Ankey ASAP: платформа поведенческого анализа пользователей и сущностей с функциями (UEBA)

Ankey ASAP

GIS
ГАЗИНФОРМ
СЕРВИС

Надёжные решения
для безопасности
бизнеса

www.gaz-is.ru

UEBA и Ankey ASAP: Что это?

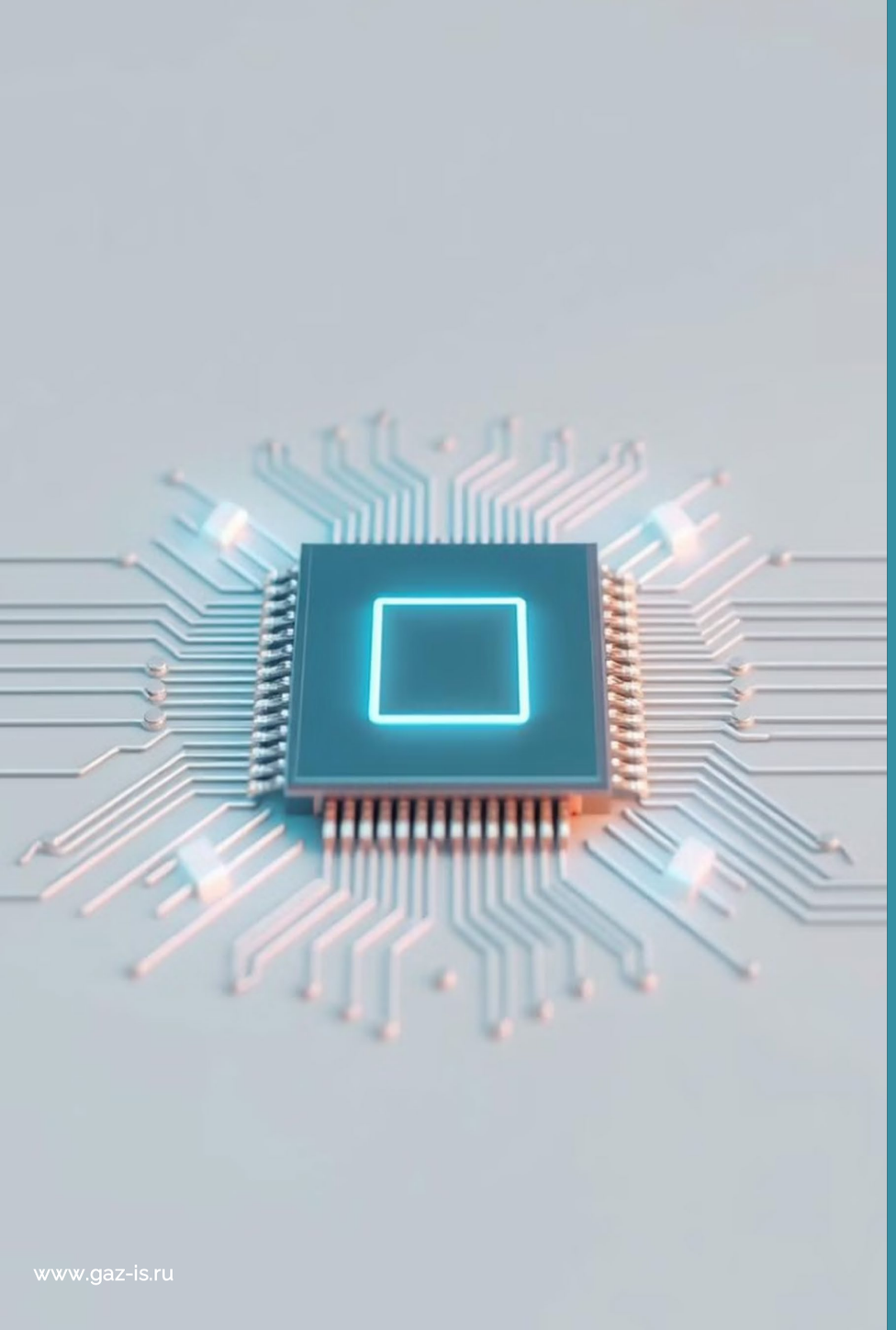
UEBA

User and Entity Behavior Analytics. Технология анализа поведения пользователей и сущностей в инфраструктуре заказчика. Она отслеживает отклонения от нормальной активности, выявляя подозрительные действия и потенциальные угрозы

Ankey ASAP

Платформа класса решений UEBA, разработанная компанией Газинформсервис. Направлена на обнаружение инсайдерских угроз и сложных атак на основе анализа поведения пользователей и сущностей в инфраструктуре заказчика

UEBA помогает в обнаружении угроз, сложных в обнаружении традиционными средствами защиты. Ankey ASAP построен на методах машинного обучения, которые мы применяем в работе наших анализаторов.



В основе ASAP: AI и ML

Ankey ASAP

Выявление деструктивных терминальных команд

При использовании легитимных или встроенных системных утилит алгоритмами обучения с учителем

Интегральная оценка поведения объектов анализа

За отклонение от нормального события назначается скоринговый балл (уровень риска), который определяет алгоритм

Выявление аномалий и классификация

Обученные модели сформировали профилях поведения объекта. После чего алгоритмы могут автоматизировать процесс классификации различных типов поведения, что помогает в определении аномалий

AI и ML позволяют Ankey ASAP адаптироваться к изменениям в поведении пользователей, выявлять сложные угрозы.

Ankey ASAP

Интеграция UEBA в инфраструктуру

1

Подключение источников данных

Для ASAP источниками данных являются SIEM и DLP. Из SIEM мы получаем нормализованные события, за счёт DLP и AD обогащаем контент о действиях пользователей

2

Профилирование объектов анализа

По 10 моделям поведения строится профиль объекта анализа. Далее по созданному профилю определяются отклонения (аномалии)

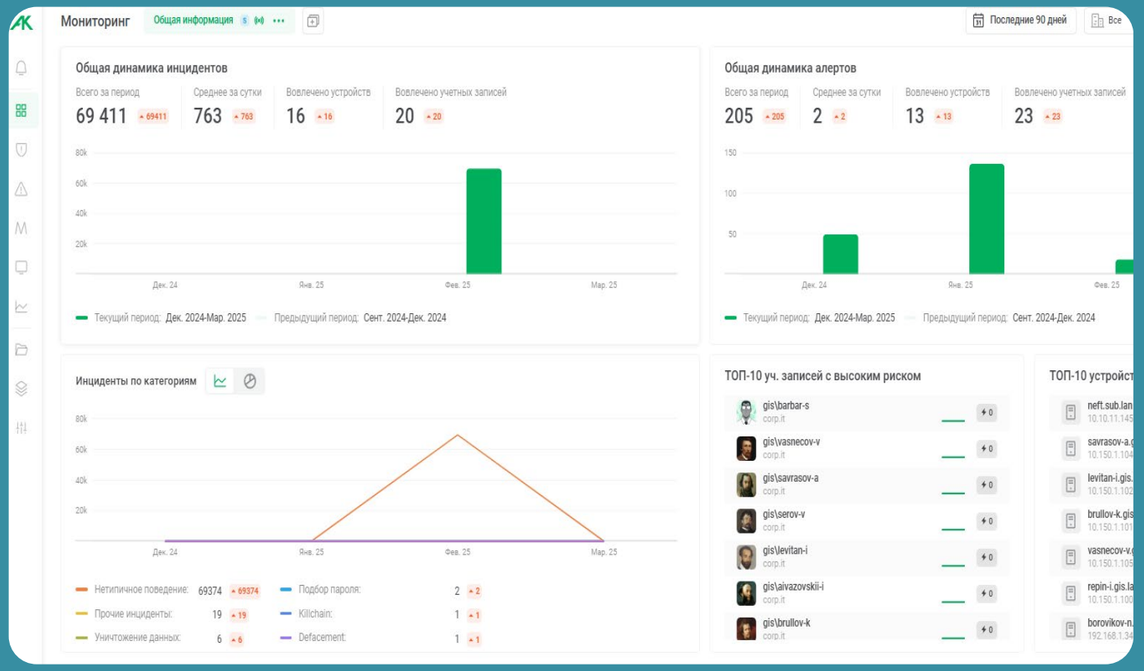
3

Анализ поведения объектов

Выявление цепочек атак и регистрация инцидентов ИБ

Ankey ASAP интегрируется в существующую инфраструктуру – между SIEM и системой реагирования. Это обеспечивает быстрый и эффективный мониторинг безопасности.

Веб-интерфейс Ankey ASAP



Главная панель

Предустановленная библиотека основных метрик безопасности

Анализ поведения

Инструменты для анализа поведения пользователей

Интуитивно понятный веб-интерфейс ASAP обеспечивает удобный доступ к информации и инструментам для анализа и расследования угрозы.

Ankey ASAP

Преимущества использования Ankey ASAP с SIEM и DLP

Усиление защиты

Вместо поиска известных сигнатур атак, UEBA выявляет отклонения от установленных базовых линий поведения

Глубокий анализ

Более глубокий анализ данных и выявление сложных угроз

Ранее распознание атаки

Подсвечивает риски ИБ в начале жизненного цикла атаки

ASAP в сочетании с SIEM и/или DLP обеспечивает комплексную защиту от различных типов угроз, а также позволяет автоматизировать процесс анализа .

Кейсы использования UEBA: от теории к практике

Выявление инсайдерских угроз

Обнаружение сотрудников, собирающих конфиденциальную информацию

Обход DLP-систем

Применение утилит для обхода

Анализ аномального поведения

Реагирование на странные действия

Ankey ASAP

Дальнейшие шаги

1. Демонстрация
2. Пилотирование
3. Договор поставки и внедрение Ankey ASAP

Запрос демоверсии продукта:
Ankey ASAP (gaz-is.ru)