ООО «СОВРЕМЕННЫЕ АЛГОРИТМЫ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
Email Security Solution

ОПИСАНИЕ ФУНКЦИОНАЛЬНЫХ ХАРАКТЕРИСТИК

На 8 листах

2023

Аннотация

Настоящий документ является описанием функциональных характеристик программного обеспечения Email Security Solution.

Положения настоящего документа разработаны в соответствии с Правилами формирования и ведения единого реестра российских программ для электронных вычислительных машин и баз данных и единого реестра программ для электронных вычислительных машин и баз данных из государств - членов Евразийского экономического союза, за исключением Российской Федерации (утв. постановлением Правительства РФ от 16 ноября 2015 г. № 1236), в соответствии с ГОСТ 34 РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов» — в части структуры и содержания документов, а также в соответствии с ГОСТ 19 «Единая система программной документации (ЕСПД)» — в части общих требований и правил оформления программных документов.

Содержание

1 ВВЕДЕНИЕ

1.1 Область применения

Email Security Solution - программа архивации, полнотекстового поиска и репутационных проверок электронной почты и может применяться в корпоративных сетях организаций/предприятий, частных почтовых серверах.

1.2 Краткое описание возможностей

ESS обеспечивает выполнение функций хранения, поиска, просмотра и анализа больших объемов данных электронной почты, позволяет производить поиск по отправителю, получателю, теме письма и вложению, осуществлять скачивание писем и вложений.

Заложена функция просмотра активности пользователей для ролей администратора или супервайзера. Антифишинговая часть программы оценивает электронные письма на причастность к фишинговой атаке, основываясь на анализе заголовков, ключевых слов и вложений.

2 ФУНКЦИОНАЛЬНЫЕ ХАРАКТЕРИСТИКИ

2.1 Основной поиск

Основной интеллектуальный поиск позволяет провести быструю выборку по определенной фразе или составить сложный запрос с использованием различных опций.

При работе с интеллектуальным поиском вы можете использовать логические операторы «И, ИЛИ, НЕ» (AND, OR, NOT), символы подстановки (* и ?), поиск с заданным расстоянием между словами, а также наименования полей. Так в запросе можно указать, какие именно слова, в каком порядке и по каким полям следует искать. При вводе слов через пробел, по умолчанию система воспринимает их связанными логическим оператором «И». Поисковые результаты будут содержать все слова из запроса.

Язык запросов поддерживает:

1. Поиск точного слова или фразы.
2. Логический оператор И.
3. Логический оператор ИЛИ.
4. Логический оператор НЕ.
5. Поиск слова с переменным окончанием.
6. Поиск слова с одним переменным символом.
7. Поиск с заданным расстоянием между словами.
8. Поиск по заданным полям.

2.2 Расширенный поиск

Позволяет провести выборку по фиксированному набору полей: отправитель, получатель, тема, тело письма, имя вложения, тело вложения, временной период. Возможно сочетать различные поисковые поля и использовать язык запросов внутри некоторых из них.

Расширенный поиск позволяет просмотреть входящие и исходящие письма избранного пользователя, а также письма пользователя самому себе.

2.3 Просмотр поисковых результатов

Поисковые результаты отображаются в виде многостраничной таблицы и содержат поля «Дата», «Отправитель», «Получатель», «Тема письма», «Размер», «Вложения», «Скоринг».

Доступна сортировка по возрастанию и убыванию в полях «Дата» и «Размер».

Функциональные возможности просмотра поисковых результатов:

1. Превью писем. В поисковых результатах возможно просмотреть каждое письмо в режиме превью, по клику на строке с данными письма. Одновременный просмотр нескольких писем в режиме превью невозможен, при просмотре следующего письма предыдущее сворачивается автоматически. В режиме превью доступно скачивание вложений в едином архиве или по отдельности.
2. Просмотр писем в новой вкладке. Доступен по клику на соответствующую иконку в правой части строки с данными письма. При просмотре письма в отдельной вкладке также доступно скачивание вложений в едином архиве или по отдельности, отображение скоринга и технических заголовков письма.
3. Скачивание писем. Возможна загрузка одного или нескольких писем на странице поисковых результатов в соответствии с проставленными отметками в чек-боксах и после нажатия во всплывающем сообщении кнопки «Скачать». Также возможно скачать письмо в новой вкладке, нажав на соответствующую кнопку.
4. Скачивание вложений. Скачать любое вложение возможно двумя способами - в режиме превью или из письма в новой вкладке. При сохранении вложения автоматически попадают в папку Загрузки на локальном ПК.

2.4 Скоринговая система

Скоринговая система оценивает потенциальную относимость письма к фишинговой атаке. Основана на анализе технических заголовков, тела письма и вложений в соответствии со следующими метриками.

Метрики скоринговой системы:

1. SPF. Механизм для проверки подлинности сообщения путем проверки сервера отправителя.
2. DKIM. Метод e-mail аутентификации, основанный на проверке подлинности цифровой подписи.
3. WHOIS. Сетевой протокол, используемый для получения регистрационных данных о владельцах доменных имён.
4. SCAM. Поиск в теме, теле письма и во вложении ключевых слов, наиболее часто используемых в фишинговых письмах.
5. AB_NEW. Тест, который определяет, является ли внешний отправитель новым для

получателя.

6. AB_SIMILAR. Оценка сходства адреса нового отправителя с иными контактами получателя.
7. ENCRYPTED. Проверка наличия зашифрованного архива во вложении.
8. LINK. Проверка наличия ссылки в теле письма.
9. SCAM_FROM. Проверка подмены описания отправителя в поле From корпоративным доменом.

В результате тестов скоринговая система присваивает письму уровень риска: низкий, средний или высокий, обозначается зеленым, желтым или красным цветом соответственно. Скоринг отображается в поисковых результатах, а также при просмотре письма в отдельной вкладке.

2.5 Личный кабинет

Функционал личного кабинета:

1. Смена пароля
2. История входов в систему с фиксацией пользователя, успеха или отказа входа, причины отказа, а также времени события.

2.6 Раздел администратор

Раздел «Администратор» предназначен для управления системой. Состоит из подразделов: активность пользователей и показатели здоровья системы. Также доступно управление пользователями через отдельный продукт IDM Keycloak.

Функциональность подраздела активности пользователей:

1. Просмотр содержимого поисковых запросов и просмотренных результатов. Активность пользователей отображается в виде многостраничной таблицы с полями «Дата», «Пользователь», «Действие», «Субъект». Одно действие пользователя соответствует одной записи в таблице. Если пользователь совершал последовательные однотипные действия, такие как переключение страниц результатов поиска - переход на каждую из этих страниц регистрируется отдельно. Количество поисковых результатов и номер страницы, открытой пользователем, отображается администратору или супервайзеру в

поле «Субъект».

2. Просмотр действий пользователей. Действия пользователей разделены на группы, каждому действию соответствует свой тип отображения данных. При нажатии на описание со стрелкой отображаются данные о действии пользователя. Виды действий и их отображение:
    1. Поиск основной (копия запроса и результатов поиска).
    2. Поиск расширенный (копия запроса и результатов поиска).
    3. Превью письма (письмо).
    4. Письмо в новом окне (письмо).
    5. Сохранено письмо (письмо).
    6. Сохранен архив писем (список сохраненных писем).
    7. Сохранено вложение (письмо).
    8. Сохранен архив вложений (письмо).
3. Поиск по активности пользователей и фильтрация результатов. Поиск в массиве логов осуществляется по пользователю или тексту его запроса.

Функциональность подраздела здоровье системы:

1. Состояние сервисов. Отражает доступность архитектурных компонентов системы, а также состояние аппаратного обеспечения главного сервера. Возникновение критических статусов отображается красным индикатором в пункте меню «Состояние сервисов» и на иконке раздела «Администратор».

2. Журнал алертов. Хранит список системных событий с временными метками, события могут быть отсортированы по типу. Журнал фиксирует начало недоступности любого из сервисов (красный) и время его восстановления (зеленый). Также в журнале отражаются события, имеющие статус предупреждений (желтый).

Управление пользователями

Для того чтобы создавать, редактировать, удалять пользователей и их права, воспользуйтесь переходом в IDM Keycloak в соответствующем меню раздела «Администратор».