ТЕХНО 2019 infotecs ФЕСТ

ТЕХНИЧЕСКАЯ КОНФЕРЕНЦИЯ

12 09 2019

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

ViPNet IDS NS

Система обнаружения атак

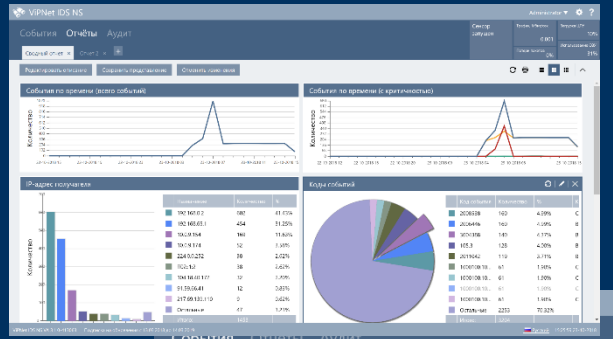
ViPNet IDS

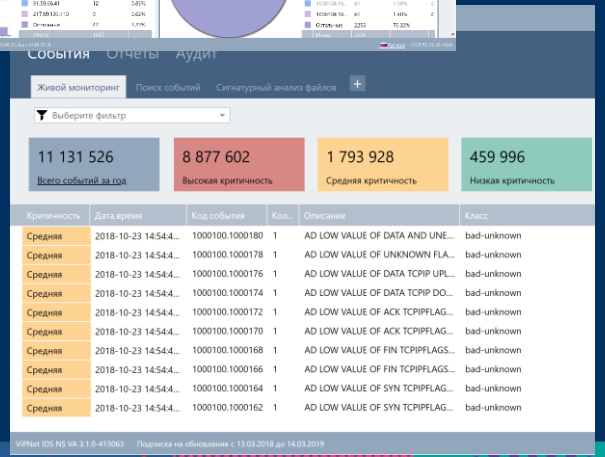
Details	Appliance	Virtual appliance
Intrusion detection system	IDS 100 IDS 1000 IDS 2000	IDS VA
Signature and Heuristic analysis Events notification Collection intrusion information SIEM Integration		

ViPNet IDS Network Sensor

ТЕХНО infotecs 2019 Фест

- ✓ **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**
  - дэшборды в режиме реального времени
  - таблицы с возможностью поиска
  - отчеты и графики
- ✓ **Оповещение**
  - web-интерфейс,
  - e-mail,
  - Syslog
- ✓ **Служебные функции**





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

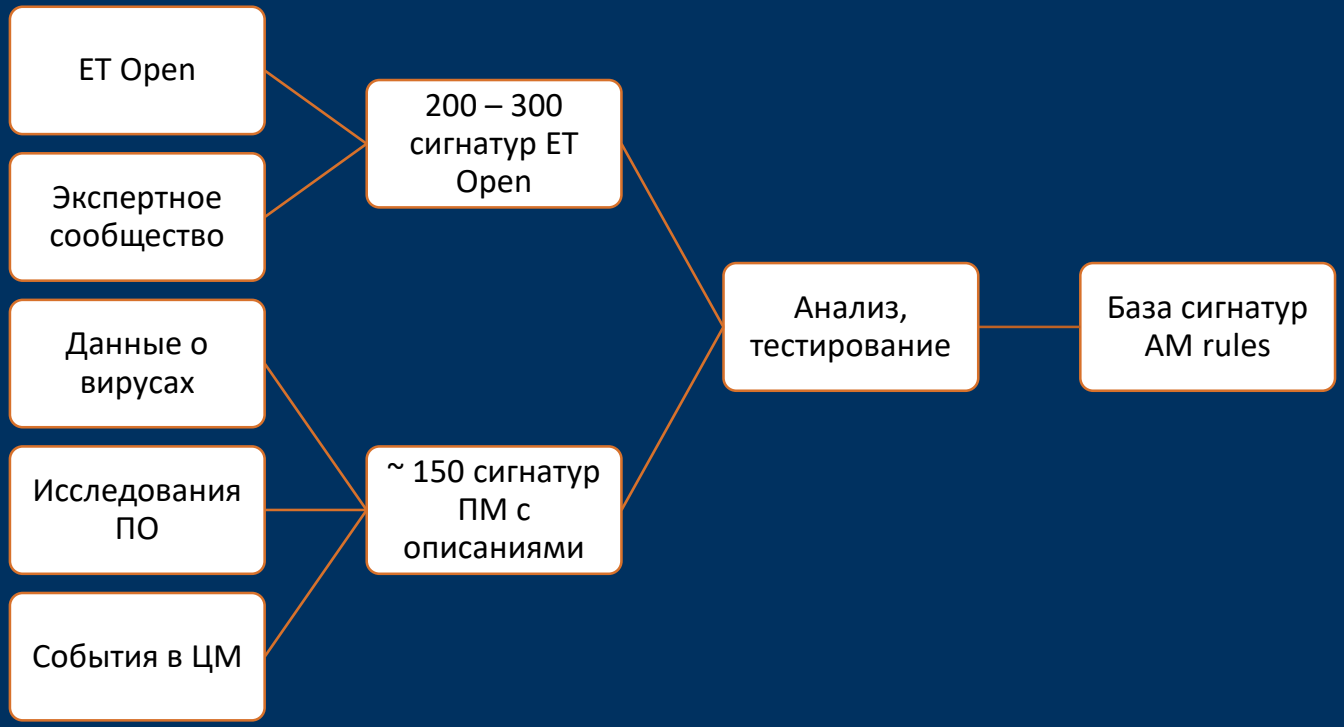
Сигнатуры от ЗАО «ПМ»

почти 10 тыс. собственных сигнатур

220 тыс. хешей вредоносов

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

Спасибо
за внимание!