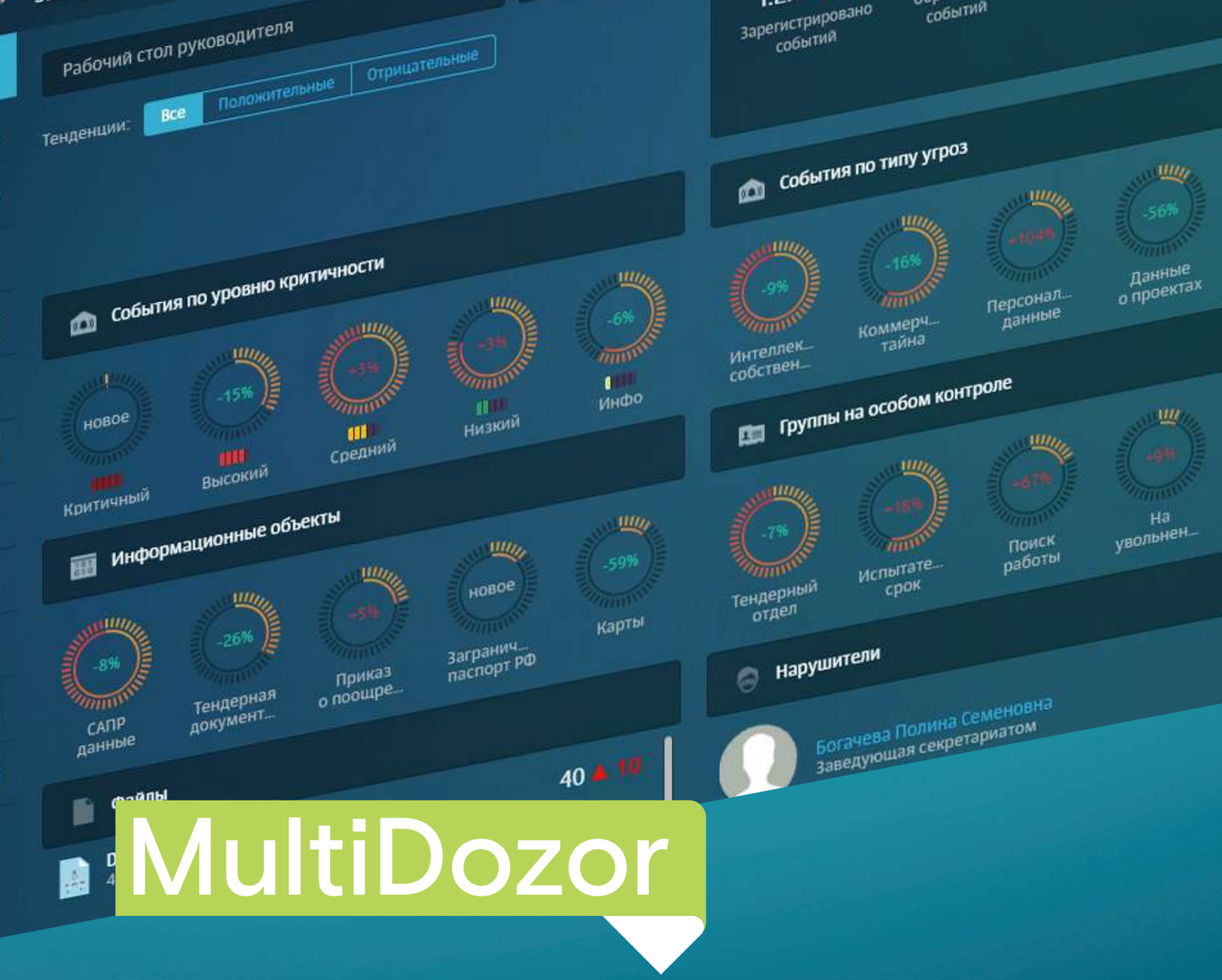

MultiDozor

Объединение разрозненных инсталляций DLP Solar Dozor
в комплексную логическую систему

rt-solar.ru
rt.ru

Ростелеком
Солар

Безопасность территориально распределенной организации

Организациям с территориально распределенной филиальной или иерархичной структурой управления необходима актуальная и цельная картина событий и процессов информационной безопасности. Зачастую данные по филиалам или иерархически связанным организациям фрагментированы, отражают события ретроспективно или с задержкой по времени, а нужную информацию приходится извлекать из нескольких независимых систем.

Такая ситуация может привести к запоздалой реакции на инцидент или его ошибочной отработке. Причиной инцидента могут быть действия сотрудников нескольких филиалов или организаций, но обнаружить их потенциально незаконную связь с помощью локальных инсталляций DLP-системы — сложная и трудоемкая задача.

Для решения задач распределенных организаций в DLP-системе Solar Dozor реализован модуль MultiDozor

Модуль объединяет разрозненные инсталляции Solar Dozor в комплексную логическую систему, предоставляя сотрудникам безопасности принципиально новые инструменты и возможности для обеспечения информационной и экономической безопасности организации. Работать с данными при этом можно как с единым целым.

Решаемые задачи

- Получение в режиме реального времени данных о событиях внутренней информационной безопасности по всей организации и отдельным структурам
- Централизованный контроль сотрудников безопасности в сети филиалов (организаций)
- Проведение сквозных расследований на распределенном архиве по всей организации
- Мониторинг персон и групп сотрудников по всей организации и отдельным структурам
- Централизованное управление и распространение политик безопасности с возможностью настройки правил для конкретных филиалов (организаций)

Преимущества MultiDozor

Все функции Solar Dozor доступны в территориально распределенном режиме

Единое досье с данными о сотрудниках всей организации

Сквозной мониторинг групп сотрудников по организации

Разграничение прав доступа офицеров безопасности

Архитектурная гибкость и сниженная нагрузка на каналы передачи данных

Архитектурные схемы MultiDozor

Solar Dozor можно устанавливать в ИТ-инфраструктурах с разными требованиями.

Обработка и хранение данных

Локально в филиалах (организациях):

Принадлежность данных к филиалам (организациям) определяется по их техническим ресурсам — подкластерам.

Централизованно:

Например, при использовании общей корпоративной почты. Принадлежность данных к филиалам (организациям) определяется по назначенным для них веткам организационно-штатной структуры из досье системы.

Децентрализованно:

Часть данных — общая для организации, другая — обрабатывается в филиалах (организациях) и при необходимости передается в единый центр обработки данных. Такая схема подходит для организаций, использующих общую почту и собирающих данные с агентов DLP-системы, установленных на компьютерах в филиалах (организациях).

Возможности модуля MultiDozor

Просмотр статистики

- Статистика по всей организации и отдельным структурам доступна на рабочих столах руководителя и аналитика.
- Информация на рабочих столах перестраивается при переключении между филиалами (организациями).

Работа с сообщениями, событиями и инцидентами

- Возможности поиска и работы с данными зависят от прав доступа офицера безопасности.
- Принадлежность данных к филиалам (организациям) отображается в карточках объектов и в результатах поисковых запросов.

Управление Dozor Endpoint Agent

- Видимость групп Dozor Endpoint Agent и данных агентских приложений ограничивается в соответствии с правами доступа офицера безопасности.
- Управлять Dozor Endpoint Agent можно как централизованно, так и локально.

Работа с досье и персонами

- В карточках персон отображается информация о принадлежности к соответствующим филиалам (организациям).
- Офицеры безопасности с доступом к данным конкретного филиала (организации) при просмотре персон других филиалов (организаций) видят только общие сведения.

Работа с группами особого контроля

- Мониторинг таких групп ведется в каждом филиале (организации) отдельно.
- Видимость таких групп и правил политики безопасности для них зависит от прав доступа офицеров безопасности.

Формирование отчетности в масштабе организации

- При создании отчетов офицер безопасности может выбрать нужный ему филиал (организацию).
- Информация о принадлежности данных к филиалам (организациям) отображается в интерфейсе и печатных формах отчетов.

Настройка политики безопасности и работа с информационными объектами

- Политика безопасности настраивается и распространяется по филиалам централизованно. Для отдельных филиалов (организаций) можно настроить специфические правила политики.
- Можно настроить детектируемые информационные объекты — общие по компании или определенные для отдельных филиалов (организаций).

Разграничение прав доступа офицеров безопасности к системе

В системе предусмотрено разделение прав доступа на несколько уровней.
В зависимости от уровня доступа офицер безопасности может работать с данными:

- всей организации
- нескольких филиалов (организаций)
- конкретного филиала (организации)

Ростелеком Солар

presale@rt-solar.ru rt.ru rt-solar.ru

+7 (499) 755-07-70