



Программный комплекс «Security Data Lake»

Описание функциональных характеристик

Разработал:
Станислав Прищеп

История изменений документа

Редактировал	Версия	Дата	Комментарий
Станислав Прищеп	1.0	04.10.2023	Начальная версия
Станислав Прищеп	1.1	29.08.2025	Добавлены модули «Сводный перечень активов» и «Адаптивные действия»

Содержание

1	Назначение и область применения	4
2	Функциональные возможности	4
3	Архитектура программного комплекса	4
4	Эксплуатационные характеристики	5
5	Описание функциональной части программного комплекса	5
6	Информация, необходимая для установки и эксплуатации	5

1 Назначение и область применения

Программный комплекс «Security Data Lake» предназначен для мониторинга и анализа машинных данных, выявления и регистрации инцидентов, выполнения действий по реагированию и расследованию инцидентов.

Область применения включает в себя корпоративные и промышленные сети и системы обработки и передачи данных.

2 Функциональные возможности

Программный комплекс реализует следующие функции:

- SDL:
 - централизованный сбор событий с компонентов вычислительной инфраструктуры;
 - мониторинг событий и обнаружение инцидентов;
 - управление инцидентами;
 - расследование инцидентов;
 - отображение сводных статистических данных о состоянии корпоративной сети;
- программный модуль "Адаптивные действия":
 - агрегация данных об активах (узлах сети и учётных записях);
- программный модуль "Сводный перечень активов":
 - автоматизация действий по реагированию на инциденты.

3 Архитектура программного комплекса

Security Data Lake представляет собой программный комплекс, включающий в себя:

- SDL:
 - брокер данных;
 - средства автоматической предобработки данных в режиме реального времени;
 - средства хранения и анализа данных;
 - средства автоматизации развёртывания и управления инсталляцией;
 - специализированные программные расширения для интеграции и реализации прикладных функций;
- программный модуль "Адаптивные действия":
 - специализированные программные расширения для интеграции и реализации прикладных функций;
- программный модуль "Сводный перечень активов":

- специализированные программные расширения для интеграции и реализации прикладных функций.

4 Эксплуатационные характеристики

Для использования программного комплекса «Security Data Lake» необходимо, чтобы рабочее место соответствовало следующим требованиям:

- функционирующая операционная система, например, Windows 10 и выше, macOS High Sierra 10.13 и старше, Ubuntu 14.04 и старше;
- процессор — 4 ядра;
- рекомендуемая оперативная память — от 512 Мбайт;
- подключение к интернету — не менее 10 Мбит/с;
- интернет-браузеры — Mozilla Firefox актуальной версии или двух предыдущих версий.

5 Описание функциональной части программного комплекса

Языки программирования: Java, TypeScript, JavaScript.

БД - Opensearch 2.19.

СУБД - Opensearch 2.19.

6 Информация, необходимая для установки и эксплуатации

Для установки и правильной эксплуатации программного комплекса «Security Data Lake» необходимо ознакомиться с Инструкцией пользователя по настройке и эксплуатации ПО «Security Data Lake», размещенной на сайте ООО «СТЭП ЛОДЖИК».

Для активации программного обеспечения необходимо обратиться к технической поддержке ООО «СТЭП ЛОДЖИК».

Техническая поддержка:

Пн-Пт, 9:00-18:00 по МСК

Тел.: +7 495 775 31 23

Адрес электронной почты: sc_support@step.ru