Ankey ASAP

Платформа расширенной аналитики безопасности

Управляйте информационной безопасностью с помощью искусственного интеллекта

GIS
ГАЗИНФОРМ СЕРВИС

Отдел продаж:
+7 (812) 677-20-53
sales@gaz-is.ru

Демоверсия:
Ankey ASAP
www.gaz-is.ru

Ankey ASAP

Программный комплекс расширенной аналитики событий и инцидентов информационной безопасности с функциями UEBA

Безопасность в кратчайшие сроки

1. **Бессигнатурные методы, основанные на поведенческой аналитике (UEBA)**
2. **Создание профиля функционирования (цифровая тень объекта)**
3. **Детектирование аномалий в информационных системах организации**
4. **Обнаружение атаки в начале жизненного цикла**

Выгоды от использования

Для руководства

- Снижение издержек на обеспечение безопасности
- Сокращение риска кибератак
- Повышение репутации компании за счёт устойчивости перед атаками

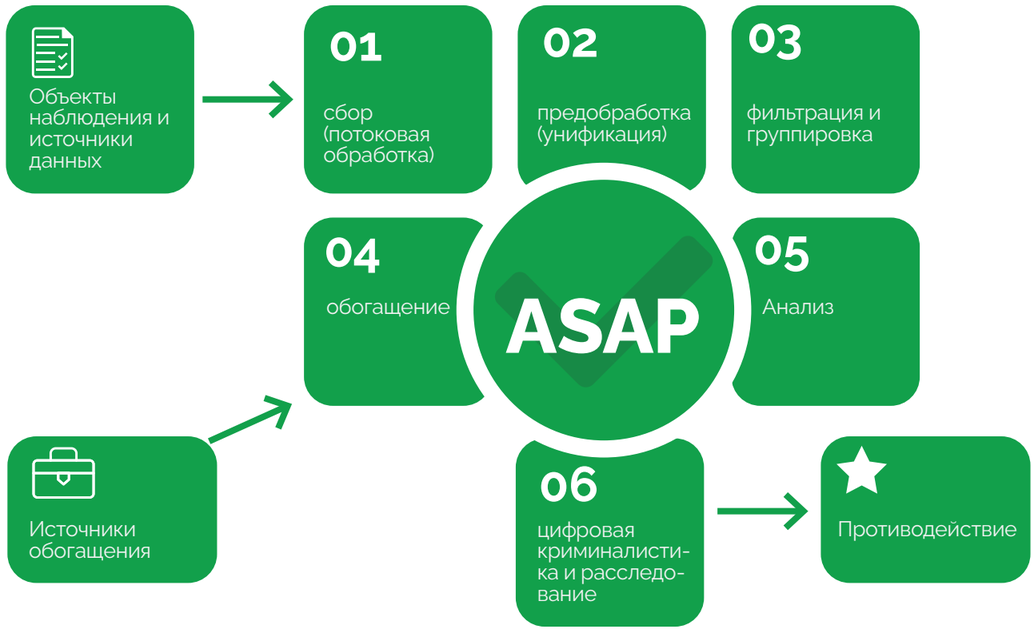
Для SOC

- BI-платформа для выявления признаков, расследования и сбора цифровых доказательств инцидентов ИБ
- Сокращение потока срабатываний за счёт качественной агрегации, алертов
- Выполнение действия регуляторов (по ФСТЭК: ИНЦ.1, 2, 3, 6; АУД. 4, 6, 7, 9)

Для ИБ

- Обнаружение аномалий и атак за счёт расширенной поведенческой аналитики
- Раннее обнаружение действий атакующего в инфраструктуре
- Интеграция с другими СЗИ и единая панель мониторинга

Алгоритм работы



Автоматизация расследования и отчётность

- Работа с информацией о событиях информационной безопасности в разрезе матрицы Mitre ATT&CK и БДУ ФСТЭК
- Снижение требований к компетенциям специалистов первой линии SOC, за счёт группировки алертов на основе скоринга
- База знаний для специалистов по информационной безопасности
- BI-аналитика для управления компьютерными инцидентами

Дальнейшие шаги сотрудничества

Демоверсия → **Пилотное внедрение** → **Расчёт спецификации**