User Behavior Analytics

Профилактика инцидентов безопасности
с помощью анализа поведения пользователей

rt-solar.ru
rt.ru

Ростелеком
Солар

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).

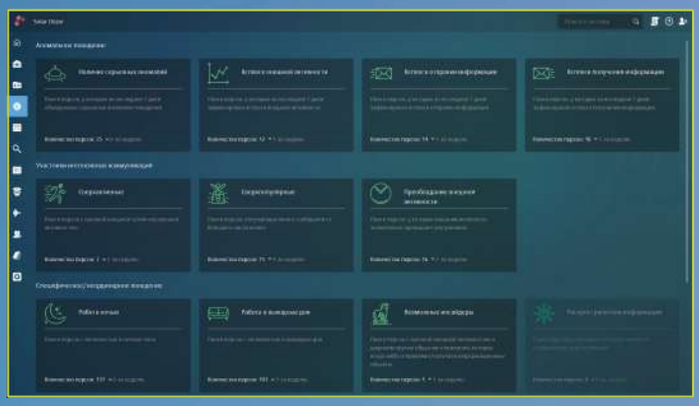
Решаемые задачи

- 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

[1]«Безопасность с фокусом на человеке». Термин введен международной консалтинговой компанией Gartner, специализирующейся на ИТ-рынке (ID: G00250121, Definition: People-Centric Security, 2013 г.)

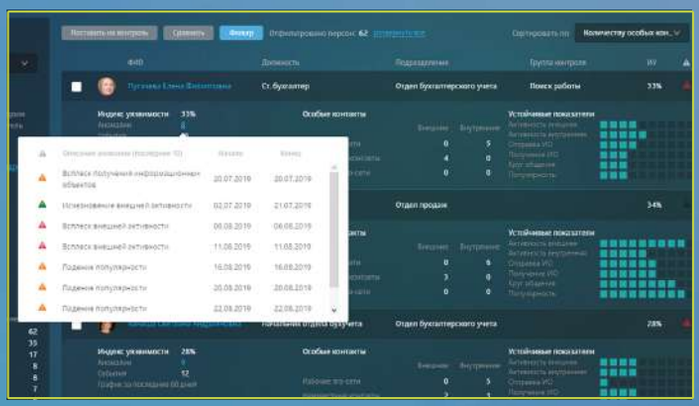
Паттерны поведения и групповые тенденции

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



Анализ поведения по выборке персон

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

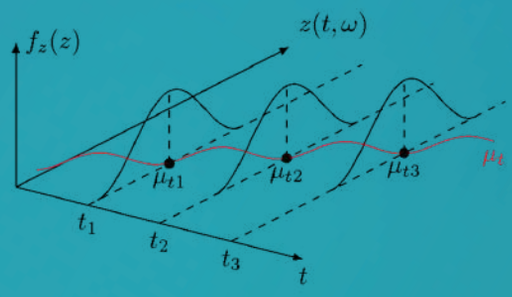


Подробная карточка поведения

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

Методы анализа Solar Dozor UBA

Реализованные в модуле UBA методы анализа и математическая модель поведения уникальны и являются собственной запатентованной разработкой компании «Ростелеком-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 7

- 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

Главное меню Solar Dozor

Ключевые особенности

1. Быстрое развертывание
2. Анализ поведения в реальном времени
3. Самоадаптация к параметрам организации
4. Уникальные аналитические инструменты
5. Отсутствие ложных срабатываний
6. Высокая точность первых результатов

О компании

№1 на рынке сервисов кибербезопасности

900+ экспертов кибербезопасности

70+ клиентов из топ-100 российского бизнеса

24/7 обеспечение кибербезопасности

400+ комплексных и сервисных проектов в год

110+ млрд анализируемых событий ИБ в сутки

Ростелеком Солар

rt-solar.ru presale@rt-solar.ru +7 (499) 755-07-70