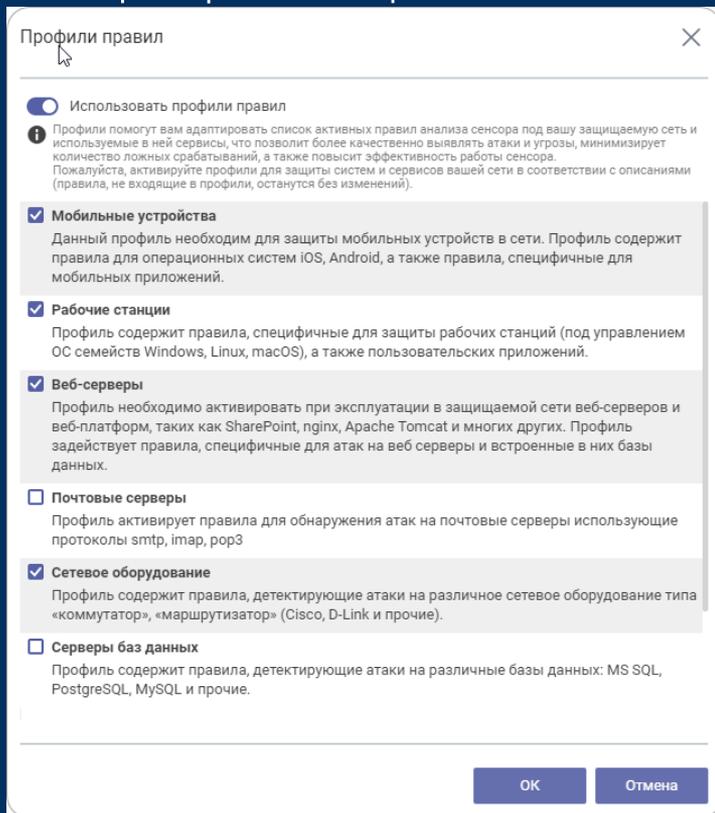
Как это работает





Как оптимизировать набор
сигнатур

Профили правил



Профили правил — это наборы системных правил, направленные на обнаружение атак на определенные сервисы, функционирующие в защищаемой сети.



Malware Detection

Система выявления вредоносного ПО -ViPNet Malware Detection

Выявление в трафике файлов в HTTP, FTP трафике

Анализ полученных файлов на наличие в них вирусов

Уведомление Администратора о выявленном вредоносном ПО

Сохранение файла в базе данных

В чем польза Malware Detection

Это не замена антивируса – это помощник любого антивирусного решения.

Malware Detection выявляет в потоке то зловредное ПО, которое еще неизвестно/не лечится антивирусами

Выявление происходит до момента прибытия malware на точку заражения – предупрежден, значит вооружен





ТЕХНО infotecs
2019 Фест

Спасибо
за внимание!