Solar Dozor

Новое поколение.
Теперь с UBA

Предотвращение утечек информации, анализ поведения пользователей и проведение расследований

rt-solar.ru
rt.ru

Ростелеком
Солар


UBA
Построение индивидуального профиля поведения
Сравнение поведения нескольких выбранных персон
Автоматическое выявление аномалий поведения
Выявление тесных рабочих и приватных контактов (эго-сетей)
Гибкий поиск по особенностям поведения
Выявление опасных массовых тенденций по паттернам поведения
Совместное рассмотрение событий ИБ и аномалий поведения
Автоматический поиск сотрудников по 19 паттернам поведения
Автоматическое определение неизвестных контактов, в т. ч. личной почты

Новое поколение.
Теперь с UBA

В Solar Dozor 7 появились принципиально новые инструменты для выявления аномалий поведения и мониторинга групп особого контроля. С их помощью можно решать задачи не только информационной, но и экономической и собственной безопасности. Например, выявлять инсайдеров и ранние признаки корпоративного мошенничества, пресекать коррупцию, управлять конфликтом интересов, отслеживать коммуникации по ключевым сделкам.

Безопасность с фокусом на человеке

UBA – главный тренд

60%

организаций используют DLP-системы

53%

организаций столкнулись с инсайдерами за последний год

на 124%

выросло использование UBA за год

Данные: Insider Threat Report 2018, CA Technologies

Каналы утечки, %

34,2%
Электронная почта

27,5%
Веб-ресурсы

19%
Устройства прямого доступа в интернет

14,6%
Съемные носители

4,2%
Печать

Данные: Solar JSOC Security Flash Report. Итоги 2018 года

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.

В седьмом поколении DLP-системы Solar Dozor концепция People-Centric Security получила принципиально новое воплощение — модуль анализа поведения пользователей (UBA). Он автоматически выявляет аномалии поведения, профилирует сотрудников по устойчивым паттернам поведения, а также выявляет и контролирует группы риска.

Также в системе появилась функциональность контроля рабочего времени и используемых приложений. Эти нововведения вызвали необходимость переосмыслить интерфейс и функциональность досье персоны, что нашло отражение в новом модуле — Dossier.

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

[1]«Безопасность с фокусом на человеке». Термин введен международной консалтинговой компанией Gartner, специализирующейся на ИТ-рынке (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, охотники, старослужащие и т. д.)

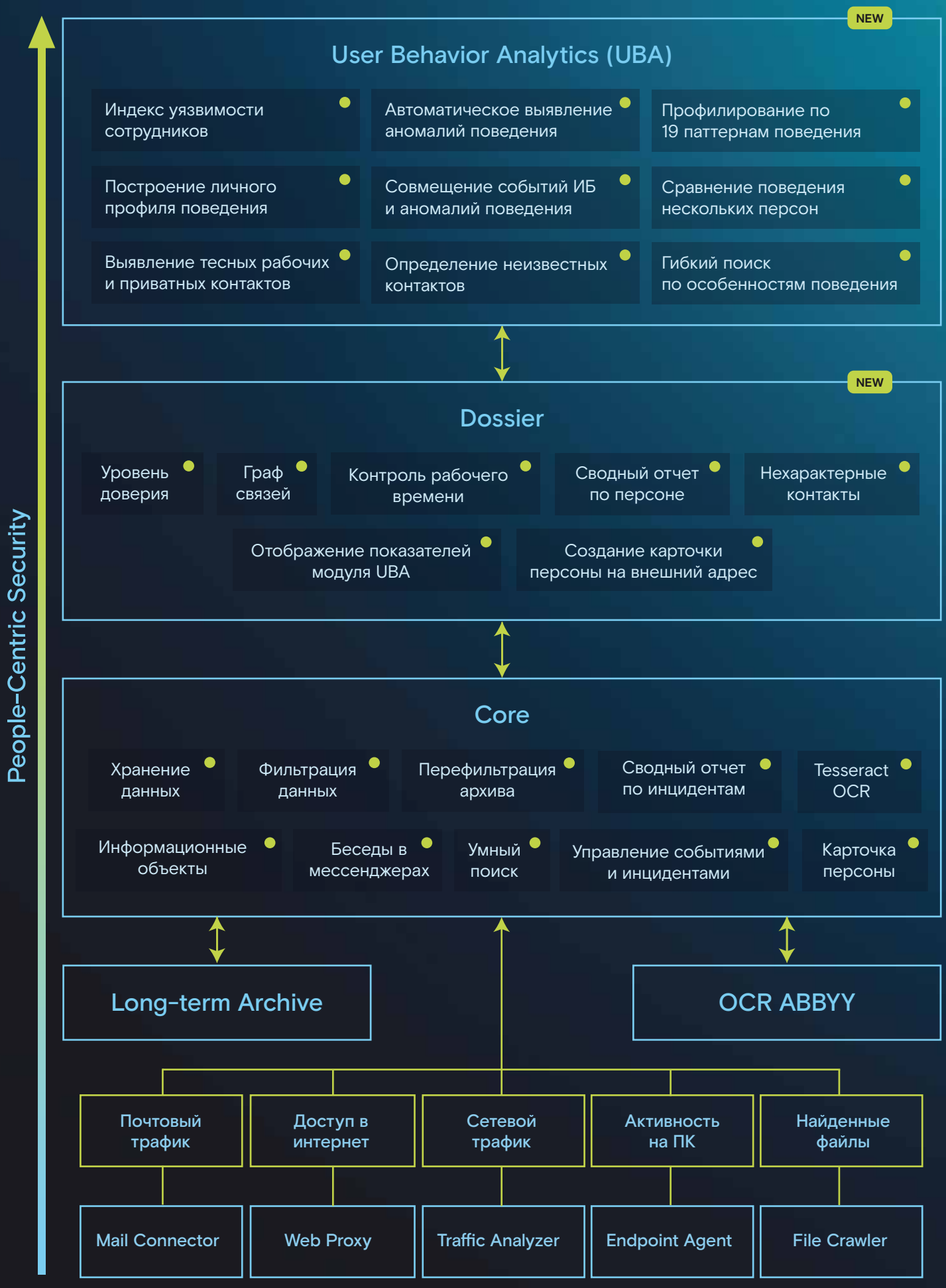
Внутренний контроль

- Выявление конфликтов интересов
- Контроль исполнения управленческих решений
- Контроль реакции на приказы и распоряжения
- Выявление лоббирования управленческих решений
- Выявление сокрытия нарушений
- Контроль 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



Новые модули

UBA

Анализ поведения пользователей

Модуль UBA открывает перед офицерами безопасности целый ряд новых возможностей. В их число входят выявление аномалий в поведении, определение круга общения и приватных контактов, а также профилирование сотрудников в соответствии с 19 устойчивыми паттернами поведения.

Фокус на человеке позволяет выявлять злоумышленников, поведение которых обычно не отличается от стандартного. Например менеджера по закупкам, иногда использующего аффилированные компании для участия в тендерах. Или инсайдера, незаметно устраивающего время от времени утечки.

Аналитическая модель модуля UBA базируется на теории вероятности, теории случайных процессов и теории графов. При этом не требуется предварительная настройка и адаптация модуля под условия эксплуатации — он полностью интегрирован в Solar Dozor и готов к работе.

Для предварительного анализа достаточно накопить массив данных о коммуникациях сотрудников за 1 месяц, для точной работы — за 2-3 месяца. Если организация уже использует Solar Dozor, то анализ поведения пользователей доступен сразу.

Dossier

Аккумуляция информации о персоне

Модуль Dossier предоставляет максимально подробную информацию о персоне. В нем собирается история переписки и отправляемых файлов, открытых приложений и времени работы с ними, посещаемых веб-ресурсах, используемых устройствах, событиях и инцидентах, а также скриншоты рабочего стола.

С помощью модуля Dossier также отображаются данные по поведению, представляемые модулем UBA: индекс уязвимости, аномалии, интенсивность отправки сообщений и информационных объектов, круг общения, популярность и особые контакты.

Для глубокого анализа доступны удобные инструменты визуализации данных: граф связей с другими персонами, сводный отчет по персоне, уровень доверия, активность пользователя на персональном компьютере.

Вместе с настроенными срезами данных, быстрым сквозным поиском и проработанным инцидент-менеджментом модуль Dossier дает офицеру безопасности набор простых и наглядных инструментов для проведения расследований, недоступный в других DLP-системах.

Возможности

Контроль каналов коммуникаций и предотвращение утечек информации

Для защиты от утечек информации Solar Dozor использует специализированные 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 и мессенджеры

USB-носители и принтеры

Веб-сервисы

Облачные и файловые хранилища

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 ретроспективного анализа ранее накопленных данных по вновь открывшимся обстоятельствам и нахождения ранее пропущенных инцидентов.

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 850+ ТБ сроком 10+ лет

Укладка 2,5+ ТБ в сутки

Мгновенный поиск по архиву

Досье на персону

Перефильтрация архива

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, 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 и отобразить его в веб-интерфейсе или выгрузить в PDF-файл для печати.

Граф связей

Поведение и аномалии

Скриншоты рабочего стола

Используемые USB-устройства

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 эгосети, 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

Паттерны поведения

Поиск похожих персон

Мониторинг групп риска

Индекс уязвимости сотрудника

Эффективное управление событиями и инцидентами

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

Управление осуществляется при помощи специального интерфейса. Он предоставляет наглядную информацию о новых событиях, сгруппированных по уровню критичности, список всех инцидентов в работе, а также подробности о конкретном событии или инциденте. Задача может быть назначена или передана конкретному офицеру в несколько кликов.

Проработанное управление событиями и инцидентами

Развитая ролевая модель

История работы с инцидентом

Уровни критичности инцидентов

Построение отчетов по событиям и инцидентам

Встроенные аналитические инструменты позволяют формировать наглядные отчеты для качественного представления результатов работы службы безопасности. В них содержится исчерпывающая информация о происшествиях, нарушителях, потоках данных и результатах проведенных расследований.

С помощью сводых отчетов руководители службы безопасности могут видеть общую картину и текущее состояние защищаемой информации. Более подробные отчеты помогают выявить недочеты в политике безопасности компании. 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

Преимущества Solar Dozor

Эффективные 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 и позволяет проводить оперативные комбинации

Снижение ложных срабатываний

- Мониторинг сотрудников обеспечивает превентивное обнаружение угроз
- Внимание аналитика фокусируется на наиболее опасных сотрудниках и потенциальных угрозах
- 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
- 300+ внедрений в крупнейших коммерческих и государственных организациях

Гибкость, стабильность и производительность

- Количество контролируемых пользователей — 200 000+
- Встраивается в любую инфраструктуру без конфликтов с другим ПО
- Позволяет реализовать любую программу хранения данных в соответствии с имеющимися мощностями
- Поддерживает модель здоровья Zabbix

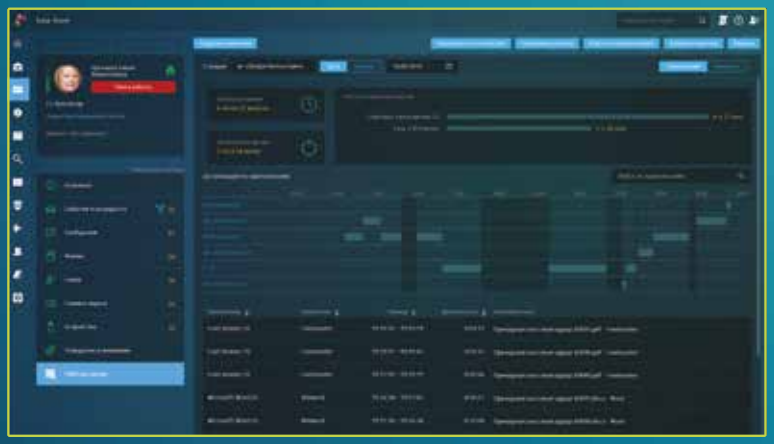
Подходит для импортозамещения

- Все модули могут работать на свободных дистрибутивах ОС GNU/Linux
- Участник Единого реестра отечественного ПО (№ 1480)
- Сертификат соответствия ФСТЭК России № 3706 позволяет использовать Solar Dozor в АС до класса защищенности 1Г, в ГИС до 1 класса защищенности, в ИСПДн до 1 уровня защищенности

Взаимодействие с Solar Dozor 7

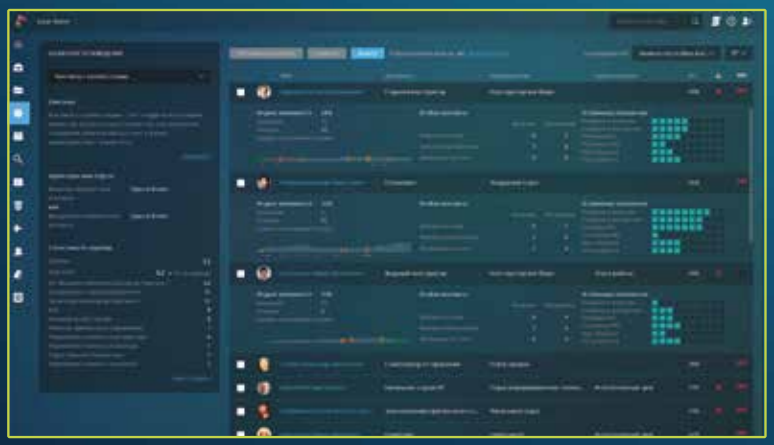
Работа с системой осуществляется через единую консоль управления, доступную из браузера. В основе интерфейса лежит концепция ситуационного центра, позволяющего оперативно оценить обстановку, выделить приоритетные направления работы и начать расследование.

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.



Контроль рабочего времени

Показывает используемые приложения и веб-сервисы, а также заголовки открытых окон



Сравнение аномалий поведения

Помогает анализировать поведение сотрудников для выявления общих черт и различий

Быстрый результат и развитая визуальная аналитика

- Единый удобный веб-интерфейс значительно ускоряет работу
- Инструменты визуализации и срезы данных облегчают оценку ситуации
- Можно мгновенно переходить к нужным массивам данных
- Аномалии поведения подкрепляются данными по рабочему времени и перемещаемым информационным объектам
- Сводные отчеты позволяют быстро понять ситуацию с внутренними угрозами
- Для анализа данных не требуется использование сторонних систем

Удобные инструменты для расследований

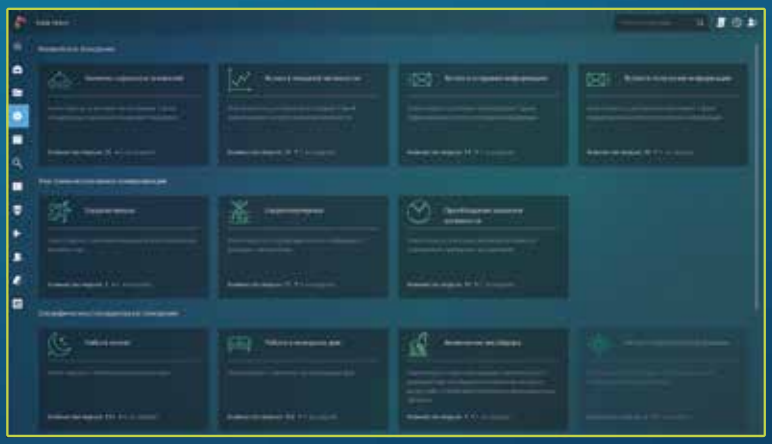
- Для работы не требуются знания в области ИТ и опыт построения поисковых запросов
- Инструменты кейс-менеджмента позволяют управлять жизненным циклом инцидента на всех этапах расследования
- Быстрый поиск в любом окне интерфейса позволяет мгновенно находить объекты и инциденты
- Продуманное взаимодействие между несколькими аналитиками, отдельный рабочий стол для руководителя
- Инцидентная модель реализована в соответствии с ГОСТ 15408 «Менеджмент ИБ»

Тепловая карта коммуникаций

Показывает интенсивность обмена информацией между сотрудниками по каналам коммуникаций

Граф связей

Помогает выявлять неформальные связи и оценивать интенсивность коммуникации



Паттерны поведения

Позволяют профилировать сотрудника по 19 устойчивым типам поведения

Кейсы использования

Утечка информации через файловые хранилища

Проблема

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

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 инцидента файл переименовали несколько раз, но благодаря тому, что Solar Dozor невосприимчив к переименованию файла и смене формата, были обнаружены все копии изначального документа.

Контроль действий увольняющегося сотрудника

Проблема

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

Решение

Возможности Solar Dozor позволили заранее 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.

Выявление инсайдера

Проблема

В компании 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 встречаются 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.

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» и новый автомобиль сотрудника.

Решение

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

Отзывы клиентов

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»

DLP-система Solar Dozor продемонстрировала высочайшую степень готовности и применимости для решения задач информационной и внутренней безопасности.

АО «СМПБМ "Малахит"»

Технологии безопасности, реализованные в Solar Dozor, соответствуют всем требованиям ООО «Газпром добыча Ямбург». DLP-комплекс развернут на 5 000 рабочих станций организации и демонстрирует высокую производительность и отказоустойчивость.

ООО «Газпром межрегионгаз Уфа»

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»

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.

Платежная система «Таможенная карта»

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

ООО «НСК»

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

АО «Корпорация "Тактическое ракетное вооружение"»

Ростелеком
Солар

rt.ru
rt-solar.ru

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

9.11.BR.SD.01