ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«DataGrain Event Stream Optimization (ESO)»

ОПИСАНИЕ ПРОЦЕССОВ

Версия 2.0.0.0

01.2023

ОГЛАВЛЕНИЕ

АННОТАЦИЯ

В данном документе содержится описание процессов, обеспечивающих поддержание жизненного цикла Системы, в том числе устранение неисправностей, выявленных в ходе эксплуатации, совершенствование программного обеспечения, а также информацию о персонале, необходимом для обеспечения такой поддержки.

Настоящий документ носит описательный характер.

1. ОБЩАЯ ИНФОРМАЦИЯ

Система DataGrain Event Stream Optimization (ESO) (далее — Система) предназначена для оптимизации входного потока событий в систему, предназначенную для анализа информации, поступающей от различных других систем, с целью сокращения финансовых затрат на лицензирование системы Security Information and Event Management (SIEM) и IT-оборудование, используемое для долгосрочного хранения данных, и для повышения эффективности и скорости работы ИБ- и бизнес-систем.

Система осуществляет статистический анализ собираемых данных и реализует их долгосрочное хранение в сжатом формате.

Система разработана ООО «Кросстех Солюшнс Групп» (далее — Вендор) в соответствии с требованиями к системам подобного класса. Система работает через web-интерфейс в браузере.

2. ОПИСАНИЕ СИСТЕМЫ

Система автоматизирует управление событиями, собираемыми с целевых источников.

Особенности и возможности Системы:

- современный быстрый Web-интерфейс;
- гибкая настройка правил для поиска событий;
- широкий спектр поддерживаемых источников данных;
- наличие оперативных графиков, диаграмм, таблиц по результатам собираемых, обрабатываемых и передаваемых данных.

Система должна применяться со следующим вспомогательным программным обеспечением:

- RED OS 7.2

Система поддерживает следующие браузеры:

- Google Chrome 49 и выше;
- Microsoft Internet Explorer 11 и выше;
- Mozilla Firefox 45 и выше

3. ЖИЗНЕННЫЙ ЦИКЛ СИСТЕМЫ

Жизненный цикл Системы — это процесс развития, начинающийся со стадии замысла и заканчивающийся прекращением применения (далее — ЖЦ).

Ценность внедрения Системы заключается в следующем:

- сокращение финансовых затрат на лицензирование системы SIEM и IT-оборудование, используемое для долгосрочного хранения данных;
- централизованный сбор, обработка и долгосрочное высокоэффективное хранение событий;
- статистический анализ собираемых и обрабатываемых событий;
- передача отфильтрованных данных на SIEM, а также другие ИБ и бизнес-системы в поддерживаемом формате.

4. ВЕРСИОНИРОВАНИЕ

Система является развивающейся, поэтому ее ЖЦ носит циклический характер, т.е. является последовательностью ЖЦ отдельных версий Системы — ее релизов.

Версии Системы имеют следующий общий вид — A.B.C.D:

- A — номер поколения ПО, повышается в момент выпуска принципиально новой реализации продукта (архитектура, технологический стек);
- B — номер функциональности ПО, повышается в момент выпуска принципиально новой функциональности в масштабе эпика;
- C — номер функции ПО, повышается в момент попадания в релиз новой функциональности в масштабе истории.
- D — номер исправлений, повышается в момент доработок, связанных с исправлением ошибок.

В момент выпуска самого первого по счету релиза проект будет иметь номер 1.0.0.0.

5. ПРОЦЕССЫ, ОБЕСПЕЧИВАЮЩИЕ ПОДДЕРЖАНИЕ ЖЦ

Жизненный цикл Системы рассматривается с точки зрения ГОСТ Р ИСО/МЭК 12207-2010 Процессы ЖЦ программных средств (Information technology, System and software engineering. Software life cycle processes). Процессы ЖЦ реализуются под управлением Сторон, вовлеченных в ЖЦ. Под Стороной понимают одну из тех организаций, которые инициируют или выполняют разработку, эксплуатацию или сопровождение Системы.

Основными сторонами являются:

- Заказчик — конечный пользователь, эксплуатирующий Систему;
- Вендор — разработчик, обеспечивающий разработку, внедрение, модернизацию и сопровождение Системы.

6. ТЕХНИЧЕСКИЕ ПРОЦЕССЫ

6.1. Разработка и совершенствование

Процесс разработки и внедрения — технический процесс, посредством которого потребности пользователей преобразуются в программный продукт. Процесс разработки строится на базе фреймворка Kanban по принципам Agile с управлением задачами в учетной системе Jira. Требования к системе декомпозируются таким образом, чтобы обеспечить возможность реализации каждой отдельной части в виде отдельного Merge Request’a.

При реализации каждая разрабатываемая функция проходит полный жизненный цикл:

- Анализ;
- Проектирование;
- Разработка;
- Тестирование.

Результат каждой итерации анализируется и корректирует план следующей итерации. Каждый компонент Системы разрабатывается силами отдельных команд.

Команды укомплектованы специалистами, которые гарантируют полный цикл реализации требований к компоненту без привлечения внешних специалистов:

- владелец продукта как источник знания о бизнес-требованиях;
- разработчики;
- тестировщики;
- аналитики необходимой квалификации.

Бизнес-требования заводятся в учетной системе Confluence в виде описания. Исходя из описания производится декомпозиция на измеримые задачи для программирования.

Каждая задача разрабатывается в отдельной ветке в Git. После проведения функционального тестирования и стабилизации, соответствующая

ветка сливается с веткой Master. В конце каждой итерации основная ветка разработки проходит тестирование для подтверждения общей работоспособности Системы.

Перед релизом все компоненты системы развертываются совместно для релизного оценочного тестирования Системы. На базе результатов тестирования в соответствии с критериями качества принимается решение о выпуске релиза или возвращении Системы на доработку.

Инсталляция Системы осуществляется Вендором или Заказчиком самостоятельно.

В случае необходимости может быть рассмотрена возможность доработки системы на основании рекомендаций от службы поддержки, а также пожеланий от конечных пользователей, которые фиксируются службой клиентской поддержки в специализированной аналитической системе.

6.2. Внедрение

Заказчик, получив дистрибутивы от Вендора, организует развертывание Системы в своей инфраструктуре. Система передается Заказчику в рамках договора на внедрение.

Процесс внедрения и доработка функционала под требования Заказчика, а также процесс функционирования, сопровождения и устранения возникающих ошибок производится в соответствии с договором на внедрение. При необходимости Вендор оказывает требуемую помощь и устраняет возникающие ошибки.

Основные цели и задачи внедрения:

- развертывание Системы в инфраструктуре Заказчика;
- подключение пользователей Заказчика к Системе;
- адаптация настроенных бизнес-процессов и процедур под требования Заказчика;
- интеграция Системы с другими системами и сервисами Заказчика;
- передача и разработка всей необходимой документации;

– обучение персонала Заказчика использованию и поддержке Системы.

6.3. Документирование

Процесс управления документацией является неотъемлемой частью всех стадий и этапов ЖЦ Системы. Документирование происходит одновременно с процессами проектирования и разработки каждого из релизов Системы или после них.

Заказчику в составе дистрибутивов предоставляется документация в составе:

– Документация на ESO.

После внедрения Системы Заказчику предоставляется следующая отчетная документация по проекту:

– Инструкция по установке;
– Руководство суперадминистратора;
– Руководство администратора;
– Руководство руководителя;
– Руководство офицера ИБ;
– другие документы по согласованию.

6.4. Управление развертыванием

Развертывание и сборка исходных кодов Системы поддерживается системой управления версиями Gitlab. Для сборки Компонентов на основе исходных кодов используется сервер непрерывной интеграции (CI), который позволяет быстро выявлять проблемы интеграции, немедленно прогонять тесты для свежих изменений, а также вместе с текущей стабильной версией иметь другие версии сборок — для тестирования, демонстрации и других действий.

6.5. Поддержка и сопровождение

Гарантийная поддержка Системы осуществляется Вендором. Срок гарантийной поддержки определяется договором на внедрение Системы.

Плановое техническое сопровождение внедренной Системы осуществляется специалистами Заказчика. При необходимости Заказчик может обратиться за поддержкой к Вендору.

6.6. Обеспечение гарантии качества

Обеспечение качества программного обеспечения (англ. Software quality assurance, SQA) — набор процедур мониторинга разработки программного обеспечения и методов, используемых для обеспечения его качества.

Руководство по качеству при разработке Вендора (далее — РК) основано на требованиях стандартов Системы менеджмента качества ГОСТ Р ИСО 9000-2015, 9001-2015, 9004-2010, 19011-2003, 10005-2007.

Управление качеством разрабатываемой Системы обеспечивается условиями договорных отношений с Заказчиками в соответствии с требованиями ГОСТ Р ИСО 9001-2015 и контролируется соответствующими службами и структурными подразделениями Вендора.

Процесс проверки качества Системы осуществляется в соответствии с запланированными мероприятиями, что удостовериться, что получаемые в результате разработки Системы результаты соответствуют поставленным целям и задачам. Проверка завершается до официального выпуска релиза Системы.

Процедуры обеспечения качества у Вендора охватывают весь цикл разработки Системы, включая такие процессы как:

- определение требований;
- проектирование;
- разработка;
- контроль исходного кода;
- анализ кода;

– конфигурационное управление;
– тестирование;
– управление релизами;
– интеграция продуктов.

Процедуры обеспечения качества включают:

– цели;
– возможности;
– процедуры;
– измерения;
– проверки.

6.7. Тестирование

Для определения полноты соответствия установленных функциональных требования и созданного релиза у Вендора организованы следующие процессы тестирования:

– функциональное тестирование (functional testing);
– системное тестирование (system testing);
– регрессионное тестирование (regression testing);
– модульное тестирование (unit testing).

6.8. Устранение неисправностей, выявленных в ходе эксплуатации

Проблемы, возникающие в процессе эксплуатации регистрируются в специализированной аналитической системе. Данная система используется не только Службой поддержки, но и другими структурными подразделениями. В данную систему также поступают все типы замечаний и пожеланий независимо от их источника возникновения.

Собранные проблемы категоризируются по критичности для использования Системы и по распространенности данной проблемы. Категоризированные проблемы, которые можно решить силами Службы поддержки Вендора, добавляются в Базу знаний. Для вновь выявленных

проблем, которые не могут быть решены силами Службы поддержки, формируется заявка на разработку. В некоторых случаях может быть разработано временно решение, реализуемое Службой поддержки и смягчающее остроту проблемы (hotfix), но не решающее проблему в полном объеме, тогда это временное решение добавляется в Базу знаний Службы поддержки.

7. ИНФОРМАЦИЯ О ПЕРСОНАЛЕ

7.1. Повышение квалификации персонала

Вендор обладает высококвалифицированной командой с опытом разработки программных продуктов и утили на языке C#. Все специалист компании проходят обучение, а также постоянно совершенствуют свои навыки с квалификацией.

Вендор уделяет значительное внимание повышению квалификации своих сотрудников. Необходимый уровень знаний, умений и навыков, как требование к каждой должности, определяется моделью профессиональных и личных компетенций, принятой для соответствующей позиции в Компании (hard/soft skills' model).

Цель повышения квалификации персонала — поддержание и повышение уровня квалификации персонала с учетом требований компаний к определенной должности, роли.

7.2. Информация о персонале, необходимом для обеспечения поддержки

Для работы с Системой необходимы следующие специалисты:

- **Пользователь Системы** — специалист (служащий организации) Заказчика, использующий Систему для осуществления собственных ежедневных трудовых функций;
- **Администратор Системы** — специалист ИТ-подразделения Заказчика, ответственный за корректную работу прикладных сервисов внутри организации, а также оказывающий внутреннюю поддержку пользователей при работе с Системой;
- **Инженер** — инженер ИТ-подразделения Заказчика, осуществляющий работы по технической поддержке Системы на территории Заказчика.

– **Администратора ОС (Системный администратор)** — специалист ИТ-подразделения Заказчика, ответственный за корректную работу базовых сервисов внутри организации (операционные системы, сетевая инфраструктура, политики безопасности).

Общая численность персонала, относящегося к перечисленным категориям, зависит от специфики решаемых прикладных задач, масштаба Системы и количества одновременно работающих пользователей.

Обучение Персонала Заказчика возможностям и методикам настройки Системы может выполняться Вендором в рамках проекта по внедрению Системы на завершающих этапах и обычно занимает от одного до нескольких дней (в зависимости от категории пользователя).

Первичный инструктаж пользователей по работе с Системой осуществляется в форме демонстрации ключевых особенностей Системы и ее использования на рабочем месте пользователя. Инструктаж может быть проведен в дистанционной (вебинар) или очной формах. Обучение Администраторов и Инженеров работе с Системой и ее развертыванию осуществляется в рамках проекта внедрения.

В ходе обучения слушатели знакомятся с возможностями поддержки и настройки. Обучение может быть проведено в очной и дистанционной (вебинар) формах. В зависимости от уровня подготовки слушателя длительность курса может быть скорректирована в соответствии с программой обучения, утвержденной Вендором.