Анализ поведения пользователей для обеспечения комплексной безопасности

User Behavior Analytics в DLP

Ростелеком
Солар

Новые тенденции в DLP

Классические задачи

- Защита от утечек
- Контроль корпоративных коммуникаций

Классические пользователи

- Информационная безопасность

Новые области применения

- Выявление групп риска
- Противодействие коррупции
- Выявление внутреннего мошенничества
- Выявление хищения бюджетных средств
- Управление конфликтом интересов
- Профилактика экстремизма и терроризма

Новые пользователи

- Экономическая безопасность
- Физическая безопасность
- Кадровая безопасность
- Комплаенс
- Внутренний контроль

Ростелеком
Солар

User Behavior Analytics (UBA)

Портрет персоны

Рабочая станция:
Используемые приложения
Хранящиеся инф. активы
Создаваемые инф. активы
Считываемые/записываемые файлы
Файлы, копируемые на внешние носители и с внешних носителей

Мессенджеры:
Активность в мессенджерах
Передача инф. активов через мессенджеры

Интернет и внешние ресурсы:
Запросы в интернет
Посещаемые сетевые ресурсы
Входящий и исходящий трафик
Скачиваемые файлы
Публикации на внешних ресурсах
Считываемые/записываемых файлы «облачных» хранилищ

Активность в течение рабочего времени

Электронная почта:
Внутренняя переписка
Прием/получение внутренних писем
Внутреннее перемещение инф. активов
Внешняя переписка
Прием/получение внешних писем
Отправка вовне инф. активов
Получение извне инф. активов

Внутренние информационные ресурсы:
Активность использования внутренних хранилищ
Считываемые/записываемые инф. активы
Публикации на внутренних ресурсах

Использование периферийных устройств:
Активность печати и использования МФУ
Отправка на печать и сканирование инф. активов

Ростелеком
Солар


Solar Dozor
Поиск в системе
Соединить карточки
Сводный отчет по персоне
Скопировать ссылку
Открыть в новой вкладке
Свернуть карточку
Закрыть
Сунгатулин Юрий Арсениевич
На контроле (2)
Ведущий конструктор
Конструкторское бюро
Принят <Нет данных>
Индекс уязвимости
29 %
Все события: 1
Все аномалии: 10
Активность
Внешняя
Внутренняя
Информационные объекты
Отправленные
Полученные
Вовлеченность
Круг общения
Популярность
Типы поведения
Контакты с неизвестными, Наличие риска, Работа ночью
Аномалии
Активность
Информационные объекты
Круг общения
Популярность
Особые контакты
Аномалии
Индекс уязвимости (ИУ) – это степень риска совершения случайных или намеренных нарушений ИБ со стороны персоны. ИУ измеряется в процентах и показывает интенсивность и мас...
Показать еще
Показатели за 24 часа
Основное
События и инциденты 0
Сообщения 7
Файлы 2
Связи 6
Снимки экрана 0
Устройства 0
Поведение и аномалии
Рабочее время
Отправка сообщений группам
Всего
Испытательный срок 1
Отдел продаж 2
Департамент внедрения и сервиса 3
Служба Безопасности 6
ГрОК Солнце 6
Получение сообщений от групп
Всего
На увольнение 1
Тестовая группа 1
СоловьиА 1
Студенты-стажеры 1
Служба Безопасности 1
Индекс уязвимости
Динамика изменения индекса уязвимости
Все аномалии
Описание аномалии
Начало
Конец
Скачок внешней активности 27.12.18 27.12.18
Резкое снижение числа получаемых инф. объектов 11.11.18 11.11.18

Solar Dozor

Поиск в системе

Аномальное поведение

Наличие серьезных аномалий

Поиск персон, у которых за последние 60 дней обнаружены серьезные аномалии поведения

Количество персон: 24 ▲5 за неделю

Всплеск внешней активности

Поиск персон, у которых за последние 60 дней зафиксирован всплеск внешней активности

Количество персон: 21 ▲5 за неделю

Всплеск отправки информации

Поиск персон, у которых за последние 60 дней зафиксирован всплеск отправки информации

Количество персон: 15 ▲2 за неделю

Всплеск получения информации

Поиск персон, у которых за последние 60 дней зафиксирован всплеск получения информации

Количество персон: 16 ▼16 за неделю

Участники интенсивных коммуникаций

Сверхактивные

Поиск персон с высокой внешней и/или внутренней активностью

Количество персон: 21 ▲1 за неделю

Сверхпопулярные

Поиск персон, получающих много сообщений от большого числа коллег

Количество персон: 38 ▲6 за неделю

Преобладание внешней активности

Поиск персон, у которых внешняя активность значительно превышает внутреннюю

Количество персон: 18 ▲5 за неделю

Специфическое/неординарное поведение

Работа ночью

Поиск персон с активностью в ночные часы

Работа в выходные дни

Поиск персон с активностью в выходные дни

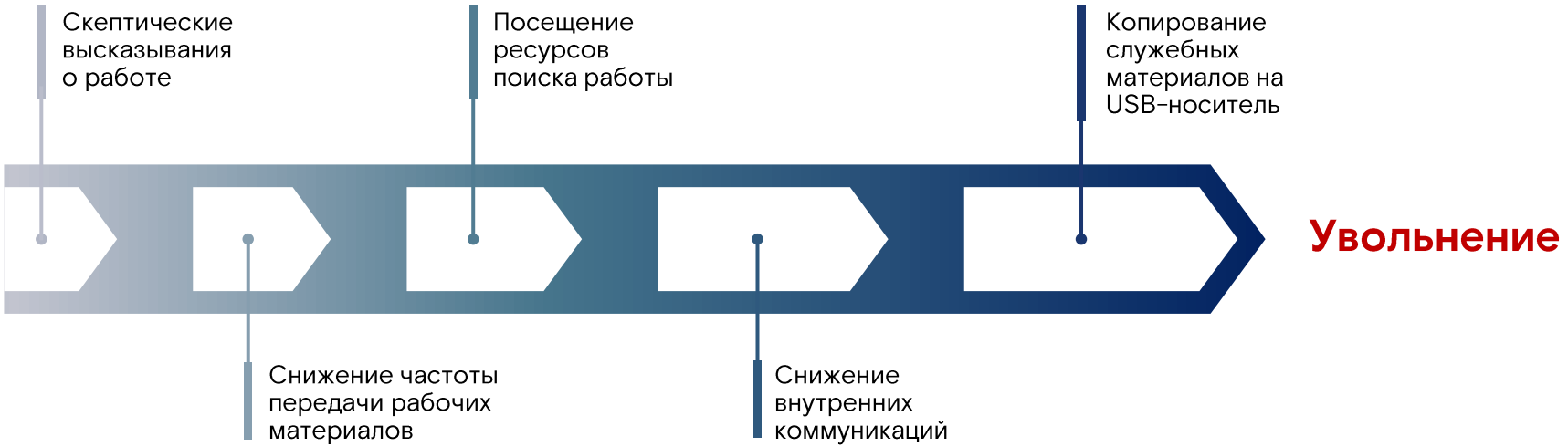
Возможные инсайдеры

Поиск персон с высокой внешней активностью и широким кругом общения в компании, которые когда-либо отправляли/получали

Распространители информации

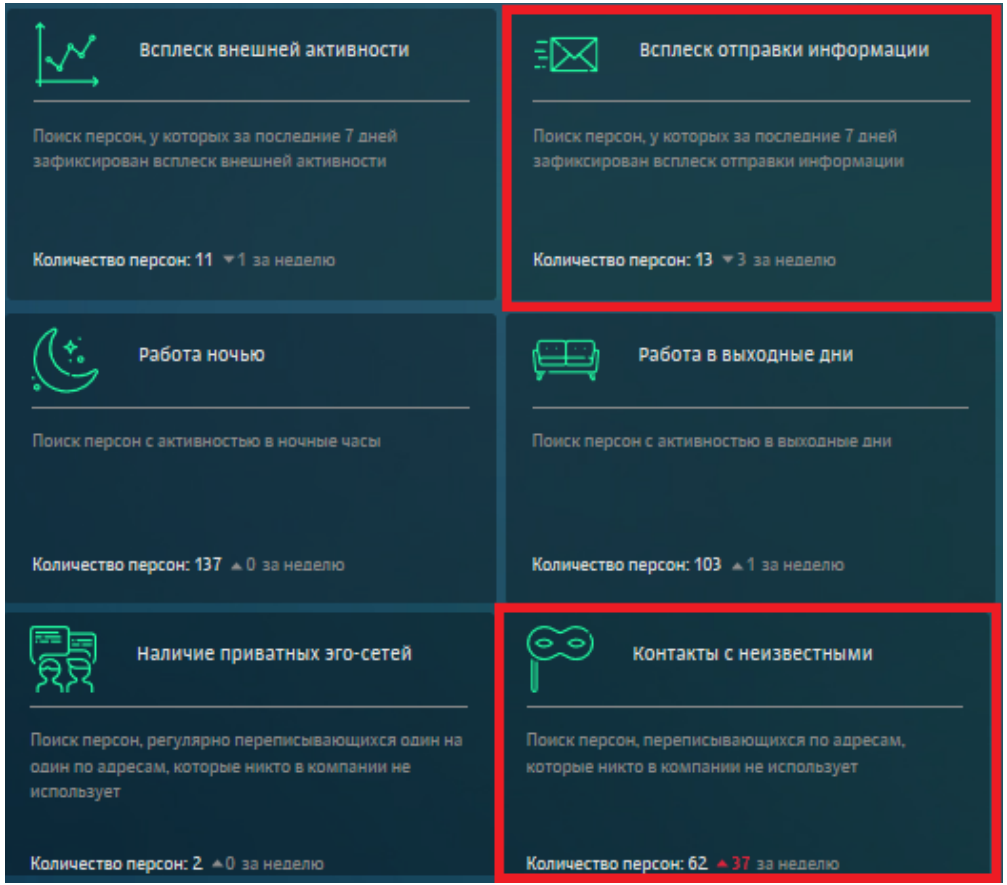
Поиск адресов, с которых часто рассылаются сообщения внутри компании

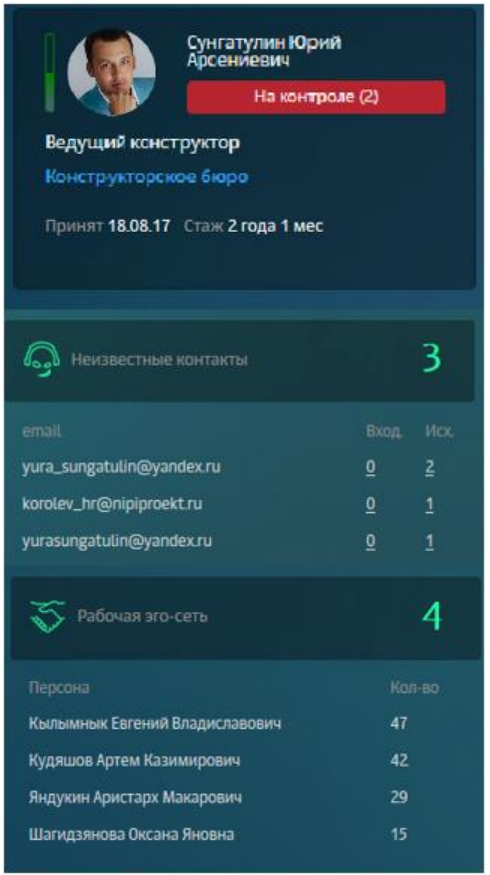
Жизненный цикл работника в UBA



Ростелеком
Солар

Как это выглядит в UBA





Контакты

Центральный офис

125009 г. Москва,
Никитский переулок, 7с1

+7 (499) 755-07-70

info@rt-solar.ru

Ростелеком
Солар