Обзор обязанностей

Обзор обязанностей администратора

Ежедневно

1. Проверить события и критичные PROBLEM.
2. Просмотреть аудит на SECURITY_ALERT / неудачные логины.
3. Убедиться, что ключевые агенты online.

Еженедельно

- Approve новых пользователей (`PENDING`).
- Проверить версию агентов и при необходимости запланировать update.
- Проверить уведомления (тестовый PROBLEM или webhook).

При изменениях инфраструктуры

- Обновить настройки: ICMP, retention, TTL сессий.
- Настроить безопасность и уведомления.
- Завести шаблоны / discovery под новые сети.

Роли

Роль	Типичные задачи
ADMIN	Всё ниже + запись
INFOSEC	Аудит, сессии, настройки (чтение), эскалации ИБ
OPERATOR	Эксплуатация узлов/событий без admin UI
VIEWER	Только просмотр

Подробнее: Роли, Пользователи.