

Подключение нового сегмента сети на мониторинг за 30 минут

Светлана Старовойт
Руководитель продуктового направления

техно infotecs
2022 Фест

ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Немного теории

Решение 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 ИБ в сетевом трафике



ViPNet IDS HS

- Выявлять события ИБ и аномалии поведения на конечных узлах

Система управления ViPNet IDS MC

The screenshot displays the ViPNet IDS MC management interface. The top section, titled 'Зарегистрированные устройства' (Registered devices), shows a list of devices with columns for 'Наименование' (Name), 'Описание' (Description), 'Платформа' (Platform), and 'Версия ПО' (Software version). The list includes devices like ALLEREY and CLOMOT. The bottom section, titled 'Мониторинг' (Monitoring), shows the system status as 'Опасное состояние' (Dangerous state) and lists several tasks with their counts and status:

Task	Count	Unit	Status
Резервное копирование не выполнялось	14	дней	Warning
Задачи, выполненные с ошибками	23	задачи	Warning
Неразосланные обновления ПО	2	обновления	Warning
Неразосланные обновления баз правил	12	запросов	Warning
Неразосланные обновления баз Malware detection	2	запроса	Warning
Система в работоспособном состоянии			Success

- Управление пользователями и инфраструктурой решения TDR
- Разворачивание и инициализация устройств
- Настройка параметров работы устройств
- Управление обновлениями БРП, Malware, ЭД
- Управление лицензиями устройств
- Управление обновлениями ПО
- Мониторинг состояния устройств TDR

Ролевой доступ в ViPNet IDS MC

Управление функциями IDS MC

Управление устройствами

Главный администратор

Главный администратор устройства

Главный администратор для
локального доступа

Администратор устройства

Администратор безопасности

Пользователь устройства

Администратор

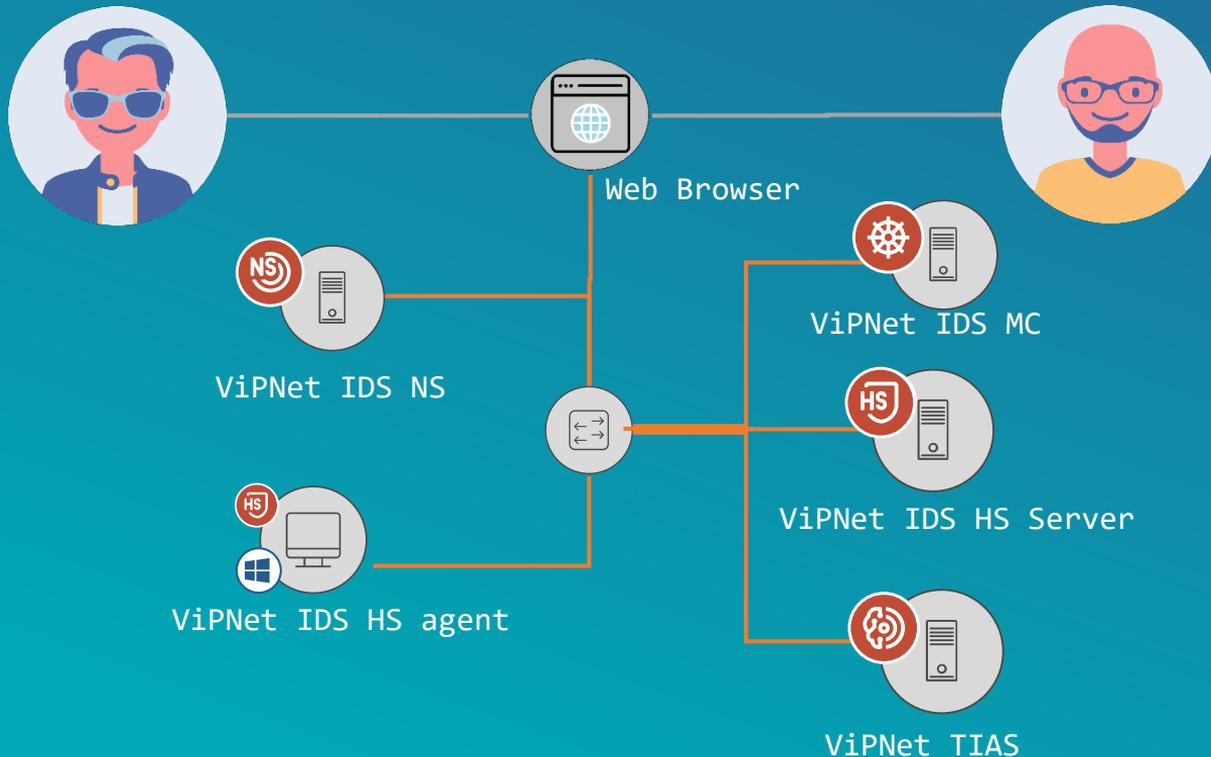
Аудитор

Мастер-класс

Описание стенда и сценария

Администратор филиала

Администратор головного офиса



1. Подключение на обслуживание новой организации (контролируемого сегмента сети)
2. Добавление в организацию нового сенсора IDS NS
3. Подключение агента IDS HS
4. Настройка работы сенсоров из IDS MC
5. Настройка автоматических обновлений
6. Мониторинг состояния устройств

ТЕХНО infotecs
2022 ФЕСТ

Спасибо за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



t.me/infotecs_news



rutube.ru/channel/24686363