

Подключение нового сегмента сети на мониторинг за 30 минут

Светлана Старовойт
Руководитель продуктового направления



техно infotecs
2023 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 web interface. The top section, titled 'Зарегистрированные устройства' (Registered Devices), shows a list of devices with columns for Name, Description, Platform, and Version. Two devices are listed: ALLEREY and CLOMOT, both running VIPNet IDS NS VA 3.5.0-509983. Below this, the 'Мониторинг' (Monitoring) section shows the system status as 'Опасное состояние' (Dangerous state). A list of alerts includes: 'Резервное копирование не выполнялось' (Backup not performed) for 14 days, 'Задачи, выполненные с ошибками' (Tasks completed with errors) for 23 tasks, 'Неразосланные обновления ПО' (Unsent software updates) for 2 updates, 'Неразосланные обновления баз правил' (Unsent rule base updates) for 12 requests, and 'Неразосланные обновления баз Malware detection' (Unsent Malware detection base updates) for 2 requests. The final status is 'Система в работоспособном состоянии' (System in operational state).

- 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

Главный администратор

Главный администратор
для локального доступа

Администратор безопасности

Администратор

Аудитор

Управление устройствами

Главный администратор устройства

Администратор устройства

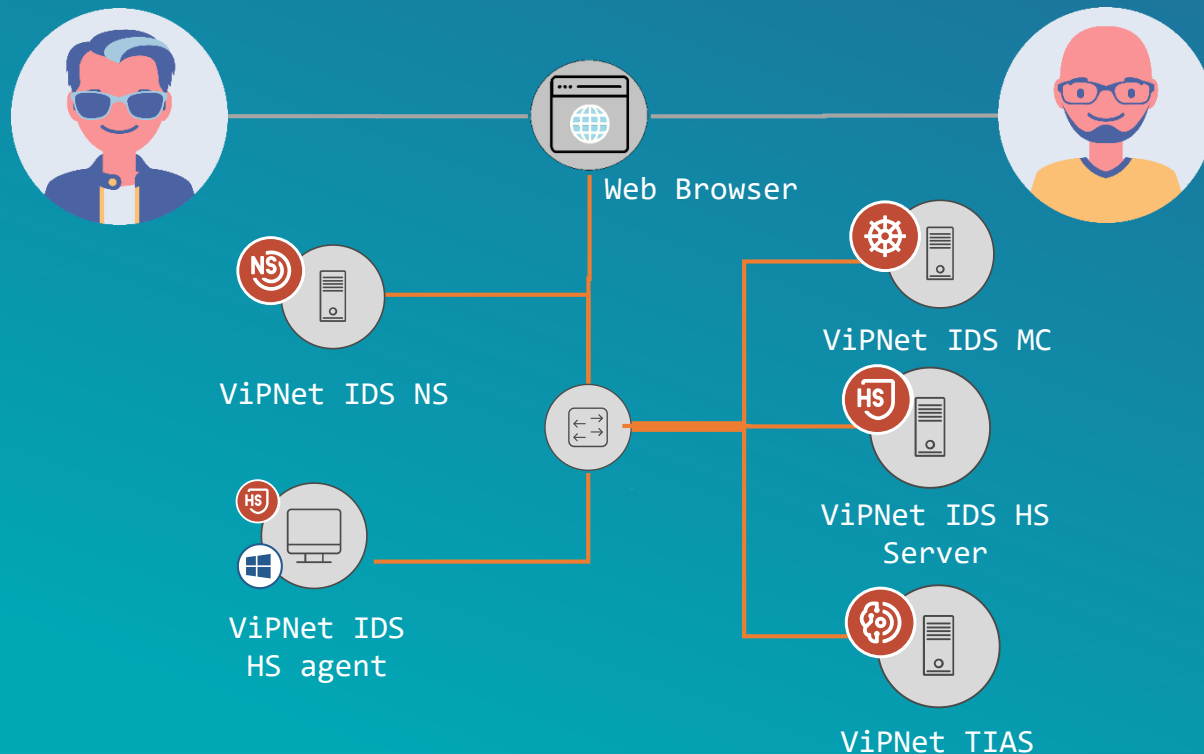
Пользователь устройства

Мастер-класс

Описание стенда и сценария

Администратор филиала в г. Хабаровск

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



Спасибо за внимание!

Подписывайтесь на наши соцсети



vk.com/infotecs_news



https://t.me/infotecs_official



rutube.ru/channel/24686363