Критерии полезности использования SOC в организации

Константин Саматов

Security Operation Center (SOC) – Центр мониторинга и реагирования на инциденты информационной безопасности (компьютерные атаки)

Мониторинг информационной инфраструктуры

Реагирование на атаки и инциденты

SOC может оказывать услуги

Внешний заказчик

- ROI
- Оборот
- Рентабельность
- Размер прибыли

Внутренний заказчик

Внешние потребители - иные ГРИИБ (ISIRT): НКЦКИ, ФинЦЕРТ

Основные функции SOC

Проактивная защита:

1. Мониторинг информационной инфраструктуры
2. Обнаружение компьютерных атак
3. Реагирование на компьютерные атаки
4. Кибербразведка

Критерии полезности

- **Время обнаружения КА**
- **Время реагирования на КА**
- **Ценность применяемых фидов**

Реактивная защита:

5. Выявление инцидентов
6. Реагирование и расследование инцидентов

Критерии полезности

- **Время обнаружения и реагирования**
- **Количество пострадавших ИР**
- **Соотношение понесенных и предотвращенных потерь**
- **Реализация рекомендаций постинцидентной обработки**

Спасибо за внимание!

Константин Саматов