SOLAR

SOLAR DOZOR

USER BEHAVIOR ANALYTICS

Профилактика инцидентов безопасности
с помощью анализа поведения пользователей

W: RT-SOLAR.RU

T: 8 (800) 302-85-23

БЕЗОПАСНОСТЬ С ФОКУСОМ НА ЧЕЛОВЕКЕ

В Solar Dozor уже много лет последовательно реализуется концепция People-Centric Security[1] (PCS). Она предполагает концентрацию внимания службы безопасности на главном источнике угроз — человеке: его фактической роли в коллективе, характере коммуникаций, особенностях работы с защищаемой информацией. Такой подход заметно эффективнее традиционного мониторинга разрозненных данных и низкоуровневых событий.

В DLP-системе Solar Dozor нового поколения (Solar Dozor 7) концепция PCS получила значительное развитие. Главным нововведением стало появление модуля анализа поведения пользователей (User Behavior Analytics, UBA).

Он в реальном времени анализирует историю коммуникаций каждого сотрудника и автоматически формирует личный профиль его нормального поведения.

На основе собранной информации выявляются аномалии в поведении сотрудника. Также модуль UBA ищет работников, попадающих под значимые для безопасности паттерны поведения (группы поведенческих особенностей и аномалий).

[1] «Безопасность с фокусом на человеке». Термин введен международной консалтинговой компанией Gartner, специализирующейся на исследовании ИТ-рынка (ID: GOO250121, Definition: People-Centric Security, 2013 г.)

РЕШАЕМЫЕ ЗАДАЧИ

Профилирование сотрудников по типу поведения

Сравнение сотрудников по типу поведения

Обогащение досье данными о поведении

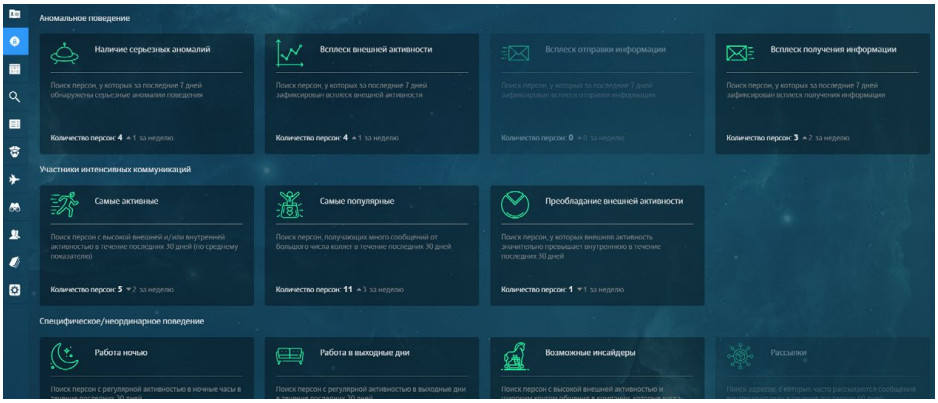
Выявление и контроль групп риска

Выявление круга общения персоны

Профилактика опасных тенденций

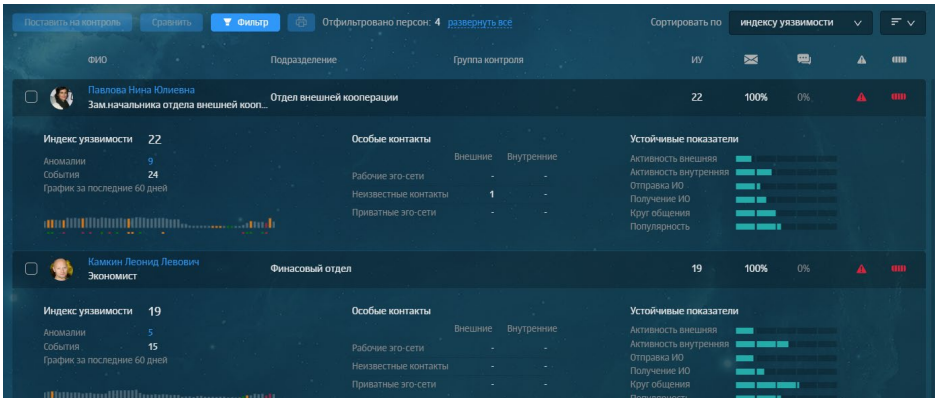
ПАТТЕРНЫ ПОВЕДЕНИЯ И ГРУППОВЫЕ ТЕНДЕНЦИИ

- Контроль и мониторинг групп сотрудников по определенным комбинациям показателей поведения и найденным аномалиям
- Профилактика случайных утечек
- Обнаружение скрытых уязвимостей и рисковых массовых тенденций в поведении
- Выявление уязвимостей в бизнес-процессах



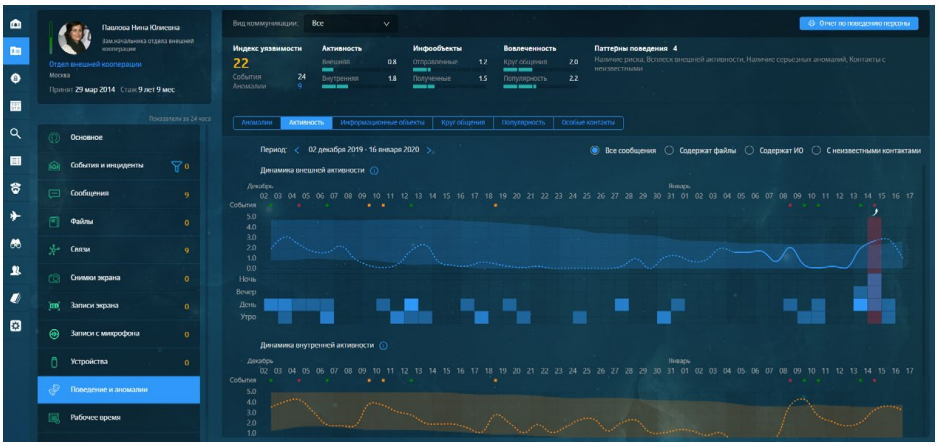
АНАЛИЗ ПОВЕДЕНИЯ ПО ВЫБОРКЕ ПЕРСОН

- Гибкий поиск по множеству критериев поведения
- Сравнительный анализ профилей поведения
- Обнаружение нехарактерного для сотрудника и его должности поведения



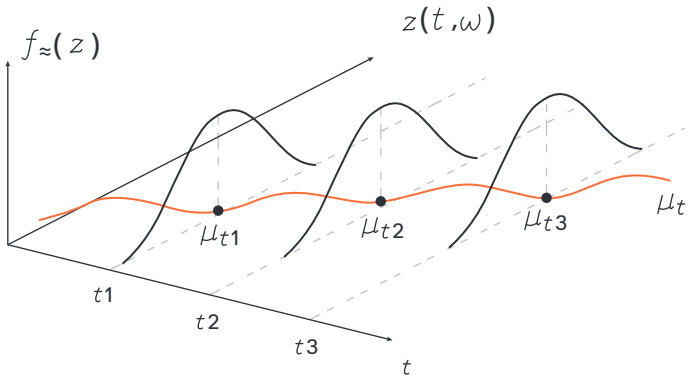
ПОДРОБНАЯ КАРТОЧКА ПОВЕДЕНИЯ

- Поиск аномалий поведения — значительных отклонений от собственной модели поведения сотрудника
- Детектирование особых контактов по уникальным алгоритмам
- Все персональные показатели в каждый момент времени сопоставляются со значениями измерений других персон и имеют единую шкалу



МЕТОДЫ АНАЛИЗА SOLAR DOZOR UBA

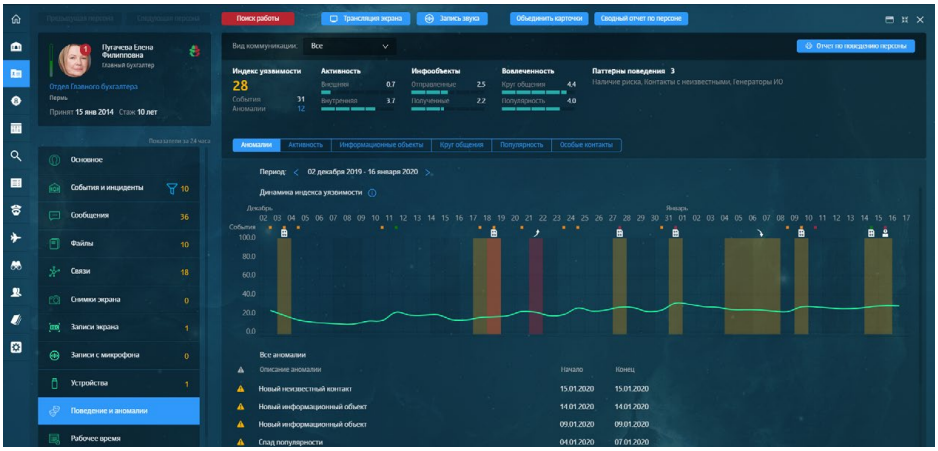
Реализованные в модуле UBA методы анализа и математическая модель поведения уникальны и являются собственной запатентованной разработкой компании «Солар». Используемые алгоритмы относятся к классу Unsupervised Machine Learning (обучение без учителя). Такие алгоритмы не требуют предварительных работ по настройке и адаптации под новые условия эксплуатации.



Представление поведения персоны в виде траектории случайного процесса

ВЗАИМОДЕЙСТВИЕ С SOLAR DOZOR

- Единая консоль управления
- Общие каналы коммуникаций
- Учет политик безопасности
- Анализ движения информационных объектов
- Отображение данных в модуле Dossier
- Анализ контактов сотрудников
- Связь с событиями и инцидентами DLP Solar Dozor
- Для точного анализа достаточно архива коммуникаций за 2 месяца



КЛЮЧЕВЫЕ ОСОБЕННОСТИ

01 Быстрое развертывание

02 Анализ поведения в реальном времени

03 Самоадаптация к параметрам организации

04 Уникальные аналитические инструменты

05 Отсутствие ложных срабатываний

06 Высоткая точность первых результатов

О КОМПАНИИ

20+

решений в продуктовом портфеле

1800+

экспертов по кибербезопасности

600+

комплексных и сервисных проектов в год

850+

организаций под защитой

180+ МЛРД

анализируемых событий ИБ в сутки

SOLAR

T +7 (499) 755-07-70
E info@rt-solar.ru

Центральный офис, 125009,
Москва, Никитский переулок, 7с1