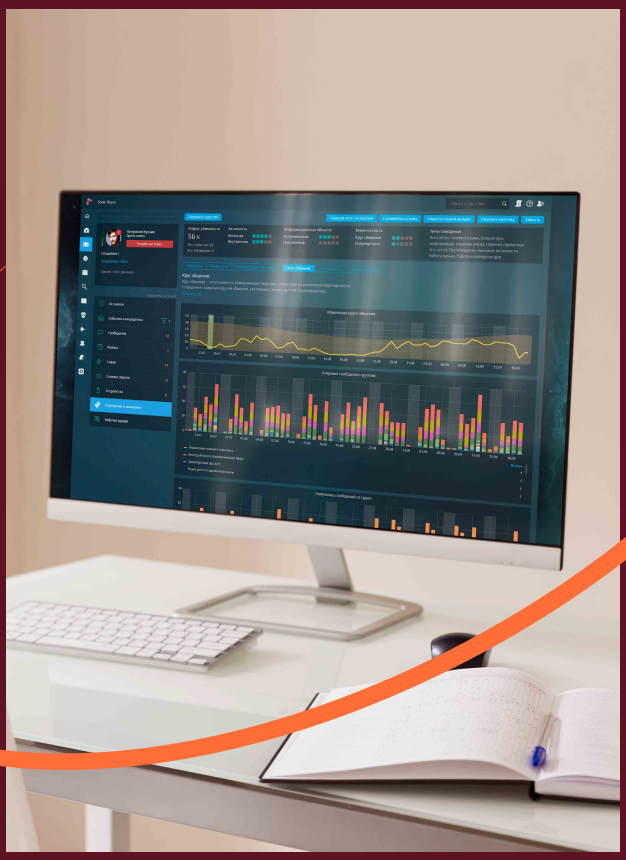
SOLAR DOZOR



Предотвращение утечек информации, профилактика инцидентов ИБ и проведение расследований

W: RT-SOLAR.RU

T: +7 (499) 755-07-70

БЕЗОПАСНОСТЬ С ФОКУСОМ НА ЧЕЛОВЕКЕ

В Solar Dozor реализована современная концепция обеспечения внутренней безопасности организации — People-Centric Security[1]. В ее основе — концентрация внимания службы безопасности не на движении информации, а на сотрудниках, их связях и поведении.

Такой подход снижает количество ложных срабатываний и отвлекающих уведомлений. В результате офицеры безопасности могут сосредоточиться на расследовании и профилактике критических инцидентов.

Модуль анализа поведения пользователей UBA автоматически выявляет аномалии поведения, профилирует сотрудников по устойчивым паттернам поведения, а также осуществляет мониторинг групп риска. Кроме того, в системе есть функция контроля рабочего времени и используемых приложений.

Solar Dozor может решать задачи, выходящие за рамки возможностей обычных DLP-систем. В их числе — выявление инсайдеров и ранних признаков корпоративного мошенничества, борьба с коррупцией, управление конфликтом интересов и ряд других задач.

Все это возможно в том числе и в организациях с территориально распределенной филиальной сетью. Благодаря модулю MultiDozor инсталляции Solar Dozor работают как комплексная логическая система.

ВНУТРЕННИЕ УГРОЗЫ

71%

компаний ежегодно сталкивается с 40+ инцидентами с участием внутренних нарушителей

74%

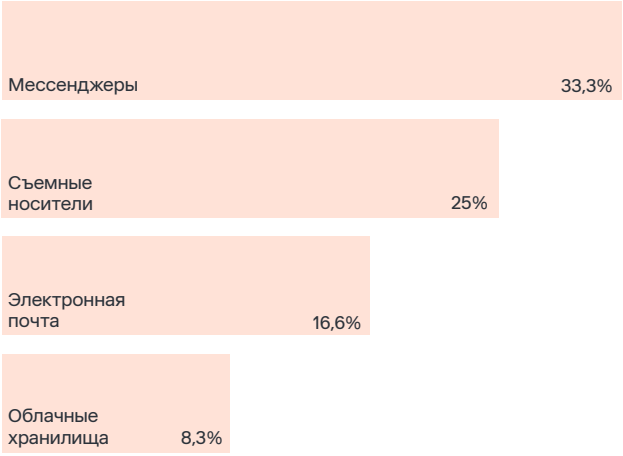
компаний уязвимы перед инсайдерскими угрозами

86 ДНЕЙ

в среднем занимает локализация инцидента внутренней безопасности

2023 Cost of Insider Risks Global Report,
2023 Insider Threat Report

КАНАЛЫ УТЕЧКИ



Исследование
«Ростелеком-Солар», 2022

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

РЕШАЕМЫЕ ЗАДАЧИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

- Защита от утечек информации
- Контроль передачи и хранения информации
- Проведение расследований инцидентов и выявление причин нарушений
- Профилактика инцидентов ИБ

ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

- Выявление признаков корпоративного мошенничества
- Мониторинг коммуникаций по ключевым сделкам
- Мониторинг непрерывности ключевых бизнес-процессов
- Мониторинг коммуникаций с контрагентами
- Выявление и мониторинг групп риска (должники, игроманы, транжиры и т. д.)
- Проведение расследований и сбор доказательной базы

БОРЬБА С КОРРУПЦИЕЙ

- Управление конфликтом интересов
- Выявление признаков аффилированности и проведение расследований
- Выявление фактов вымогательства и получения взяток
- Выявление и мониторинг групп риска (друзья, старослужащие и т. д.)

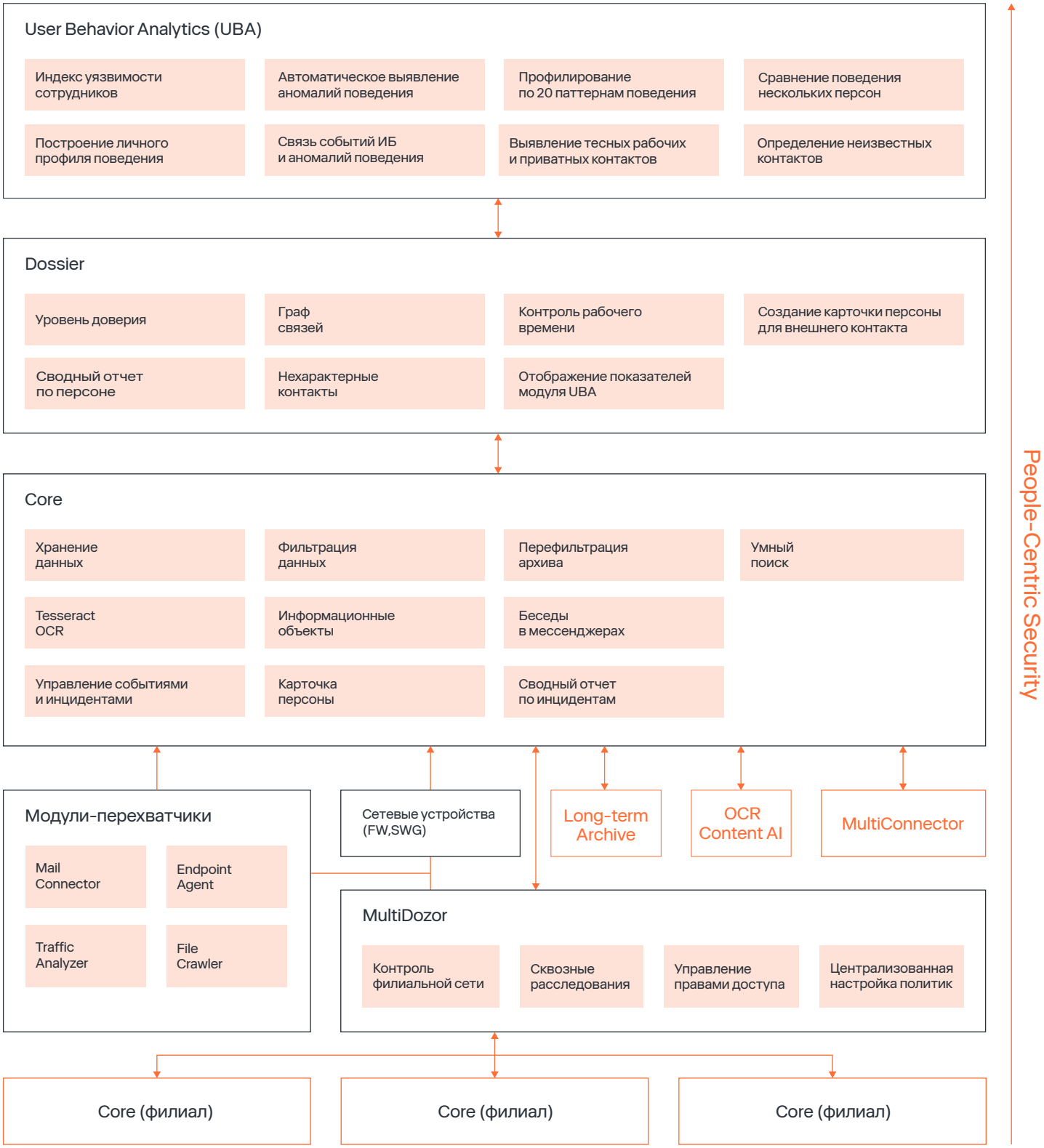
ВНУТРЕННИЙ КОНТРОЛЬ

- Выявление конфликтов интересов
- Контроль исполнения управленческих решений
- Контроль реакции на приказы и распоряжения
- Выявление лоббирования управленческих решений
- Выявление сокрытия нарушений
- Контроль психологического климата в коллективе
- Выявление фактов саботажа
- Оценка соответствия регламентам (кодексам, стандартам, законам)

СОБСТВЕННАЯ БЕЗОПАСНОСТЬ

- Выявление распространителей слухов и инсайдеров
- Выявление компрометирующих связей (с конфликтно уволенными, конкурентами, криминалом)
- Выявление сокрытия нарушений режима охраны
- Выявление признаков вербовочных разработок (разведка, шпионаж)
- Дезинформация получателя информации
- Компрометация источника и ранее полученной информации
- Профилактика экстремизма и терроризма

КОНЦЕПТУАЛЬНАЯ АРХИТЕКТУРА



ВОЗМОЖНОСТИ

КОНТРОЛЬ КАНАЛОВ КОММУНИКАЦИИ И ПРЕДОТВРАЩЕНИЕ УТЕЧЕК ИНФОРМАЦИИ

Для защиты от утечек информации Solar Dozor использует специализированные модули — модули-перехватчики. Они собирают и передают на анализ все сообщения сотрудников, контролируют действия пользователей на персональных компьютерах, а также проверяют локальные и облачные файловые ресурсы.

Применение перехватчиков дает возможность контролировать корпоративную электронную почту, USB-носители, веб-сервисы, файловые хранилища, социальные сети и мессенджеры, блокируя передачу конфиденциальной информации за пределы организации. Срабатывания внутри сообщений подсвечиваются, помогая быстро понять, где и почему сработало то или иное правило политики ИБ.

- Электронная почта
- Социальные сети
- USB-носители
- Веб-сервисы
- Облачные и файловые хранилища
- Мессенджеры

ВЫЯВЛЕНИЕ РАННИХ ПРИЗНАКОВ КОРПОРАТИВНОГО МОШЕННИЧЕСТВА И ПРОВЕДЕНИЕ РАССЛЕДОВАНИЙ

Все собранные перехватчиками сообщения помещаются в долгосрочный архив, который может расширяться практически безгранично. При необходимости возможна перефильтрация архива для нахождения ранее пропущенных инцидентов и ретроспективного анализа ранее накопленных данных на основании вновь открывшихся обстоятельств.

Технология быстрого поиска, аналогичная поисковикам Яндекс или Google, позволяет за секунды находить нужные сообщения и инциденты безопасности. При этом не нужно составлять сложные поисковые запросы — при начале ввода имени или части адреса Solar Dozor сразу отображает сотрудников, данные которых содержат вводимые символы.

- Хранение 1000+ ТБ сроком 10+ лет
- Укладка в архив 3+ ТБ в сутки
- Поиск среди 17 млн сообщений за 1 сек
- Перефильтрация архива
- Контроль сетевых хранилищ 1,8 Тбит/сутки
- Досье на персону

ВЕДЕНИЕ ДОСЬЕ ПО ПЕРСОНАМ, АНАЛИЗ СВЯЗАННОЙ С НИМИ ИНФОРМАЦИИ

Вся информация о сотрудниках и внешних контактах накапливается в специализированном разделе интерфейса — «Досье на персону». «Персона» — лежащая в основе досье сущность — обеспечивает работу в системе с конкретными людьми, а не с их идентификаторами и адресами, которые далеко не всегда очевидны.

В «Досье» сосредоточены главные инструменты анализа персоны: граф связей, библиотека скриншотов, записи видео и звука с рабочей станции, информация об активности на рабочем месте, используемых приложениях, веб-ресурсах и устройствах, а также данные об аномальном поведении. На основе информации в «Досье» можно мгновенно создать сводный отчет по персоне за требуемый период.

- Граф связей
- Поведение и аномалии
- Скриншоты и видео с рабочей станции
- Запись звука с микрофона рабочей станции
- Запись видео экрана рабочей станции
- Контроль рабочего времени

ВЫЯВЛЕНИЕ АНОМАЛЬНОЙ АКТИВНОСТИ И ПРОФИЛИРОВАНИЕ СОТРУДНИКОВ

Модуль UBA открывает новое измерение в анализе поведения человека. Он позволяет автоматически выявлять аномалии поведения, приватные контакты и устойчивые личные эго-сети, а также профилировать сотрудников, относя их к одной из устойчивых групп поведения («мертвые души», собиратели информационных объектов, потенциальные инсайдеры и т. д.).

Определение аномалии не является доказательством злого умысла. Тем не менее перед совершением преступления любой злоумышленник проводит подготовительные действия, которые являются отклонением от нормы. Solar Dozor отмечает такие действия, предоставляя возможность вовремя принять превентивные меры защиты.

- Рабочие и приватные контакты
- Поиск похожих персон
- Индекс уязвимости сотрудника
- Паттерны поведения
- Сравнение поведения нескольких персон
- Мониторинг групп риска

ЭФФЕКТИВНОЕ УПРАВЛЕНИЕ СОБЫТИЯМИ И ИНЦИДЕНТАМИ

Реализованная в Solar Dozor методология управления разбором происшествий и максимальный контроль расследований обеспечивают полный цикл работы с событиями и инцидентами. События информационной безопасности автоматически регистрируются и классифицируются по уровню критичности.

Специальный интерфейс предоставляет список всех инцидентов в работе и наглядную информацию о новых событиях, сгруппированных по уровню критичности, а также подробности о конкретном событии или инциденте. Задача может быть назначена или передана конкретному офицеру в несколько кликов.

- Проработанное управление событиями и инцидентами
- Уровни критичности инцидентов
- Развитая ролевая модель
- История работы с инцидентом

ПОСТРОЕНИЕ ОТЧЕТОВ ПО СОБЫТИЯМ И ИНЦИДЕНТАМ

Solar Dozor позволяет формировать наглядные отчеты для представления результатов работы службы безопасности. В них содержится исчерпывающая информация о происшествиях, нарушителях, потоках данных и итогах проведенных расследований.

С помощью сводных отчетов возможно увидеть общую картину и текущее состояние защищаемой информации. Более подробные отчеты помогают выявить недочеты в политике безопасности организации. Среди специализированных отчетов есть «Тепловая карта коммуникаций» и «Отчет по персоне».

- Тепловая карта коммуникаций
- Отчет по отправителям и получателям информации
- Сводный отчет по инцидентам
- Сводный отчет по персоне

ПОДДЕРЖКА ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОЙ СТРУКТУРЫ ОРГАНИЗАЦИИ (MULTIDOZOR)

Если организация имеет территориально распределенную структуру или иерархичную модель управления, инсталляции Solar Dozor могут работать как одно целое. Модуль MultiDozor объединяет их в комплексную логическую систему.

Офицеры безопасности могут в режиме реального времени централизованно контролировать процессы, получать аналитику и мониторить группы особого контроля в разрезе всей организации, а также проводить сквозные расследования по всей сети филиалов (организаций).

- Единая логическая структура
- Централизованный мониторинг сети филиалов (организаций)
- Централизованная настройка политики безопасности
- Проведение сквозных расследований

ПРЕИМУЩЕСТВА SOLAR DOZOR

Эффективный перехват и блокировка

- Перехват основного трафика на сетевом шлюзе снижает нагрузку на рабочие станции сотрудников
- Возможность установки «в разрыв» обеспечивает блокирование утечек даже при больших потоках трафика
- Изменение и/или удаление содержимого сообщений электронной почты предотвращает утечки

Снижение ложных срабатываний

- Мониторинг действий сотрудников для превентивного обнаружения угроз
- Внимание аналитика фокусируется на потенциальных угрозах и сотрудниках из групп риска
- События и инциденты легко фильтруются и сортируются для максимального сужения выборки
- Данные размечаются тегами по аналогии с поисковиками и социальными сетями

Высокая экспертиза

- 20+ лет развития продукта с учетом российской специфики
- Крупнейшая в России команда по DLP — 120+ профильных специалистов
- Отработанная методология внедрения и эксплуатации DLP-системы
- 600+ внедрений в крупнейших коммерческих и государственных организациях

Гибкость, стабильность и производительность

- Самое крупное внедрение DLP в Европе — 300 000+ агентов на одну инсталляцию
- Встраивается в любую инфраструктуру без конфликтов с другим ПО
- Позволяет реализовать любую программу хранения данных в соответствии с имеющимися мощностями
- Поддерживает модель здоровья Zabbix

Подходит для импортозамещения

- Все модули могут работать на свободных дистрибутивах ОС GNU/Linux
- Полнофункциональный агент для ПК с ОС Linux
- Участник Единого реестра отечественного ПО (№ 1480)
- Сертификат соответствия ФСТЭК России № 4459

Контроль сети филиалов (MultiDozor)

- Все функции Solar Dozor доступны в территориально распределенном режиме
- Единое досье с данными о сотрудниках всей организации
- Сквозной мониторинг групп сотрудников
- Разграничение прав доступа офицеров безопасности
- Архитектурная гибкость и сниженная нагрузка на каналы передачи данных

ВЗАИМОДЕЙСТВИЕ С SOLAR DOZOR

Работа с системой осуществляется через единую консоль управления, доступную из браузера. В основе интерфейса лежит концепция ситуационного центра, позволяющая оперативно оценить обстановку, выделить приоритетные направления работы и начать расследование.

Интерфейс адаптирован для работы на различных типах устройств и поддерживает разрешение вплоть до 4K. При необходимости прямо из окна интерфейса можно вызвать интерактивную инструкцию по работе с системой.

Быстрый результат и развитая визуальная аналитика

Мгновенный переход к нужным массивам данных

Анализ данных не требует использования сторонних систем

Удобный веб-интерфейс, значительно ускоряющий работу

Отчеты позволяют быстро понять ситуацию с внутренними угрозами

Аномалии поведения подкрепляются данными о рабочем времени и передаваемых объектах

Инструменты визуализации и срезы данных, облегчающие оценку ситуации

Удобные инструменты для расследований

Для работы не требуются знания в области ИТ и опыт построения поисковых запросов

Быстрый поиск в любом окне интерфейса позволяет мгновенно находить объекты и инциденты

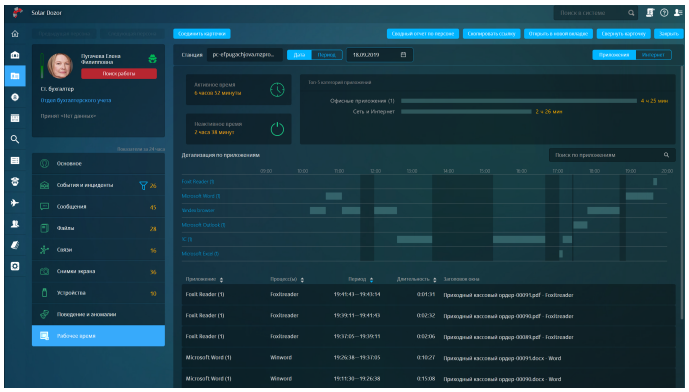
Инструменты кейс-менеджмента позволяют управлять жизненным циклом инцидента на всех этапах расследования

Продуманное взаимодействие между несколькими аналитиками, отдельный рабочий стол для руководителя

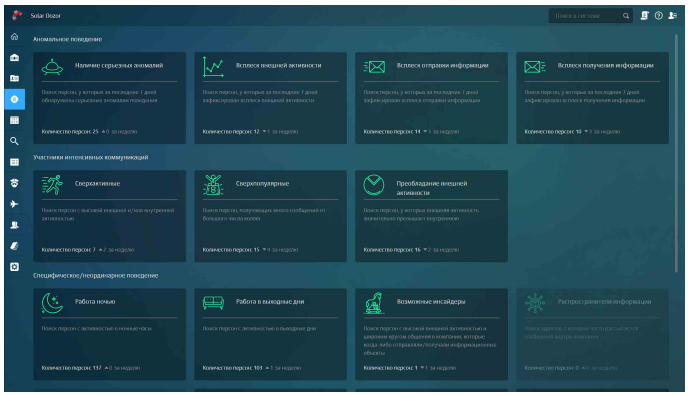
Инцидентная модель реализована в соответствии с ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»

В карточке досье персоны в компактном формате собрана вся информация о сотруднике, его активностях, внешних контактах для продвинутой аналитики и расследования инцидентов ИБ

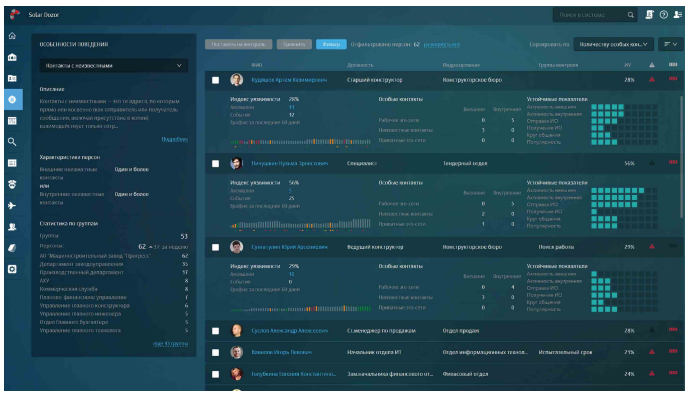
Контроль рабочего времени показывает используемые приложения и веб-сервисы, а также заголовки открытых окон



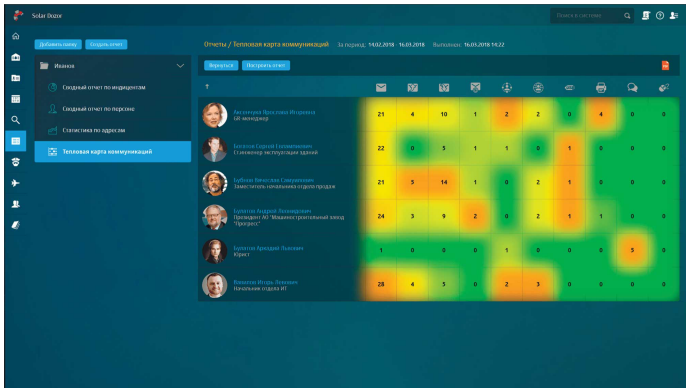
Паттерны поведения позволяют профилировать сотрудника по 20 устойчивым типам поведения



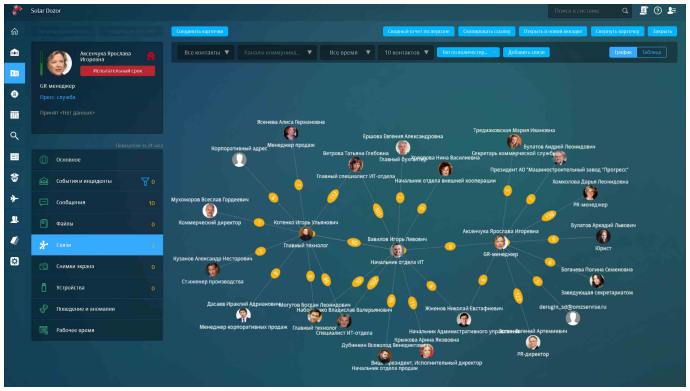
Сравнение аномалий поведения помогает анализировать поведение сотрудников для выявления общих черт и различий



Тепловая карта коммуникаций показывает интенсивность обмена информацией между сотрудниками по каналам коммуникации



Граф связей помогает выявлять неформальные связи и оценивать интенсивность коммуникации



КЕЙСЫ ИСПОЛЬЗОВАНИЯ

[01] Утечка информации через файловые хранилища

Проблема

Во внутренний периметр организации попал документ для ограниченного круга лиц. Его распространение вызвало отрицательную реакцию среди сотрудников.

Решение

Модуль инспектирования файловых систем Dozor File Crawler по расписанию проверил всю рабочую сеть организации и обнаружил файл, размещенный в общедоступной папке корпоративного хранилища. К моменту обнаружения файл переименовали несколько раз, но, благодаря тому что Solar Dozor невосприимчив к переименованию файла и смене формата, были обнаружены все копии изначального документа.

[02] Контроль действий увольняющегося сотрудника

Проблема

Увольняющийся работник решил скопировать документы, содержащие информацию о стратегии организации и подробности контактов с поставщиками. Их распространение могло нанести существенный материальный и репутационный ущерб.

Решение

Возможности Solar Dozor позволили вовремя зафиксировать факт поиска работы и поставить сотрудника на особый контроль. Во время попытки копирования конфиденциальных документов на USB-носитель действия сотрудника были заблокированы, а служба безопасности уведомлена об инциденте.

[03] Выявление инсайдеров

Проблема

В организации начали происходить утечки информации, которые не детектировались существующей DLP-системой. Было принято решение попробовать другое решение — Solar Dozor.

Решение

После ретроспективного анализа данных почтового архива модулем UBA выяснилось, что у одного из сотрудников периодически фиксируются аномалии поведения. Более детальный анализ показал, что сотрудник иногда отправлял на свою корпоративную почту несвойственные ему документы, после чего открывал почту из дома и копировал их себе на ПК.

[04] Выявление признаков корпоративного мошенничества

Проблема

У службы безопасности возникло подозрение, что один из менеджеров по закупкам мошенничает с тендерами. Основой для подозрений стали поисковые запросы товаров в категории «роскошь».

Решение

Возможности модуля UBA по построению сети контактов позволили выявить приватную эго-сеть — внешний контакт, с которым общался только закупщик. После анализа стало понятно, что сотрудник отправлял данные конкурсов в аффилированную с ним компанию.

Отзывы клиентов

СБЕР БАНК

В России нет аналогичных внедрений DLP-решений, работающих в инфраструктурах подобного масштаба с петабайтами хранящихся данных, терабайтами оперативной памяти, тысячами ядер, сотнями серверов.

ПАО «Сбербанк»

Федеральная пассажирская компания

Поскольку АО «ФПК» придает большое значение вопросам ИБ, тот факт, что Solar Dozor способен защитить организацию от самого широкого спектра внутренних угроз, стал ключевым аргументом в его пользу.

АО «Федеральная пассажирская компания»

Отдельно хотелось бы отметить высокий уровень реализации модуля «Досье», который позволяет сформировать единую картину действий каждого сотрудника, гибко анализировать их по большому количеству срезов и критериев, а также формировать наглядные отчеты для представления руководству.

ООО «РН-Морской терминал Туапсе»

Архив Solar Dozor практически не имеет ограничения по объему данных и сроку хранения, обеспечивает богатые возможности для проведения ретроспективного анализа. А скорость поиска на десятках ТБ данных составляет менее секунды.

АО «Россельхозбанк»

Технологии безопасности, реализованные в Solar Dozor, соответствуют всем требованиям ООО «Газпром добыча Ямбург». DLP-комплекс развернут на 5000 рабочих станций организации и демонстрирует высокую производительность и отказоустойчивость.

ООО «Газпром добыча Ямбург»

Solar Dozor выделяется среди других решений простым и интуитивно понятным интерфейсом, легким в освоении. Правильная и продуманная архитектура продукта позволяет быстро настраивать решение и не требует сложной перенастройки существующей сетевой инфраструктуры.

ООО «Таможенная карта»

НСК

Solar Dozor позволяет гибко настраивать политики безопасности и дает меньше ложных срабатываний, чем конкурентные решения.

ООО «НСК»

Корпорация Тактическое Ракетное Вооружение

Solar Dozor полностью решил комплекс задач по защите от внутренних угроз организации.

АО «Корпорация "Тактическое ракетное вооружение"»

SOLAR

W: RT-SOLAR.RU
W: RT.RU

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

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