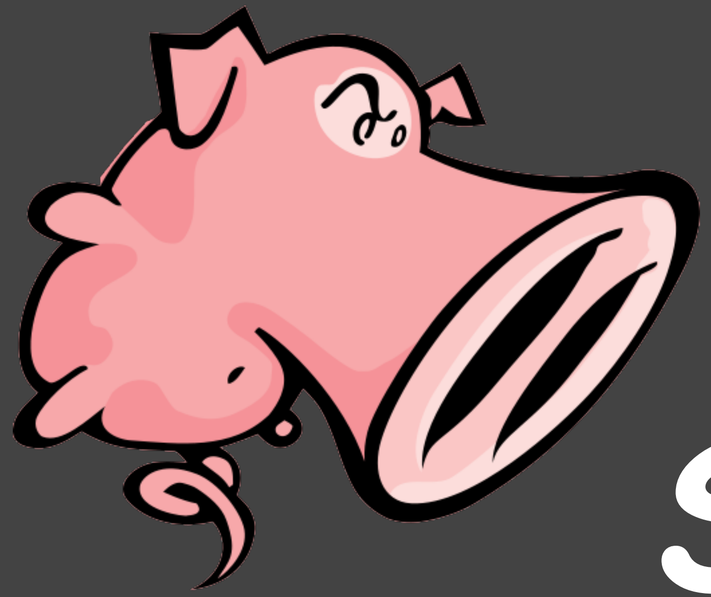


SNORT

Что это и для чего?

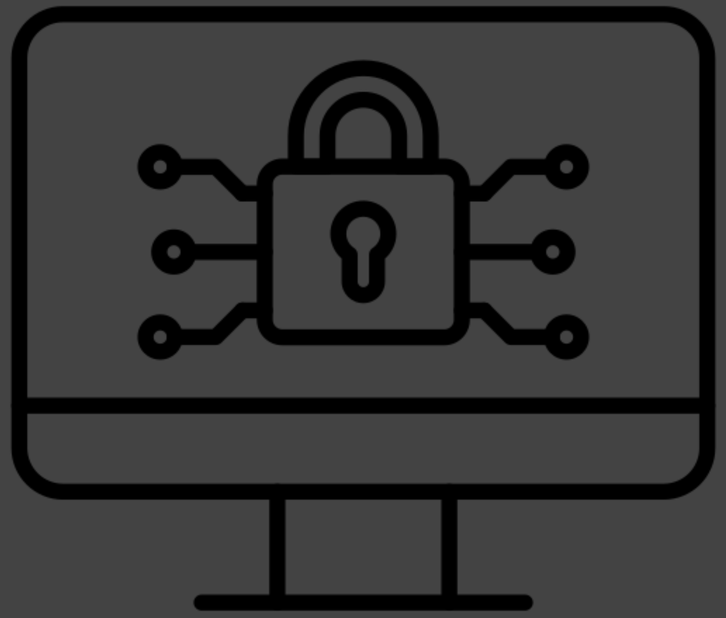
Система для обнаружения и предотвращения вторжений (IDS/IPS)

IDS - Intrusion detection system

IPS - Intrusion Prevention System

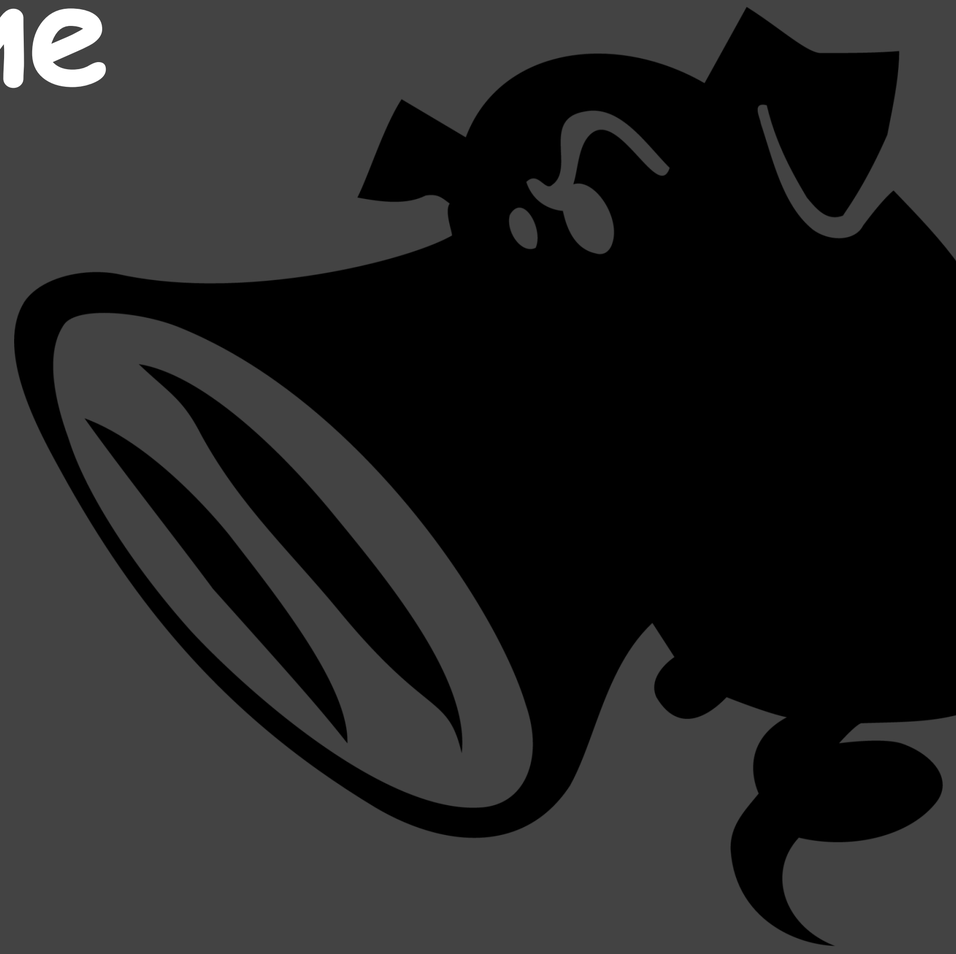
Основной функционал

- Обнаружение вторжений (IDS)
- Предотвращение вторжений (IPS)
- Логирование и анализ трафика
- Отчёты и уведомления
- Гибкость настроек



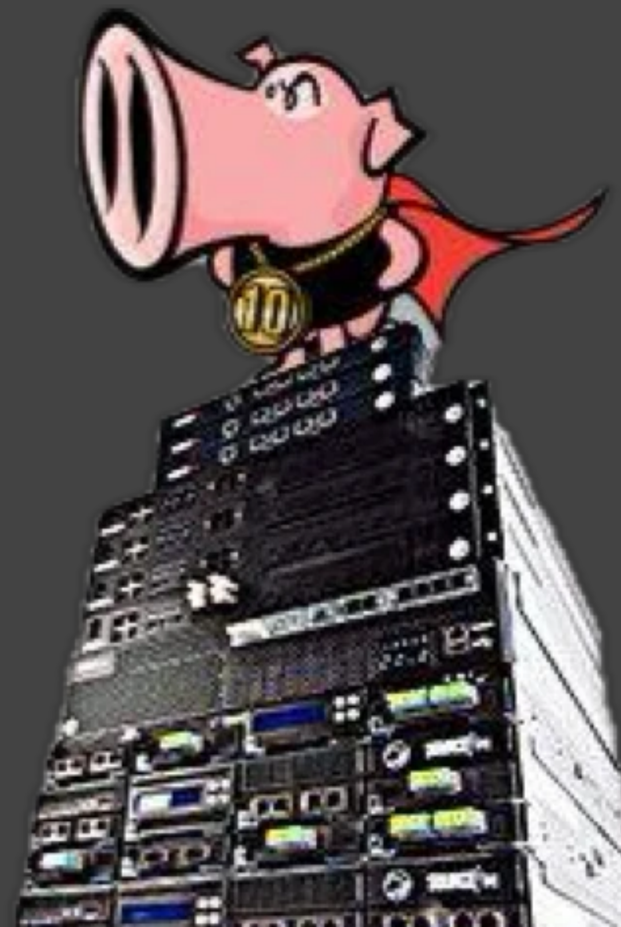
Применение

- Корпоративные сети
- Учебные заведения
- Провайдеры и дата-центры
- Малый и средний бизнес
- Личные и домашние сети



Преимущества

- Бесплатный и открытый
- Гибкость настроек и интеграции
- Поддержка различных сетевых протоколов



Недостатки

- Зависимость от сигнатур для обнаружения новых атак
- Высокая нагрузка на сеть и оборудование
- Требуются знания для настройки кастомных правил

Заключение и немного про инфобез

https://clck.ru/3EZrni