Анализ поведения пользователей (UBA)

Поведение инсайдера

Максим Бузинов

Руководитель исследовательской группы
Центра продуктов Дозор компании «Ростелеком-Солар»

Ростелеком
Солар

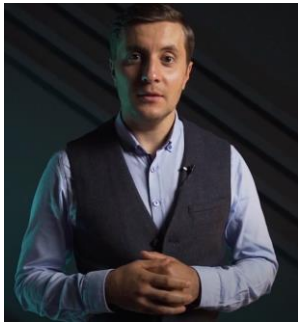
Поведенческая аналитика Solar Dozor UBA

Теоретик

Максим Бузинов

Руководитель исследовательской группы Центра продуктов Дозор компании «Ростелеком-Солар»

Практик



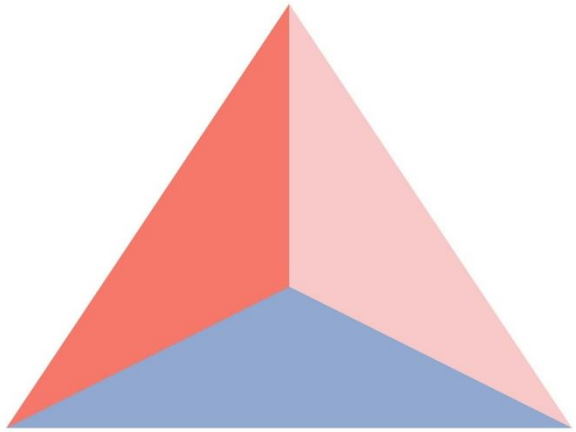
Виталий Петросян

Старший аналитик внедрения компании «Ростелеком-Солар»

Ростелеком
Солар

Принципиальные аспекты поведенческого анализа

- Непрерывное изменение
- Субъективность
- Многогранность



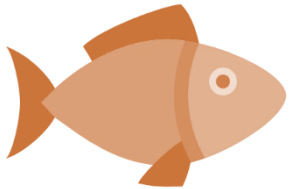
Человек — это текущий процесс...

Карл Роджерс

Ростелеком
Солар

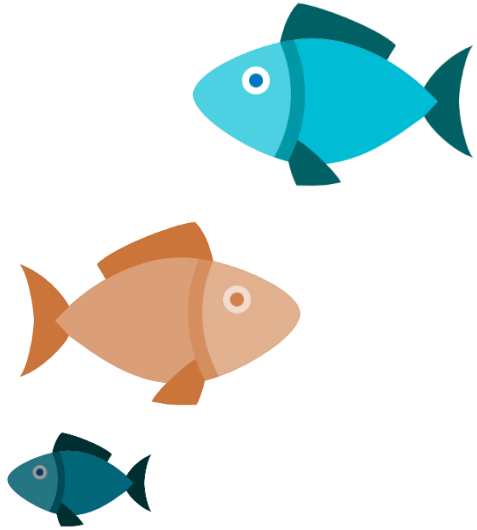
Когда ты один, твое странное поведение вовсе не кажется странным.

Стивен Кинг



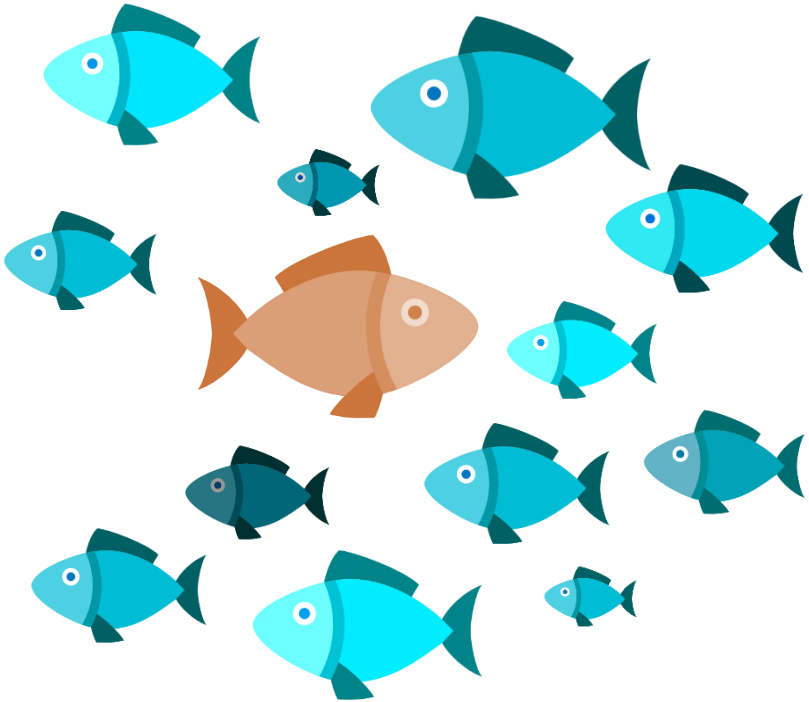
Когда ты один, твое странное поведение вовсе не кажется странным.

Стивен Кинг



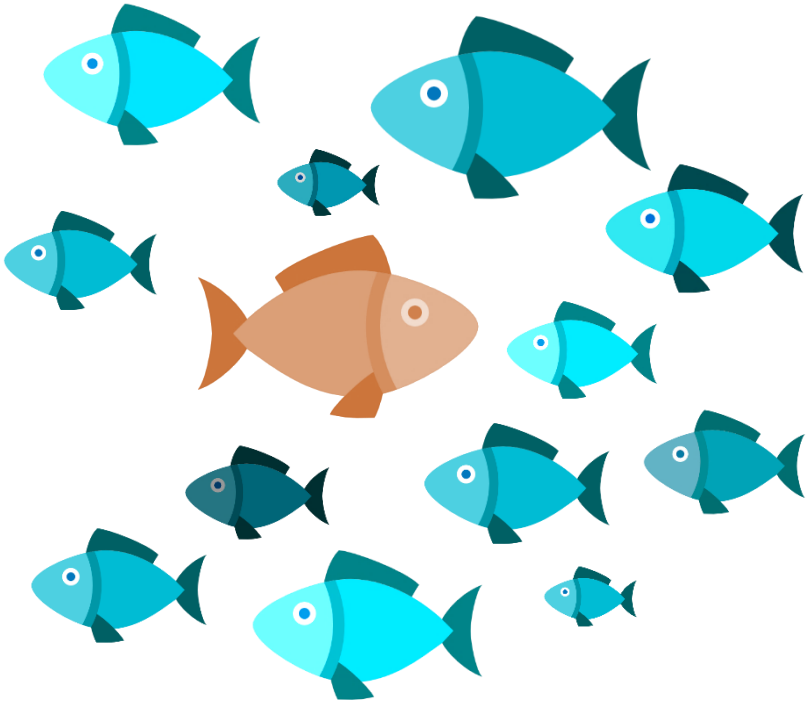
Когда ты один, твое странное поведение вовсе не кажется странным.

Стивен Кинг

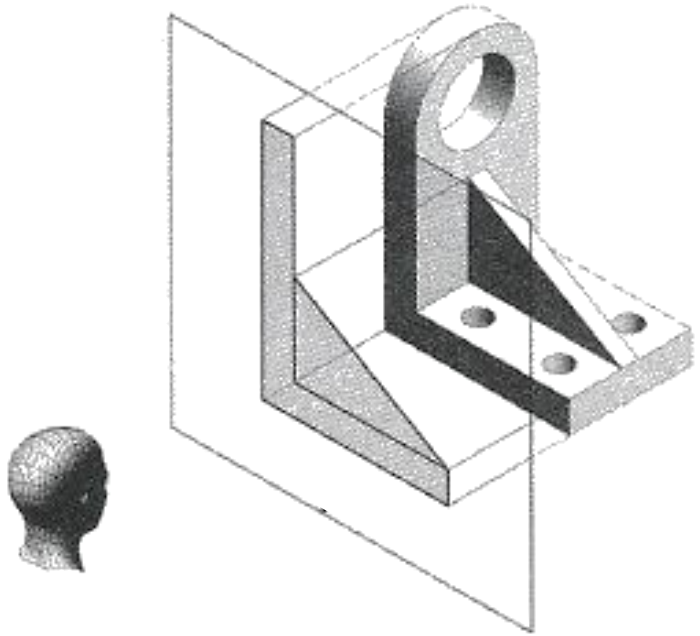


Когда ты один, твое странное поведение вовсе не кажется странным.

Стивен Кинг



Угол зрения имеет значение



Три кита любой UBA

- Мониторинг в реальном времени
- Относительная качественная оценка
- Максимальное число точек зрения

Что внутри Solar Dozor UBA

Математический аппарат

- Теория случайных процессов и теория вероятности
- Теория графов
- Мат. статистика

Алгоритмы

- Machine Learning&Anomaly Detection (LOF mod) ©
- Oriented Graphs. Поиск неизвестных контактов ©
- Oriented Graphs. Определение эго-сетей ©

Базы данных

- ClickHouse (Яндекс)

Интеграция с DLP Solar Dozor

- Лингвистический детектор
- Политики и Досье
- Архив сообщений и событий

Ростелеком
Солар

Преимущества современной UBA системы

Автономность
и самообучаемость

Интеграция
с DLP/SIEM системами

Минимальные затраты
на установку и развертывание

Ценность поведенческой аналитики

1. Выявление уязвимостей, недоступных для традиционных DLP, SIEM систем
2. Прогнозирование и профилактика инцидентов
3. Построение полной картины инцидента

Контакты

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

presale@rt-solar.ru

Ростелеком
Солар