SOLAR DOZOR

Предотвращение утечек информации, профилактика инцидентов ИБ и проведение расследований

Solar Dozor

Это система для предотвращения утечек конфиденциальной информации (Data Leak Prevention, DLP). Она обеспечивает контроль коммуникаций сотрудников, возможность блокировки или модификации нежелательных сообщений, выявление и мониторинг групп риска, а также ретроспективный анализ архива коммуникаций для проведения расследований.

Кроме того, Solar Dozor анализирует поведение пользователей (User Behavior Analytics) и выявляет в нем аномалии, определяет круг общения и приватные контакты сотрудников, а также профилирует их на основе 20 устойчивых паттернов поведения.

Если организация состоит из нескольких дочерних зависимых обществ или территориально распределенных филиалов, инсталляции Solar Dozor могут работать как единое целое (функции модуля MultiDozor).

Отработанная методология внедрения и эксплуатации DLP-системы

Единый веб-интерфейс и единая политика безопасности

Развитые визуальные инструменты и графические отчеты

Полнофункциональные агенты для Windows, Linux, macOS

600+

проектов в крупнейших государственных и коммерческих организациях

120+

сотрудников — это крупнейшая команда в России

300+

тысяч подтвержденных агентов в одной инсталляции

1000+ ТБ

объем подтвержденного архива у клиента

Принцип работы

ПЕРЕХВАТ ПО КОНТРОЛИРУЕМЫМ КАНАЛАМ КОММУНИКАЦИЙ

- Электронная почта
- Мессенджеры
- Публикации в сети
- Файловые ресурсы
- USB-носители и принтеры
- Веб-запросы

ФИЛЬТРАЦИЯ ПЕРЕХВАЧЕННОЙ ИНФОРМАЦИИ

Правила политики

АНАЛИЗ ОБРАБОТАННОЙ ИНФОРМАЦИИ

- Досье на персоны и группы
- Информационные объекты
- Аналитика и отчетность
- Анализ поведения пользователей
- Управление событиями и инцидентами
- Архив коммуникаций

Решаемые задачи

- Выявление признаков корпоративного мошенничества
- Мониторинг коммуникаций сотрудников
- Проведение расследований
- Профилактика инцидентов ИБ
- Выявление и мониторинг групп риска
- Профилактика экстремизма и терроризма
- Управление конфликтом интересов
- Отслеживание аномалий поведения

Узнать больше о Solar Dozor

Возможности

Контроль каналов коммуникации и предотвращение утечек информации

Электронная почта

Социальные сети и мессенджеры

USB-носители и принтеры

Веб-сервисы

Облачные и локальные файловые хранилища

Ведение досье по персонам, анализ связанной с ними информации

Граф связей

Анализ поведения пользователей

Скриншоты рабочего стола

Контроль рабочего времени

Используемые USB-устройства

Запись звука с рабочей станции

Выявление ранних признаков корпоративного мошенничества и проведение расследований

Мгновенный поиск по архиву

Перефильтрация архива

Досье на персону

Мониторинг групп особого контроля

Выявление аномальной активности и профилирование сотрудников

Рабочие и приватные контакты

Паттерны поведения

Поиск похожих персон

Мониторинг групп риска

Индекс уязвимости сотрудника

Эффективное управление событиями и инцидентами

Инцидентная модель в соответствии с ГОСТ 15408 «Менеджмент ИБ»

Развитая ролевая модель

История работы с инцидентом

Уровни критичности инцидентов

Построение отчетов по событиям и инцидентам

Тепловая карта коммуникаций

Сводный отчет по персоне

Отчет по отправителям и получателям информации

Сводный отчет по инцидентам

Поддержка территориально распределенной структуры организации

Централизованный контроль деятельности сотрудников в сети филиалов (организаций)

Работа с данными разрозненных филиалов (организаций) как с единым целым

Гибкая настройка политик безопасности: централизованная политика и локальные правила

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

Ключевые клиенты

СБЕР БАНК

ГАЗПРОМ ДОБЫЧА ЯМБУРГ

Федеральная пассажирская компания

Корпорация Тактическое Ракетное Вооружение

НСК

РОСАТОМ

ЮНИ ПРО

SOLAR

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

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