CROSSTECH
SOLUTIONS GROUP

DataGrain Event Stream Optimization (DataGrain ESO)

CROSSTECH
SOLUTIONS GROUP

Crosstech Solutions Group

Российский разработчик решений для мониторинга, контроля и комплексной защиты от внутренних угроз с учетом специфики каждой отдельной организации.

Продукты входят в реестр российского ПО и рекомендованы для импортозамещения на предприятиях России

6
решений

>50
актуальных партнеров

5
лет на IT-рынке

www.ct-sg.ru

CROSSTECH
SOLUTIONS GROUP

Решения Crosstech Solutions Group

Docs Security Suite (DSS)

Платформа маркирования, уникализации и шифрования электронных документов, позволяющая разграничить доступ пользователей к конфиденциальной информации и настроить политики действий с документами

Jay Data

Российская платформа, осуществляющая поиск, классификацию, маскирование конфиденциальной информации в базе данных, что позволяет компаниям обеспечить надежную защиту чувствительных данных от нелегитимного использования сотрудниками и сторонними лицами

DataNova Object Recognition (OR)

Решение, реализованное на основе глубоких нейронных сетей в алгоритмах компьютерного зрения, позволяющее с помощью перехвата видеопотока с веб-камеры осуществлять мониторинг за деятельностью сотрудников, выявлять нелегитимную активность согласно настроенным политикам безопасности

CROSSTECH
SOLUTIONS GROUP

Решения Crosstech Solutions Group

DataGrain RUMA

Аналитическая платформа, предназначенная для анализа и внутреннего мониторинга действий пользователей и сущностей, построения профилей активности в различных разрезах, выявления аномалий и подозрений на инциденты

DataGrain ESO

Решение, предназначенное для сбора, сжатия и хранения событий ИБ, с возможностью разграничения прав доступа и осуществления анализа собираемых данных

CrossTech Smart Assets (CTSA)

Комплексный продукт, ориентированный на физический учёт, финансовый контроль и управление контрактными обязательства IT-активов организации в течение всего жизненного цикла

CROSSTECH
SOLUTIONS GROUP

DataGrain Event Stream Optimization (DataGrain ESO)

Решение, предназначенное для сбора, унификации, сжатия и хранения событий ИБ, с возможностью разграничения прав доступа и осуществления статистического анализа собираемых данных

Соответствие требованиям законодательства:
152-ФЗ, ФСТЭК No21, 17

Решение ESO включено в единый реестр российского ПО МИНКОМ связи от 03.02.2023 №16469

CROSSTECH
SOLUTIONS GROUP

DataGrain Event Stream Optimization (ESO)

Задачи, которые решает ESO:

- Централизованный сбор, обработка и долгосрочное высокоэффективное хранение событий
- Поиск и анализ данных событий информационной безопасности
- Визуализация и отчетность
- Масштабируемая архитектура

Результат внедрения ESO:

- Интеграция с источниками данных по различным протоколам и интерфейсам
- Приведение данных к единой структуре
- Снижение затрат на хранения исторических данных
- Соблюдение требований регуляторов

CROSSTECH
SOLUTIONS GROUP

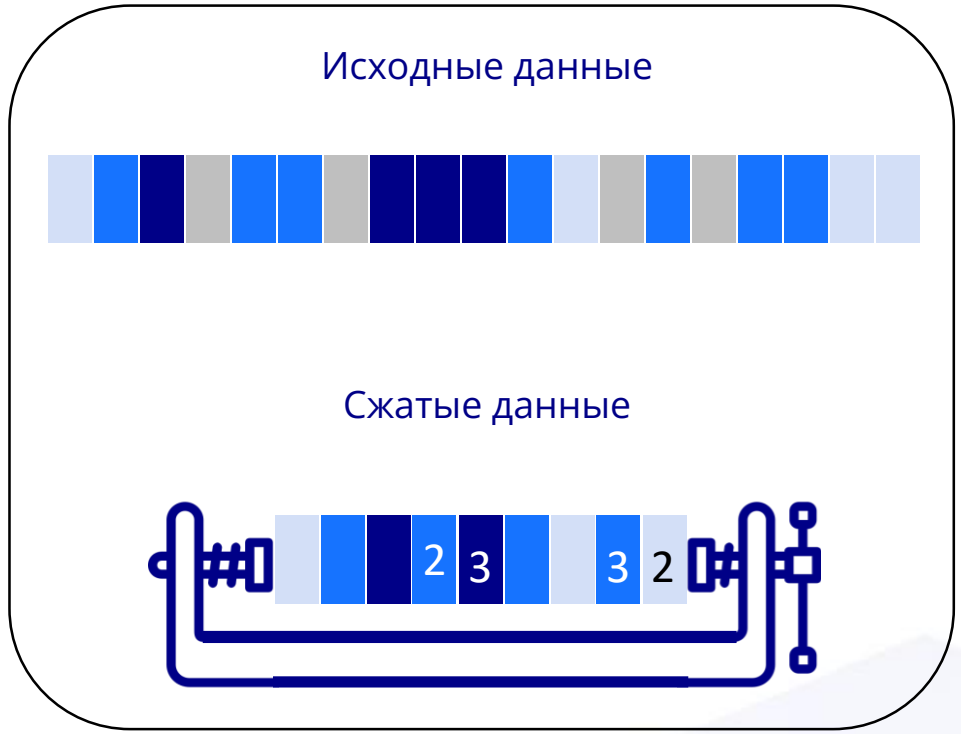
Сбор журналов из различных источников

- Сбор журналов из различных источников с учетом типа, формата и содержания для обеспечения эффективной и точной обработки данных
- Сбор и обработка данных в распределенных средах
- Обеспечение консистентности данных, объединение данных из разных источников в единую структуру
- Обеспечение точности и надежности обработки данных, включая обработку больших объемов данных с высокой скоростью

CROSSTECH
SOLUTIONS GROUP

Эффективное хранения данных

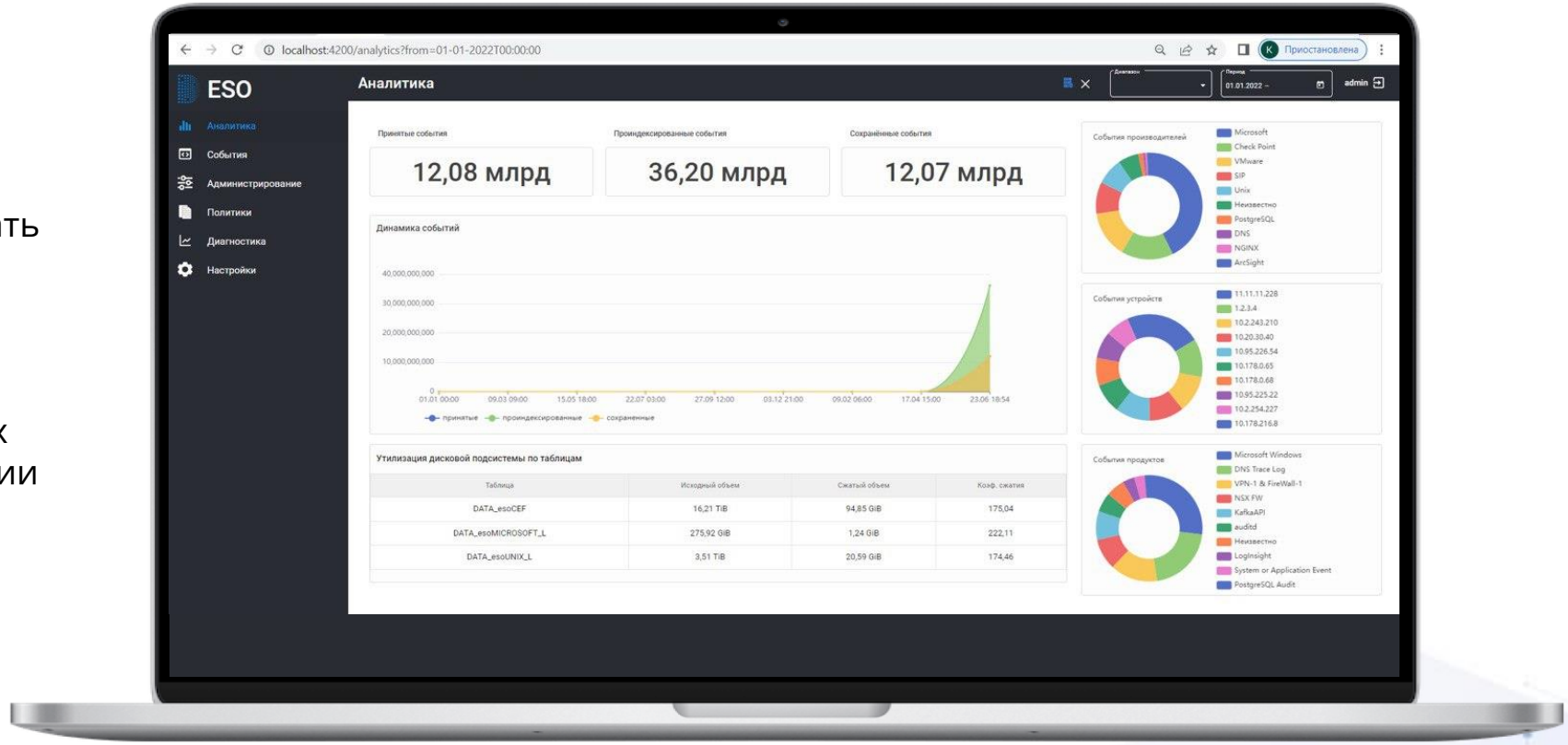
- Оптимизированная архитектура для эффективного использования ресурсов
- Хранение журналов достаточного объема и срока, с учетом типа данных, требований безопасности, доступности и соответствия законодательству
- Возможность обработки миллионов запросов в секунду и предоставление результаты с низкой задержкой
- Встроенные механизмы отказоустойчивости, репликации и восстановления данных
- Возможность масштабирования в случае роста объема хранимых данных
- Высокий коэффициент сжатия данных



CROSSTECH
SOLUTIONS GROUP

Поиск и анализ данных

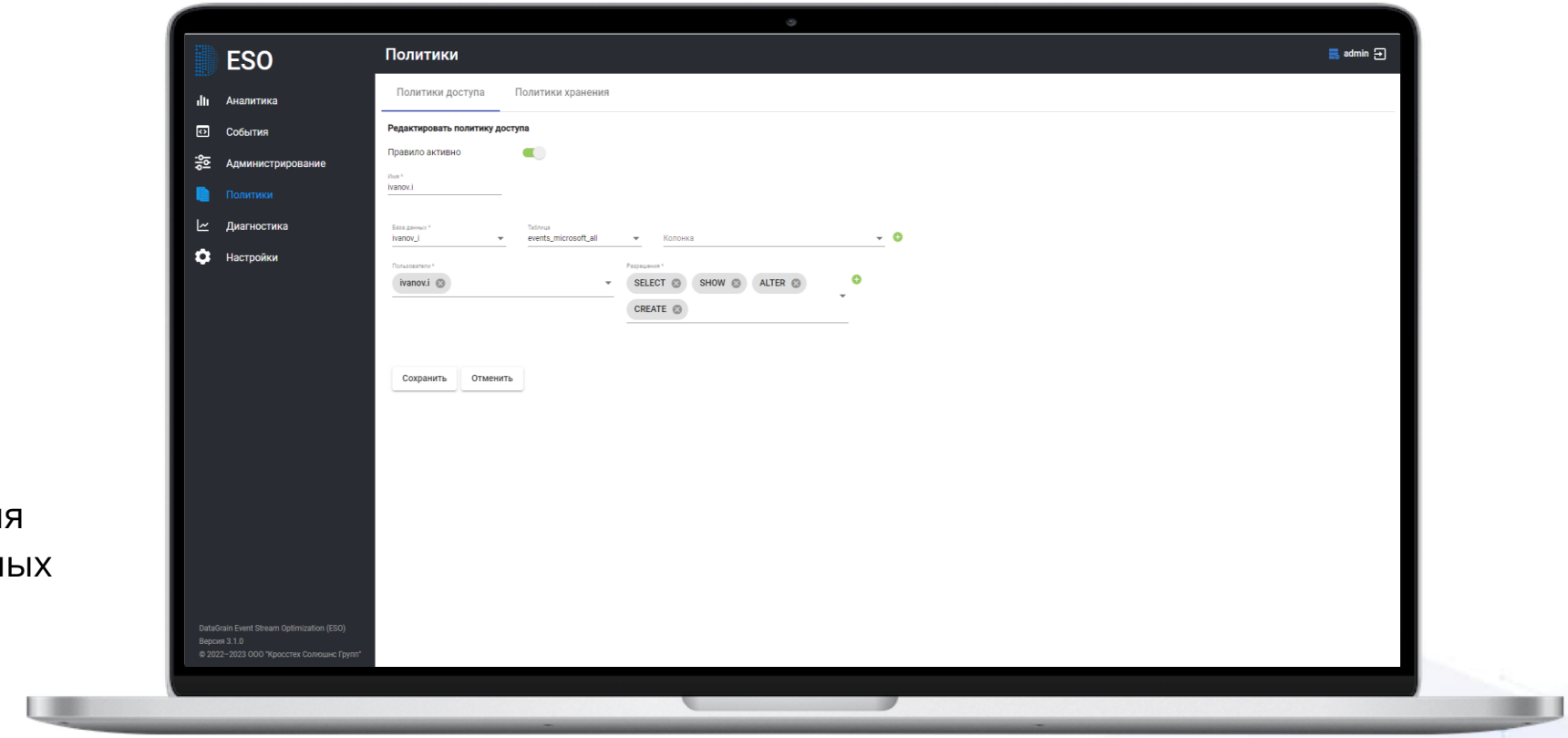
- Мониторинг и анализ приходящих событий для обзора текущего состояния системы
- Пользовательский интерфейс, который позволяет вводить поисковые запросы и просматривать результаты поиска в удобном формате
- Поддержка SQL-запросов, возможность выполнения сложных аналитических запросов и агрегации данных
- Дополнительные возможности оперативного поиска, такие как автодополнение запросов, использования фильтров, сортировки и других функций для более точной настройки вывода результатов



CROSSTECH
SOLUTIONS GROUP

Управление доступом

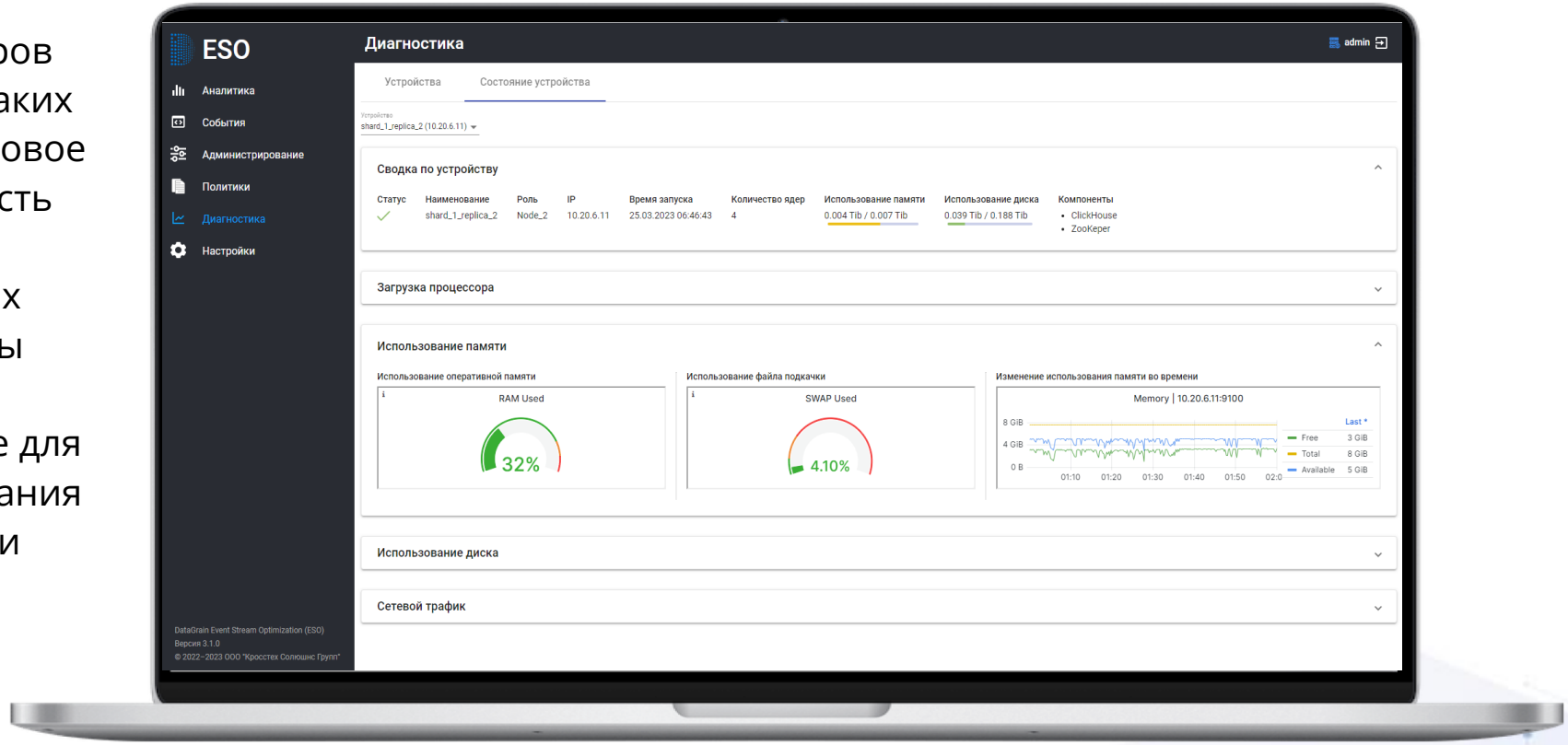
- Создание изолированной базы данных в хранилище для каждого пользователя
- Возможность определения, какие пользователи имеют доступ к определенным базам данных и таблицам
- Возможность определения, какие операции и действия пользователя разрешены в отношении баз данных и таблиц
- Запись и мониторинг действий пользователей с целью обеспечения прозрачности и анализа безопасности



CROSSTECH
SOLUTIONS GROUP

Мониторинг

- Мониторинг основных параметров производительности системы, таких как использование памяти, дисковое пространство и сетевая активность
- Мониторинг доступности важных компонентов и сервисов системы
- Отчеты и аналитические данные для визуализации, анализа и понимания состояния и производительности системы



CROSSTECH
SOLUTIONS GROUP

Кейсы.
№1

Описание ситуации

Субъектам КИИ необходимо соответствовать мере ИНЦ.6 «Хранение и защита информации о компьютерных инцидентах» по Приказу ФСТЭК России № 239

Решение

Решение ESO обеспечивает долгосрочное высокоэффективное хранение событий безопасности с высоким коэффициентом сжатия

Результат

Благодаря ESO компания выполнила требования регулятора и сократила затраты на средства хранения событий безопасности

CROSSTECH
SOLUTIONS GROUP

Кейсы.
№2

Описание ситуации

Компания с крупной инфраструктурой испытывает сложности с процессом расследования инцидентов из-за наличия множества различных СЗИ и решений для хранения логов безопасности

Решение

С помощью решения ESO было реализовано единое централизованное хранилище событий безопасности

Результат

Была повышена эффективность проведения расследований за счет централизации всех журналов безопасности в ESO, обеспечение возможности анализа хранимых данных с использованием пользовательских фильтров, датасетов, витрин (дашбордов)

CROSSTECH
SOLUTIONS GROUP

При возникновении вопросов, пожалуйста, обращайтесь

+7 (495) 532 10 96

Москва, Ленинградский пр. 31А, стр. 1

info@ct-sg.ru