Программный комплекс «Security Data Lake»

Инструкция пользователя по настройке и эксплуатации системы

Разработал:
Станислав Прищеп

История изменений документа

Редактировал	Версия	Дата	Комментарий
Станислав Прищеп	1.0	04.10.2023	Начальная версия

Содержание

1 Введение

1.1 Для кого предназначено это руководство

Инструкция включает в себя сведения для следующих функциональных ролей Пользователей:

- Аналитик первой линии;
- Аналитик второй линии;
- Аналитик третьей линии;
- Руководитель Центра мониторинга.

Аналитик первой линии осуществляет первоочередные действия по реагированию на выявленные Системой инциденты и имеет доступ к функциям системы по редактированию статусов инцидентов, отправке карточек инцидентов, поиску исходных событий с использованием преднастроенных дашбордов.

Аналитик второй линии дополнительно к функциям Аналитика первой линии осуществляет действия по детальному анализу исходных событий, созданию и участию в расследованиях, исключению ложных срабатываний с использованием функций глушения.

Аналитик третьей линии дополнительно к функциям Аналитика второй линии осуществляет действия по ретроспективному анализу событий и выявлению инцидентов с использованием кастомных визуализаций и дашбордов, аудиту срабатывания правил глушений, разработке и добавлению в Систему фильтров исключений для алгоритмов корреляции.

Руководитель осуществляет действия по контролю ключевых показателей, аудиту анализа инцидентов и аудиту расследований, выявлению отклонений от заданных значений SLA.

1.2 Термины, определения и сокращения

Автоматизированная система — организационно-техническая система, состоящая из средств автоматизации определенного вида или нескольких видов деятельности людей и персонала, осуществляющего эту деятельность.

Актив — всё, что имеет ценность для организации в интересах достижения целей деятельности и находится в её распоряжении.

Артефакт угрозы — любая информация об угрозе.

Визуализация — элемент интерфейса для графического наглядного отображения данных в виде графиков, гистаграмм, круговых диаграмм, таблиц, карт, текстовых блоков и др.

Датасет модели данных — составной элемент датамодели, представляющий собой подмножество полей данных относящихся к одной категории.

Дашборд — страница интерфейса, на которой размещен набор панелей визуализаций.

Инцидент — любое непредвиденное или нежелательное событие, которое влечет негативные последствия для деятельности организации.

Модель данных (датамодель) — структура полей, применимая к необработанным данным для упрощения их использования. Каждая модель данных указывает на категорию данных исходного события. Составным элементом датамодели является датасет.

Область мониторинга — территориальные объекты, информационные системы и компоненты ИТ-инфраструктуры Заказчика, осуществляющие передачу событий в Центр мониторинга Исполнителя.

Панель визуализации — место размещения визуализации на дашборде.

Правило корреляции — поисковый запрос и алгоритм обработки его результатов.

Рабочее пространство — логическая сущность, связывающая воедино набор других сущностей (дашбордов, визуализаций, служебных индексов, индекс-паттернов, ролей пользователей, настроек), предоставляемая и индивидуально настраиваемая в соответствии с потребностями отдельной группы пользователей Security Data Lake.

Событие — идентифицированное появление определённого состояния системы, сервиса или сети.

Сценарий мониторинга событий — комплекс мер выявления и реагирования на инциденты, включающий в себя алгоритм обнаружения инцидентов, правила формирования контекста инцидента, плейбука реагирования на инцидент и рекомендаций по обработке инцидента.

Угроза — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения.

Центр мониторинга — автоматизированная система, включающая взаимоувязанный комплекс организационных процессов, программно-технических средств и персонала.

Events Per Second (EPS) — количество событий в секунду, поступающих в Центр мониторинга.

SDL — Security Data Lake.

2 Техническая поддержка

Техническая поддержка:

Пн-Пт, 9:00-18:00 по МСК

Тел.: +7 495 775 31 23

Адрес электронной почты: sc_support@step.ru

Веб-портал: https://service.step.ru

3 Об инструкции пользователя

Данная инструкция содержит описание пользовательских интерфейсов и основные возможности по работе с системой Security Data Lake (SDL).

SDL предназначена для автоматизации центра мониторинга.

Задачи системы:

- мониторинг событий;
- выявление и регистрация инцидентов;
- обеспечение действий по реагированию и расследованию инцидентов.

4 Функции SDL

4.1 Регистрация

Для регистрации пользователя необходимо обратиться, в службу техподдержки по электронной почте на адрес sc_support@step.ru с просьбой о регистрации в системе нового пользователя. В письме указать:

1. Роль пользователя в системе (Аналитик первой линии/ Аналитик второй линии/ Аналитик третьей линии / Руководитель центра мониторинга).
2. Фамилию Имя и Отчество пользователя.
3. E-mail адрес пользователя.
4. IP-адрес или диапазон IP-адресов, с которых будет осуществляться доступ к системе.

После регистрации в системе логин и пароль высылается на адрес электронной почты.

4.2 Вход в систему

Доступ пользователя к Системе осуществляется через веб-интерфейс по адресу: https://sdl.soc.step.ru/slsdl. В качестве веб-браузера поддерживаются актуальные версии Firefox, Chrome, Safari (Mac), Edge Chromium.

Для входа в Систему необходимо (Рисунок 1):

1. Открыть веб-браузер.
2. Перейти по адресу: https://sdl.soc.step.ru/slsdl.
3. В появившемся окне подтвердить свою личность с помощью полученного логина и пароля.

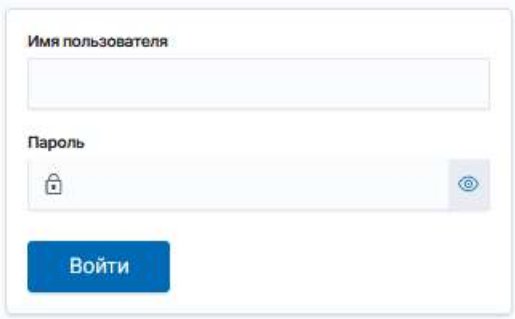


Рисунок 1. Вход в Систему

4.3 Смена пароля

Для смены пароля, после входа в систему, необходимо:

1. Нажать на изображение инициалов текущего пользователя в правом верхнем углу пользовательского веб-интерфейса.
2. Нажать «Сбросить пароль».
3. В появившемся окне задать новый пароль своей учётной записи.

4.4 Выход из системы

Для смены пароля, после входа в систему, необходимо:

1. Нажать на изображение инициалов текущего пользователя в правом верхнем углу пользовательского веб-интерфейса.
2. Нажать «Выйти».

4.5 Использование системы

Security Data Lake предоставляет руководителям и специалистам центров мониторинга набор инструментов анализа больших массивов машинных данных для наблюдения за состоянием защищённости вычислительной сети и управления инцидентами. Продукт реализует принцип единого окна доступа к данным о событиях, активах, угрозах и инцидентах, обеспечивает их наглядное представление и корреляцию.

4.5.1 Анализ инцидентов

4.5.1.1 Обзор функций анализа инцидентов

В Security Data Lake просмотр инцидентов и их обработка осуществляются на дашборде **Анализ инцидентов**.

Каждый инцидент указывает на одно или несколько событий, обнаруженных с помощью правил корреляции. Например, инцидент может быть создан при обнаружении:

- аномального всплеска ошибок доступа;

- единичного события, указывающего на использование административных функций;
- сетевого соединения с узлом из списка известных угроз.

Для обработки инцидентов дашборд снабжён функциями, позволяющими оценивать срочность инцидента, осуществлять поиск по инцидентам, назначать инциденту ответственного, менять статус обработки инцидента, изучать детали инцидента и выполнять другие первоочередные действия.

4.5.1.1.1 Как Security Data Lake обнаруживает инциденты

Для обнаружения инцидентов Security Data Lake периодически запускает правило корреляции, которое осуществляет поиск среди загруженных в систему данных и обрабатывает результаты поиска по заданному алгоритму. Когда правило корреляции обнаруживает заданную закономерность, то создаётся новый инцидент.

4.5.1.1.2 Рабочий процесс обработки инцидентов

Процесс обработки инцидентов с помощью дашборда **Анализ инцидентов** может учитывать принятые в организации правила и рабочие процессы. Ниже приведён пример такого рабочего процесса.

1. Старший Аналитик первой линии отслеживает статусы инцидентов на дашборде **Анализ инцидентов**, используя встроенные возможности сортировки и фильтрации.
2. Когда инцидент требует реагирования, старший Аналитик назначает инциденту владельца — одного из младших Аналитиков первой линии.
3. Младший Аналитик (текущий владелец инцидента) обновляет статус инцидента с **Новый** на **Выполняется** и приступает к действиям по реагированию на инцидент.
4. Младший Аналитик (текущий владелец инцидента) анализирует инцидент, собирает дополнительную информацию о нём и отмечает результаты своих действий в поле **Комментарий**. В рамках реагирования на инцидент владелец может также запускать настроенные адаптивные действия. Если реагирование покажет, что инцидент нуждается в более детальном анализе, Аналитик может добавить инцидент к расследованию.
5. После того как младший Аналитик (текущий владелец инцидента) решит все задачи по реагированию, он устанавливает инциденту статус **Решён**.
6. Младший Аналитик (текущий владелец инцидента) передаёт решённый инцидент на проверку, для этого назначает ему нового владельца — старшего Аналитика.
7. Старший Аналитик (текущий владелец инцидента) проверяет и подтверждает результаты реагирования и устанавливает инциденту статус **Закрыт**.

4.5.1.2 Поиск и редактирование инцидентов

Следует использовать дашборд **Анализ инцидентов** для поиска и редактирования инцидентов как части рабочего процесса по их обработке. Здесь есть возможность применить и сохранить дополнительные фильтры отображения инцидентов, выполнить поисковый запрос, назначать ответственного за инцидент и фиксировать его статус.

4.5.1.2.1 Применение фильтров и тегов

Для быстрого поиска инцидентов на дашборде могут применяться сортировка, фильтры по значениям полей и тегам. Все отображаемые инциденты содержат поля **Время**, **Срочность**, **Статус** и **Владелец**, которые помогут отслеживать и ранжировать инциденты. Например, чтобы сосредоточиться на анализе последних зарегистрированных инцидентах, в качестве фильтра можно задать временной диапазон. А чтобы просмотреть необработанные инциденты — задать фильтр по полю **Статус**.

Чтобы ускорить анализ инцидента и поиск схожих инцидентов на дашборде есть возможность добавления тегов значениям полей инцидента. Чтобы добавить значению тег, необходимо вызвать меню действий с одним из дополнительных полей инцидента и нажать **Редактировать тег**. Для фильтрации по тегам использовать фильтр **Поиск по тегу**.

Есть возможность быстро отфильтровать инциденты, используя предустановленные панели фильтрации. Например, при выборе поля **Правило корреляции** отобразится выпадающий список с перечнем встречающихся в инцидентах правил. Указав в поле первые буквы правила корреляции, отобразятся варианты начинающихся с них названий правил. По мере ввода наименования правила корреляции, доступные для выбора значения, будут обновляться.

4.5.1.2.2 Назначение инцидента

Есть возможность назначить владельца сразу одному или нескольким инцидентам.

1. Выбрать один инцидент или несколько инцидентов.
2. Нажать **Редактировать выбранные**.
3. В поле **Владелец** выбрать ответственного, которому необходимо назначить инцидент или инциденты.
4. Нажать **Сохранить**.

4.5.1.2.3 Обновление статуса инцидента

Сразу после создания все инциденты имеют статус **Новый**. По мере того как инцидент проходит разные стадии обработки, в соответствии с принятым в организации рабочим процессом, его статус можно изменять.

1. Выбрать один или несколько инцидентов и нажать **Редактировать выбранные**. Чтобы выполнить действие со всеми найденными инцидентами, нажать **Редактировать все * инциденты**.
2. В окне **Редактировать инциденты** указать необходимые значения.
3. При необходимости добавить комментарий, чтобы описать результаты действий с инцидентом.
4. Сохранить изменения.

Настройками системы может быть задано условие об обязательном комментировании при редактировании инцидентов. В таком случае потребуется ввести комментарии заданной длины.

Примечание — Если отредактированный инцидент пропал с дашборда, необходимо проверить применённые поисковые запросы и фильтры. Например, если установлен фильтр для отображения только инцидентов со статусом «Новый» после того, как пользователь изменил статус инцидента на «Выполняется» он перестанет отображаться, пока не будет удалён или отключён соответствующий фильтр.

Есть возможность выбрать один из следующих статусов инцидента (Таблица 1).

Таблица 1. Статус инцидента

Статус	Описание
Новый	Статус по умолчанию для всех новых инцидентов. Означает, что обработка инцидента не проводилась
Выполняется	Владелец выполняет действия по реагированию на инцидент
Решён	Владелец выполнил необходимые действия по реагированию, инцидент ожидает проверки
В ожидании	По инциденту необходимо выполнить действия до его закрытия
Закрыт	Обработка инцидента завершена

Наименования статусов инцидентов и их описания задаются параметрами системы и могут быть изменены в соответствии с принятыми в организации правилами и рабочими процессами.

4.5.1.2.4 Уровни срочности инцидентов

Уровень срочности инцидента указывает на приоритет его обработки. Срочность может принимать следующие значения:

- информационная;
- низкая;

- средняя;
- высокая;
- критическая.

При создании инцидента ему автоматически назначается уровень срочности, исходя из значения критичности правила корреляции и максимального приоритета (ценности) затронутых инцидентом сетевых узлов и учётных записей (см. п. 4.5.1.6).

В ходе обработки инцидента уровень его срочности может быть изменён вручную.

4.5.1.3 Просмотр деталей инцидента

После того, как инцидент обнаружен, необходимо выяснить детали его возникновения. Для этого в инцидент при регистрации помещается связанный с ним контекст и ссылки, включая дополнительные поля, связанные события и сценарий действий по реагированию.

Необходимо нажать на стрелку слева от имени инцидента, чтобы развернуть и просмотреть его более детально в виде карточки.

- ознакомиться с описанием инцидента и зарегистрированными в нём дополнительными полями данных в разделе **Описание**;
- следовать сценарию по реагированию на инцидент, приведённому в разделе **Реагирование:**, если он был задан в правиле корреляции, создавшем инцидент;
- нажать **Посмотреть все действия с инцидентом** разделе **История**, чтобы просмотреть все действия по обработке инцидента, включая комментарии, события изменения статуса, владельца и срочности;
- в разделе **Связанные расследования** просмотреть перечень расследований, к которым инцидент в настоящее время добавлен. Нажать на название расследования, чтобы его открыть;
- перейти по ссылке в разделе **Правило корреляции** для просмотра корреляционного правила, которым инцидент был обнаружен;
- перейти по ссылке в разделе **Связанные события**, чтобы просмотреть исходные события, на основании которых инцидент был создан;
- если основанием для создания инцидента выступало только одно событие, оно будет отображено в оригинальном виде в разделе **Исходное событие**;
- просмотреть историю выполненных с инцидентом адаптивных действий в разделе **Адаптивные действия**, в том числе чтобы убедиться, что они выполнены успешно.

4.5.1.3.1 Почему для некоторых инцидентов могут отсутствовать связанные события?

Правила корреляции, в зависимости от заданного в них алгоритма, могут регистрировать инцидент как на основе наличия событий, так и при условии их отсутствия. Например, правило «Отсутствуют события от источника» обнаруживает отсутствие в системе событий от узла в течение заданного интервала времени.

В инциденте, зарегистрированном таким правилом, при переходе по ссылке в разделе **Связанные события** исходных событий может быть не найдено. Чтобы найти точное время, когда искомые данные поступали последний раз, можно попробовать расширить просматриваемый временной интервал. Но, возможно, что данные так и не будут найдены, если они никогда не поступали или максимальная длительность их хранения была превышена и они были удалены.

4.5.1.3.2 Цепочки инцидентов

Цепочки инцидентов представляют собой последовательность инцидентов, связанных между собой значениями заданных полей.

Для их отображения на дашборде **Анализ инцидентов** используется индивидуальный формат, включающий в себя сводные данные полей исходных событий и перечень исходных инцидентов с возможностью перехода к карточкам исходных инцидентов.

4.5.1.4 Реагирование на инцидент

После просмотра и анализа деталей инцидента возникает необходимость выполнить действия по реагированию на него, например, в соответствии с описанным в инциденте сценарием реагирования. К действиям по реагированию относятся: глушение инцидента, передача информации об инциденте, добавление одного или сразу нескольких инцидентов в расследование, или сбор дополнительного контекста инцидента и выполнение адаптивных действий.

4.5.1.4.1 Выполнение адаптивных действий

Исходя из имеющейся информации об инциденте, можно запустить настроенные в системе адаптивные действия. Такими действиями могут быть, например, запросы к внешним системам для сбора дополнительной информации, выполнения на них заданных функций или отправки данных из инцидента.

Для запуска адаптивного действия:

1. Нажать на многоточие в столбце **Действие** справа от имени инцидента.
2. Выбрать одно из адаптивных действий.
3. Заполнить форму ввода данных адаптивного действия, если появилось соответствующее окно.

Чтобы удостовериться в успешном выполнении адаптивного действия можно раскрыть инцидент и проверить статус в разделе **Адаптивные действия**.

Некоторые адаптивные действия предустановлены в составе Security Data Lake (см. п. 4.5.1.5).

4.5.1.4.2 Добавление инцидентов в расследование

В случае, когда провести анализ одного или нескольких инцидентов необходимо за рамками процедур оперативного реагирования, они добавляются в расследование.

Чтобы добавить инцидент в существующее расследование:

1. В зависимости от того, добавляется один или несколько инцидентов:
   - чтобы добавить один инцидент в расследование, необходимо нажать в строке инцидента на многоточие в столбце **Действия** и выбрать **Добавить к расследованию**;
   - чтобы добавить несколько инцидентов в расследование, отметить в строке инцидента флажком в левом столбце нужные инциденты и нажать **Добавить выбранные к расследованию**.
2. В окне добавления расследования выбрать в выпадающем списке целевое расследование.
3. Нажать **Сохранить**.
4. В появившемся окне нажать **Закрыть** или перейти к расследованию по предложенной ссылке.

Чтобы добавить инцидент в новое расследование:

1. Отметить флажком добавляемые инциденты и нажать **Добавить выбранные к расследованию**.
2. В появившемся окне нажать **Создать расследование**.
3. Ввести название расследования.
4. При необходимости изменить статус расследования.
5. При необходимости заполнить поле **Заметка** информацией о задачах расследования и поле **Комментарий** первым сообщением в расследовании.
6. Нажать **Сохранить**, чтобы завершить действие, и вернуться к анализу инцидентов или выбрать **Начать расследование**, чтобы сразу перейти к созданному расследованию.
7. В появившемся окне нажать **Закрыть** или перейти к расследованию по предложенной ссылке.

Для ознакомления с подробной информацией о расследований инцидентов в Security Data Lake см. п. 4.5.2.

4.5.1.4.3 Поиск по дополнительным полям

Есть возможность использовать теги и быстрый поиск по дополнительным полям для поиска связанных инцидентов и событий.

1. Нажать на многоточие в столбце **Действие** справа от дополнительного поля и выбрать **Редактировать тег**, чтобы назначить полю тег для последующего просмотра и поиска.
2. Навести на значение дополнительного поля и нажать на значок линзы справа от него для применения фильтра по соответствующему полю и значению.
3. Закрепить применённые фильтры и применить их на других дашбордах Security Data Lake, например, для просмотра событий доступа на дашборде **Поиск по событиям доступа**.

4.5.1.4.4 Глушение инцидентов

Есть возможность использовать функцию глушения, чтобы исключить из обработки инциденты, удовлетворяющие заданным условиям. Глушения представляют собой исключающие фильтры и скрывают соответствующие условиям инциденты с дашборда **Анализ инцидентов**, но при этом не влияют на регистрацию инцидентов. Перечень визуальных панелей, на которых применяются фильтры глушений, может быть изменён (см. п. 4.5.3).

Чтобы создать глушение:

1. В строке инцидента, на базе которого необходимо создать фильтр глушения, нажать на многоточие в столбце **Действия** и выбрать **Заглушить инциденты**.
2. В появившемся окне указать **Наименование условия глушения**.
3. При необходимости заполнить поле **Описание**, например, указать в нём причины создания глушения.
4. При необходимости изменить предлагаемый интервал действия глушения. За пределами указанного интервала глушение не будет действовать и скрывать инциденты. Если дату окончания действия глушения оставить пустым, все инциденты после даты начала действия глушения будут скрыты.
5. Удостовериться, что поле **Выбранные поля** содержит необходимый перечень полей. Их значения из исходного инцидента будут применены в качестве условий. Результирующий поисковый запрос фильтра глушения будет отображён в поле **Предпросмотр запроса**.
6. Если условия глушения необходимо скорректировать, нажать **Изменить** и отметить применяемые в глушении поля и их значения.
7. Нажать **Сохранить**.

4.5.1.5 Встроенные адаптивные действия

Security Data Lake включает в себя несколько предустановленных адаптивных действий, доступных из дашборда **Анализ инцидентов**.

4.5.1.5.1 Отправить карточку инцидента

Действие **Отправить карточку инцидента** позволяет передать карточку инцидента из дашборда **Анализ инцидентов** за пределы Security Data Lake.

1. Выберите действие **Отправить карточку инцидента**.
2. В появившемся окне, при необходимости, указать параметры инцидента, которые необходимо изменить до его отправки: **Время**, **Срочность**, **Статус** и **Владелец**.
3. Если вместе с карточкой инцидента необходимо отправить комментарий, заполнить поле **Комментарий**.
4. В поле **Предпросмотр** можно увидеть в каком виде карточка инцидента будет отправлена.
5. Нажать **Сохранить и отправить** для выполнения действия.

4.5.1.6 Как определяется срочность инцидента

Новым инцидентам в Security Data Lake автоматически назначается уровень срочности, определяемый исходя из правил сопоставления степени критичности правила корреляции и приоритета затронутых инцидентом активов. В качестве активов выступают сетевые узлы и учётные записи, информация о которых внесена в систему. На дашборде **Анализ инцидентов** уровень срочности инцидента указан в поле **Срочность**.

В случае, если в качестве актива в инциденте присутствует как сетевой узел, так и учётная запись, для вычисления срочности используется максимальный из назначенных им приоритетов.

Ниже приведена таблица определения уровня срочности инцидента, исходя из предустановленных правил сопоставления (Таблица 2).

Таблица 2. Таблица определения уровня срочности инцидента

Приоритет (ценность) актива / учётных данных	Уровень критичности правила корреляции					
	Информационный (informational)	**Не установлен (unknown)**	**Низкий (low)**	**Средний (medium)**	**Высокий (high)**	**Критический (critical)**
Не установлен (unknown)	Информационный (informational)	Низкий (low)	Низкий (low)	Низкий (low)	Средний (medium)	Высокий (high)
Низкий (low)	Информационный (informational)	Низкий (low)	Низкий (low)	Низкий (low)	Средний (medium)	Высокий (high)
Средний (medium)	Информационный (informational)	Низкий (low)	Низкий (low)	Средний (medium)	Высокий (high)	Критический (critical)
Высокий (high)	Информационный (informational)	Средний (medium)	Средний (medium)	Средний (medium)	Высокий (high)	Критический (critical)
Критический (critical)	Информационный (informational)	Средний (medium)	Средний (medium)	Высокий (high)	Критический (critical)	Критический (critical)

- Если критичность правила корреляции информационная, то срочность созданных им инцидентов всегда будет информационной, независимо от приоритета актива.
- Если приоритет актива не установлен или низкий, а критичность правила не установлена, низкая или средняя, то срочность инцидента низкая.
- Если приоритет актива не установлен или низкий, а критичность правила высокая, то срочность инцидента средняя.
- Если приоритет актива не установлен или низкий, а критичность правила критическая, то срочность инцидента высокая.
- Если приоритет актива средний, а критичность правила не установлена или низкая, то срочность инцидента низкая.
- Если приоритет актива средний, а критичность правила средняя, то срочность инцидента средняя.
- Если приоритет актива средний, а критичность правила высокая, то срочность инцидента высокая.
- Если приоритет актива средний, а критичность правила критическая, то срочность инцидента критическая.
- Если приоритет актива высокий, а критичность правила не установлена, низкая или средняя, то срочность инцидента средняя.
- Если приоритет актива средний, а критичность правила высокая, то срочность инцидента высокая.
- Если приоритет актива средний, а критичность правила критическая, то срочность инцидента критическая.

- Если приоритет актива высокий, а критичность правила неизвестна, низкая или средняя, то срочность подключения средняя.
- Если приоритет актива критический, а критичность правила средняя, то срочность инцидента высокая.
- Если приоритет актива критический, а критичность правила высокая или критическая, то срочность инцидента критическая.

Для активов и правил корреляции, у которых в системе не задан приоритет и уровень критичности, уровень срочности инцидента определяется по значению «Не установлен».

4.5.1.6.1 Изменение срочности инцидента

Можно повлиять на степень срочности регистрируемых инцидентов несколькими способами.

4.5.2 Расследование инцидентов

4.5.2.1 Обзор функций расследования инцидентов

Для обмена информацией и совместной работы над инцидентами в Security Data Lake используется функция расследования. Здесь можно создать и редактировать расследования, фиксировать и просматривать выполненные в ходе расследования действия и комментарии.

Действия с расследованиями описаны в следующих подразделах: 4.5.2.2, 4.5.2.3, 4.5.2.4, 4.5.2.5.

4.5.2.1.1 Просмотр расследований

Список расследований представлен на дашборде **Расследования**. На нём отображаются основные данные доступных расследований (имя, последний комментарий, статус, участников, время создания и последнее действие). Можно найти нужное расследование с использованием поисковой строки или фильтра, включить отображение только тех расследований, в которых пользователь является одним из участников.

4.5.2.1.2 Пример рабочего процесса проведения расследования

Пример рабочего процесса проведения расследования:

1. После регистрации, анализа и проведения первоочередных действий с инцидентом, если возникает необходимость запросить и собрать дополнительные свидетельства инцидента, провести их экспертизу или получить консультацию от технических специалистов, для него создаётся расследование. Если инцидент связан с другими инцидентами, они объединяются в общее расследование. Для этого Аналитик, используя дашборд **Анализ инцидентов**, выбирает и добавляет инциденты в расследование.

2. Расследование может быть создано и без инцидентов. Например, когда есть только подозрение на наличие в корпоративной сети вредоносных действий и необходимо исследовать зарегистрированные в Security Data Lake исходные события, чтобы это подтвердить или опровергнуть. Создание таких расследований осуществляется Аналитиком на дашборде **Расследования**.
3. Аналитик при создании расследования указывает статус проведения расследования и записывает его цели и задачи в заметку.
4. Создавший расследование Аналитик автоматически становится его участником.
5. При необходимости Аналитик добавляет в расследование других Аналитиков, профильных технических специалистов и ответственных за объект мониторинга в качестве новых участников.
6. Новые участники получают уведомление о добавлении их в расследование, переходят в расследование и анализируют собранные в нём инциденты и данные.
7. Участники расследования выполняют задачи расследования в соответствии со своей ролью и профилем деятельности. Результаты выполнения задач и артефакты расследования фиксируются в комментариях или приложенных к расследованию файлах.
8. Участники расследования актуализируют статус расследования в соответствии с принятыми в организации этапами проведения расследований.
9. Все участники расследования получают уведомления об изменении статуса расследования, новых комментариях, файлах и действиях в расследовании.
10. Аналитики второй и третьей линии, просматривают завершённые расследования и выгружают результаты расследований для последующего анализа и формирования отчётности.

4.5.2.2 Создание расследования

В Security Data Lake создать новое расследование можно несколькими способами:

- с дашборда **Анализ инцидентов** при просмотре инцидентов (см. п. 4.5.2.3.1);
- с дашборда **Расследования**.

Создав расследование, пользователь становится его участником и может его изменять и добавлять в него данные. Например, добавлять участников, удалять связанные с расследованием инциденты, менять статус, добавлять комментарии, заметки и вложения.

4.5.2.2.1 Создание расследования с дашборда Расследование

Для создания расследования необходимо перейти на дашборд **Расследования** и выполнить следующие шаги:

1. Нажать **Создать расследование**.
2. В открывшемся окне ввести название расследования.
3. При необходимости указать текущий статус расследования.
4. При необходимости заполнить поля **Заметка**, например, указав в нём причины создания расследования.
5. При необходимости добавить в расследование первое сообщение, заполнив поле **Комментарий**.
6. Нажать **Создать**.

Расследование будет создано и добавлено к списку расследований.

4.5.2.3 Добавление деталей к расследованию

Работающий над расследованием пользователь Security Data Lake может добавлять в него инциденты, комментарии и файлы. Они выступают свидетельствами расследования и подтверждают выполнение его задач. Рекомендуется записывать все выполняемые в ходе расследования важные шаги. В качестве комментариев к расследованию фиксируются телефонные и электронные беседы, ссылки на внешние публикации, поисковые запросы к исходным событиям. В виде файлов в расследование могут загружаться снимки экрана и файлы.

4.5.2.3.1 Добавление инцидента в расследование

Добавить инцидент в расследование можно с дашборда **Анализа инцидентов** (см. п. 4.6.2).

Если статус, срочность, владелец или другие данные инцидента изменятся, то информация о нём в расследовании также обновится.

4.5.2.3.2 Добавление комментариев

По мере проведения расследования в него могут быть добавлены комментарии.

1. Перейти в расследование, открыв его через дашборд **Расследования**.
2. Заполнить поле ввода комментария. При необходимости использовать встроенные инструменты форматирования списков, кода и ссылок.
3. Нажать **Отправить**.

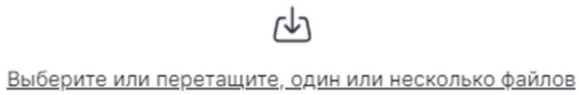
Комментарий появится в истории изменений.

4.5.2.3.3 Добавление файлов

При необходимости в расследование можно сохранять файлы:

1. Перейти в расследование, открыв его через дашборд **Расследования**.

2. Добавить сохраняемый файл в поле:



3. Нажать **Отправить**.

Файлы будут добавлены и будут отображаться во вкладке **Вложения**.

4.5.2.4 Внесение изменений в расследование

В процессе проведения расследования можно менять его наименование, статус и заметку, удалять расследование.

4.5.2.4.1 Изменение заметки и наименование расследования

Перейдя в расследование, можно изменить заметку и наименование расследования. Например, чтобы более точно описать расследуемый инцидент.

1. Перейти в расследование, открыв его через дашборд **Расследования**.
2. Нажать кнопку **Изменить**.
3. Скорректировать текст в поле **Наименование**.
4. Скорректировать текст в поле **Заметка**.
5. Нажать **Сохранить**.

4.5.2.4.2 Обновление статуса расследования

Сразу после создания все расследования имеют статус Новый. По мере того как проводится расследование, его статус можно изменять в соответствии с принятым в организации рабочим процессом:

1. В карточке расследования нажать **Изменить**.
2. Выбрать статус из раскрывающегося списка.
3. Нажать **Сохранить**.

В системе предустановлены следующие статусы расследований, приведенные ниже (Таблица 3).

Таблица 3. Статус расследований

Статус	Описание
Новое	Означает, что расследование ещё не начиналось
В работе	Участник выполняет задачи расследования
В ожидании	Участники временно не могут продолжить расследование, необходима дополнительная информация или действия
Закончено	Задачи расследования решены, результаты расследования ожидают проверки
Закрыто	Обработка расследования завершена

Наименования статусов расследований и их описания задаются параметрами системы и могут быть изменены в соответствии с принятыми в организации правилами и рабочими процессами.

4.5.2.4.3 Удаление расследования

Можно удалить одно или сразу несколько расследований.

Порядок действий следующий:

1. Установить флажки в левом столбце расследований, которые необходимо удалить.
2. Нажать **Удалить * расследований**.
3. Нажать **Удалить**, чтобы подтвердить действие.

Расследования будут удалены и перестанут отображаются в списке дашборда **Расследования**. При этом выполненные в расследованиях действия сохранятся в системе в течение срока, заданного политикой хранения индексов ***-investigations-history**.

4.5.2.4.4 Добавление и удаление инцидентов в расследовании

Добавить инцидент в расследование можно на дашборде анализа инцидентов (см. п. 4.6.2).

Для удаления инцидента из расследования:

1. В карточке расследования в таблице с перечнем инцидентов нажать на многоточие в столбце **Действие** справа от имени инцидента.
2. Выбрать **Удалить из расследования**.

Инцидент будет удалён из таблицы.

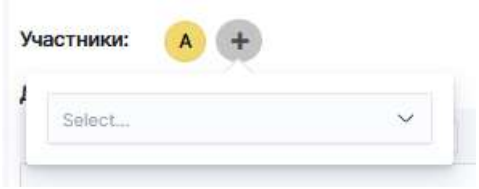
4.5.2.5 Совместная работа над расследованием

В расследовании одновременно могут участвовать сразу несколько участников.

4.5.2.5.1 Добавление участника к расследованию

Порядок действий следующий:

1. Открыть расследование, к которому необходимо добавить участника.
2. Нажать на значок  .
3. Ввести или выбрать из списка возможных участников имя пользователя, которого необходимо добавить:



4. Инициалы выбранного пользователя отобразятся среди участников расследования.

Список возможных участников расследования ограничен и определяется ролями доступа и параметрами расследований.

Если все возможные участники уже добавлены в расследование, список возможных участников будет пуст.

4.5.2.5.2 Просмотр участников расследования

Инициалы участников расследования отображаются на дашборде **Расследования** и в каждом отдельном расследовании. Следует навести указатель мыши на значок с инициалами, чтобы посмотреть полное имя.

4.5.2.5.3 Удаление участника из расследования

Чтобы удалить участника расследования:

1. Открыть расследование.
2. Нажать на значок участника.
3. Нажать **Удалить из участников**.

Значок с инициалами пользователя перестанет отображаться в поле **Участники**.

4.5.3 Управление глушениями инцидентов

Возможности по управлению глушениями в Security Data Lake включают в себя создание глушений с настраиваемыми условиями фильтрации, изменение и отключение ранее созданных глушений, аудит действий с глушениями и контроль заглушенных инцидентов.

4.5.3.1 Создание нового глушения

Чтобы создать глушение с настраиваемым условием фильтрации, необходимо выполнить следующие действия:

1. Выбрать в верхнем меню **Настройки** > **Глушение инцидентов**.
2. Нажать **Создать новое условие**.
3. Заполнить поле **Наименование условия глушения**.
4. Указать подробности в поле **Описание** (при необходимости).
5. В поле **Запрос** ввести поисковый запрос, используя синтаксис Lucene, при этом поисковый запрос должен включать в себя указание временного интервала по полю `@timestamp`. Все инциденты, удовлетворяющие введённому запросу, будут скрыты с визуализаций дашборда **Анализ инцидентов** и других визуализаций, использующих индекс-паттерн **alerts_with_suppression**.
6. Нажать **Сохранить**.

Примечание — Обычно одним из условий фильтрации в запрос также включается наименование правила корреляции, например, запрос rule_id:client-soc_windows_scheduled_task_created AND @timestamp:[2022-03-01T03:00:00.000Z TO *] AND TaskName:\\GoogleUpdate скроет инциденты, созданные после 3 часов ночи

01.03.2022 в часовом поясе UTC правилом client-soc_windows_scheduled_task_created и содержащие значение \GoogleUpdate в поле TaskName.

4.5.3.2 Изменение глушения

Чтобы изменить глушение:

1. Выбрать в верхнем меню **Настройки** > **Глушение инцидентов**.
2. Нажать на название глушения, чтобы открыть окно **Изменить условие**.
3. Внести необходимые изменения в поля **Описание** и **Запрос**.
4. Нажать **Сохранить**.

4.5.3.3 Отключение глушения

Чтобы отключить глушение:

1. Выбрать в верхнем меню **Настройки** > **Глушение инцидентов**.
2. Нажать **Отключить** в столбце **Статус** отключаемого глушения.

4.5.3.4 Удаление глушения

Чтобы удалить одно или несколько глушений:

1. Выбрать в верхнем меню **Настройки** > **Глушение инцидентов**.
2. Отметить глушения, которые необходимо удалить, и нажать **Удалить X глушений**, где X — количество выбранных глушений.
3. Подтвердить действие.

4.5.3.5 Аудит глушений

Аудит действий с глушениями и подпадающих под условия глушений инцидентов осуществляется с использованием дашборда **Аудит глушений** (см. п. 4.6.6.1.2).

4.5.4 Дашборды

4.5.4.1 Обзор встроенных дашбордов

Security Data Lake включает в себя более 50 связанных между собой дашбордов и более 200 графических визуализаций для отображения и обработки данных. Они позволяют контролировать состояние защищённости корпоративной сети, просматривать зарегистрированные инциденты и расследования, анализировать оперативные данные, осуществлять мониторинг доменов, проводить аудит рабочих процессов и процессов обработки данных в системе.

Пользователь может выбрать наиболее подходящий дашборд, по его назначению.

4.5.4.1.1 Контроль состояния защищённости

Для контроля активности угроз и состояния процессов по их обработке предназначены дашборды сводных аналитических данных. К таким дашбордам относятся:

- **Статистика инцидентов** — предоставляет статистику по обнаруженным инцидентам за выбранный интервал времени. Следует использовать данный

дашборд для определения часто используемых векторов, техник и тактик реализации атак, подверженных инцидентам объектов мониторинга, учётных записей и сетевых узлов (см. п. 4.6.1.1);

- **Работа SOC** — отображает значения и динамику изменения основных ключевых показателей уровня оказания услуг центра мониторинга, построенного на базе Security Data Lake (см. п. 4.6.1.2).

4.5.4.1.2 Просмотр зарегистрированных инцидентов и расследований

Просматривать, обрабатывать и расследовать инциденты в Security Data Lake можно с помощью следующих дашбордов:

- **Анализ инцидентов** — показывает подробные сведения об инцидентах. Здесь можно искать, назначать, реагировать и просматривать сведения об инцидентах (см. п. 4.6.2).
- **Расследования** — содержит список всех расследований. Есть возможность создания, изменения и совместной работы над расследованиями.

4.5.4.1.3 Анализ оперативных данных

Security Data Lake включает в себя набор встроенных аналитических инструментов анализа вредоносной активности. Они представлены в разделе дашбордов **Оперативные данные** и могут использоваться при анализе контекста инцидентов, поиска дополнительных признаков вредоносных действий, подтверждения или повышения степени срочности инцидентов или для обнаружения инцидентов вручную:

- группа дашбордов **Оперативные данные по угрозам** позволяют получить дополнительные сведения о выявленных артефактах известных угроз (см. п. 4.6.4.1);
- группа дашбордов **Оперативные данные по Веб** включают в себя инструменты анализа данных веб-трафика, включая анализ HTTP-категорий веб-ресурсов, идентификационных строк веб-клиентов (HTTP User Agent), сроков регистрации доменных имён, URL-адресов (см. п. 4.6.4.2).

4.5.4.1.4 Мониторинг доменов

Для наблюдения за объектом мониторинга Security Data Lake предоставляет отдельный набор дашбордов и визуализаций. Они объединены в группы по направлениям (доменам):

- дашборды раздела **Активы** отображают внесённые в Security Data Lake данные о сетевых узлах, учётных записях и сведения об их взаимодействии между собой (сетевые сессии (см. п. 4.6.5.1));

- дашборды домена **Доступ** отображают сведения о событиях аутентификации и управления доступом (см. п. 4.6.5.2);
- дашборды раздела **Сеть** отображают данные о сетевых коммуникациях (см. п. 4.6.5.3);
- дашборды домена **Конечные узлы** отображают сведения о заражениях вредоносным программным обеспечением (см. п. 4.6.5.4).

4.5.4.1.5 Аудит процессов

Дашборды раздела **Аудит** предназначены для анализа происходящих в Security Data Lake процессов. К ним относятся сбор данных, выполнение задач по реагированию и расследованию инцидентов (см. п. 4.6.6.1).

4.5.4.2 Ключевые индикаторы

Ключевые индикаторы — визуальное представление метрик. Эти метрики формируются поисковыми запросами, встроенными в визуализацию, и используют единую модель данных Common Information Model (CIM). Ключевые индикаторы расположены в верхней части дашбордов и отображают значения за последние 24 часа и их изменения.

4.5.4.2.1 Толкование ключевых индикаторов на дашбордах

Толкование ключевых индикаторов на дашбордах приведено ниже (Рисунок 2, Таблица 4).

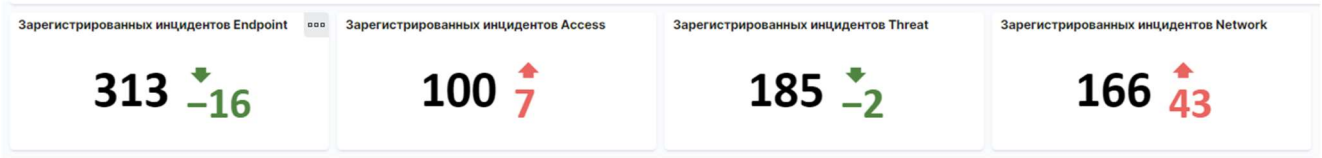


Рисунок 2. Толкование ключевых индикаторов на дашбордах

Таблица 4. Толкование ключевых индикаторов на дашбордах

Поле	Описание
Название	Краткое описание ключевого индикатора
Значение	Числовой показатель, который помогает оценить состояние объекта мониторинга. Рассчитывается по данным за последние 24 часа. При наведении на значение появляется всплывающая подсказка с описанием ключевого показателя. Можно нажать на индикатор, чтобы перейти к исходным данным
Изменение	Изменение значения по сравнению с предыдущими сутками. Изменения в большую сторону отображаются красным цветом, в меньшую — зелёным
Тренд	Стрелка вверх или вниз, указывающая направление тренда. Стрелка меняет цвет и направление в зависимости от значения изменения

4.6 Справочник дашбордов

4.6.1 Сводная аналитика

4.6.1.1 Дашборд Статистика инцидентов

Дашборд **Статистика инцидентов** предназначен для предоставления сводной информации по инцидентам в разрезе доменов и полезен для просмотра общего состояния объекта мониторинга.

4.6.1.1.1 Панели

Панели и их описание приведены в таблице ниже (Таблица 5).

Таблица 5. Панели

Панель	Описание
Ключевые индикаторы	Отображают на индикаторах количество инцидентов по доменам за последние 24 часа. Дополнительные сведения см. в п. 4.5.4.2
Количество инцидентов по срочности	Отображает на гистограмме количество инцидентов каждого уровня срочности за выбранный интервал времени. Оценка уровня срочности формируется исходя из значения критичности правила корреляции и максимального приоритета (ценности) затронутых инцидентом активов и учётных данных, в соответствии с заложенной в программу таблицей сопоставления. Можно применить фильтр к текущему дашборду или перейти на дашборд **Анализ инцидентов**
Количество инцидентов по времени и доменам	Отображает количество инцидентов по доменам на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду или перейти на дашборд **Анализ инцидентов**
Количество инцидентов по правилам корреляции	Отображает таблицу правил корреляции с наибольшим значением зарегистрированных инцидентов за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Анализ инцидентов**
Количество инцидентов по расположению	Отображает распределение инцидентов на карте по расположению узла назначения. Расположение определяется по географическим координатам. Можно применить фильтр к текущему дашборду
Количество инцидентов по объектам мониторинга	Отображает в таблице объекты мониторинга и количество инцидентов для каждого из них за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Анализ инцидентов**
Количество инцидентов по учётным записям	Отображает в таблице самые частые учётные записи с инцидентами и количеством инцидентов за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Анализ инцидентов**

Панель	Описание
Количество инцидентов по узлам источников	Отображает в таблице самые частые источники инцидентов с указанием количества правил корреляции и количества доменов за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Анализ инцидентов**

4.6.1.2 Дашборд Работа SOC

Дашборд **Работа SOC** отображает сводную информацию о центре мониторинга и включает в себя данные по необработанным инцидентам с истекающим сроком реагирования, действиям по реагированию и расследованию, статистике регистрации инцидентов, статистике регистрации событий.

4.6.1.2.1 Панели

4.6.1.2.1.1 Необработанные инциденты с истекающим сроком реагирования

Необработанные инциденты с истекающим сроком реагирования приведены ниже (Таблица 6).

Таблица 6. Необработанные инциденты с истекающим сроком реагирования

Панель	Описание
Датчики («Низкий», «Средний», «Высокий», «Критический»)	Отображают на круговой шкале количество незаглушенных инцидентов соответствующего уровня срочности за выбранный интервал времени, срок обработки которых истекает. Учитываются инциденты со статусом, отличным от конечного (по умолчанию конечным статусом является «Закрыт», подробнее см. п. 4.5.1.2) и с момента регистрации которых прошло: • для статуса «Низкий» — больше 225 минут; • для статуса «Средний» — больше 105 минут; • для статуса «Высокий» — больше 45 минут; • для статуса «Критический» — больше 30 минут. Шкала выделяется цветом при превышении заданного в параметрах визуализации количества инцидентов
Количество необработанных инцидентов по времени и срочности	Отображает на гистограмме количество незаглушенных инцидентов со статусом, отличным от конечного (по умолчанию конечным статусом является «Закрыт», подробнее см. п. 4.5.1.2) по уровню срочности на временной шкале за выбранный интервал времени. Для фильтрации обработанных инцидентов необходимо добавить в визуализацию фильтр исключений по статусам или адаптивным действиям, указывающим на завершение обработки инцидента. Можно применить фильтр к текущему дашборду
Количество необработанных информационных инцидентов по времени	Отображает на гистограмме количество незаглушенных инцидентов с информационным уровнем срочности на временной шкале за последние 7 дней. Можно применить фильтр к текущему дашборду

4.6.1.2.1.2 Действия по реагированию и расследованию

Действия по реагированию и расследованию приведены ниже (Таблица 7).

Таблица 7. Действия по реагированию и расследованию

Панель	Описание
Ключевые индикаторы	Отображают на индикаторах ключевые метрики действий с инцидентами, глушениями и расследованиями за последние 24 часа. Дополнительные сведения см. в п. 4.5.4.2
Количество действий с инцидентами, глушениями и расследованиями	Отображает на гистограмме количество действий по инцидентам, глушениям и расследованиям на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду
Количество инцидентов по владельцу и срочности	Отображает на гистограмме владельцев инцидентов, количество инцидентов и степень срочности для незаглушенных инцидентов за выбранный интервал времени. Эта панель полезна для понимания распределения количества и срочности инцидентов между владельцами. Дополнительные сведения см. в п. 4.5.1.6. Можно применить фильтр к текущему дашборду

4.6.1.2.1.3 Статистика регистрации инцидентов

Статистика регистрации инцидентов приведена ниже (Таблица 8).

Таблица 8. Статистика регистрации инцидентов

Панель	Описание
Количество инцидентов по времени и объектам мониторинга	Отображает на гистограмме количество инцидентов по объектам мониторинга на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду
Количество инцидентов по объектам мониторинга	Отображает на гистограмме количество инцидентов для каждого объекта мониторинга. Можно применить фильтр к текущему дашборду
Ключевые индикаторы	Отображают на индикаторах ключевые метрики инцидентов со статусом «Новый» и правил корреляций уникальных для объектов мониторинга

4.6.1.2.1.4 Статистика регистрации событий

Статистика регистрации событий приведена ниже (Таблица 9).

Таблица 9. Статистика регистрации событий

Панель	Описание
Среднее значение EPS по времени и объектам мониторинга	Отображает на гистограмме среднее значение EPS по объектам мониторинга на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду
Объём событий по объектам мониторинга	Отображает на гистограмме объём событий в Гбайт для каждого объекта мониторинга. Можно применить фильтр к текущему дашборду

Панель	Описание
Ключевые индикаторы	Отображают на индикаторах ключевые метрики событий. Дополнительные сведения см. в п. 4.5.4.2

4.6.2 Дашборд Анализ инцидентов

Дашборд **Анализ инцидентов** отображает сводную информацию по анализу незаглушенных инцидентов и предназначен для изучения инцидентов и выполнения действий по их обработке.

4.6.2.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, выбрав значение из выпадающего списка (Таблица 10).

Таблица 10. Фильтры

Фильтр	Описание
Статус	Отображает на дашборде данные по выбранным статусам обработки инцидентов
Владелец	Отображает на дашборде данные по выбранным владельцам инцидентов
Поиск по тегу	Отображает на дашборде данные по выбранным тегам значений дополнительных полей инцидентов
Объект	Отображает на дашборде данные по выбранным объектам мониторинга
Правило корреляции	Отображает на дашборде данные по выбранным правилам корреляции
Домен	Отображает на дашборде данные по выбранным доменам
Killchan steps	Отображает на дашборде данные по выбранным категориям Killchan steps
Mitre ATT&K Tactics	Отображает на дашборде данные по выбранным категориям Mitre ATT&K Tactics
Mitre ATT&K Techniques	Отображает на дашборде данные по выбранным категориям Mitre ATT&K Techniques

4.6.2.2 Панели

Панели и их описание приведены ниже (Таблица 11).

Таблица 11. Панели

Панель	Описание
Количество инцидентов по срочности	Отображает на круговой диаграмме соотношение числа инцидентов отдельных уровней срочности к общему количеству незаглушенных инцидентов за выбранный интервал времени. Можно применить фильтр к текущему дашборду
Количество инцидентов по времени	Отображает на гистограмме количество инцидентов на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду

Панель	Описание
Перечень инцидентов	Отображает в таблице незаглушенные инциденты за выбранный интервал времени, включая наименование, время, срочность, домен, наименование, статус, владелец, комментарии и другие их атрибуты. Каждый инцидент можно посмотреть более детально, выполнить с ним предустановленнные действия. Дополнительные сведения см. в п. 4.5.1

4.6.3 Дашборды Расследования

Для проведения расследований инцидентов в Security Data Lake используются дашборды **Расследования** и **Редактирование расследования**. Здесь есть возможность создавать и редактировать расследования, добавлять в расследования участников и взаимодействовать с ними.

4.6.3.1 Список расследований

Дашборд **Список расследований** отображает перечень расследований, позволяет создавать и удалять расследования, переходить к их просмотру и редактированию.

4.6.3.1.1 Панель

Панель и ее описание приведено ниже (Таблица 12).

Таблица 12. Панель

Панель	Описание
Список расследований	Отображает в таблице все расследования. Включает в себя наименование, последний комментарий, статус, время создания, время последнего действия и участников. Можно фильтровать, создавать и удалять расследования, перейти к дашборду **Расследование**

4.6.3.2 Редактирование расследования

Дашборд **Расследование** отображает сведения о расследовании, позволяет изменять расследование и добавлять к расследованию новую информацию.

4.6.3.2.1 Панель

Панель и ее описание приведено ниже (Таблица 13).

Таблица 13. Панель

Панель	Описание
Расследование	Отображает атрибуты расследования, действия в расследовании и связанные с расследованием инциденты. Можно редактировать атрибуты, добавлять в расследование комментарии и файлы, выполнять действия с инцидентами, вернуться к дашборду **Список расследований**

4.6.4 Оперативные данные

4.6.4.1 Дашборды подраздела Оперативные данные по угрозам

Дашборды подраздела **Оперативные данные по угрозам** предназначены для анализа артефактов известных угроз, полученных из каталогов киберугроз (Threat Intelligence).

4.6.4.1.1 Активность угроз

Дашборд **Активность угроз** предоставляет информацию о фактах обнаружения артефактов угроз в Security Data Lake.

4.6.4.1.1.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, выбрав значение из выпадающего списка (Таблица 14). Фильтры не применяются к ключевым показателям.

Таблица 14. Фильтры

Фильтр	Описание
Группа угроз	Отображает на дашборде данные по выбранным группам угроз. В зависимости от каталога угроз и его интеграции с Security Data Lake, угрозы могут быть сгруппированы по наименованию, источнику или другому конкретному признаку
Категория угроз	Отображает на дашборде данные по выбранным категориям угроз. Категория указывает на общий признак угроз или артефактов. К таким признакам относятся класс или вектор атаки, вид вредоносного программного обеспечения и т. п. Например APT, BotNet или Network activity
Поле с артефактом	Отображает на дашборде данные по выбранным полям с артефактами. В событиях обнаружения угроз это значение указывает на наименование поля исходного события Security Data Lake, в котором был обнаружен артефакт

4.6.4.1.1.2 Панели

Панели и их описание приведены ниже (Таблица 15).

Таблица 15. Панели

Панель	Описание
Ключевые индикаторы	Отображают на индикаторах ключевые метрики артефактов за последние 24 часа. Дополнительные сведения см. в п. 4.5.4.2
Количество обнаружений угроз по времени	Отображает на графике количество событий обнаружения угроз по коллекциям на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду или перейти на дашборд **Артефакты угроз**

Панель	Описание
Количество обнаружений по коллекциям угроз	Отображает в таблице количество уникальных артефактов и событий обнаружения угроз по каждой коллекции за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Артефакты угроз**
Количество обнаружений по правилам корреляции	Отображает в таблице метрики (количество уникальных артефактов, количество обнаружений) для группы уникальных значений (наименование правила корреляции, коллекция угроз) за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Артефакты угроз**
Количество обнаружений по источникам угроз	Отображает в таблице количество событий обнаружения угроз для группы уникальных значений (ID источника, путь источника и формат) за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Артефакты угроз**
Данные последних обнаруженных артефактов	Отображает в таблице метрики (время последнего обнаружения, количество уникальных узлов назначения, количество уникальных узлов источников, количество уникальных групп угроз, количество уникальных коллекций угроз, количество уникальных категорий угроз и количество полей, содержащих артефакт) для каждого значения поля с артефактом за выбранный интервал времени. Значение поля с артефактом указывает на значение поля исходного события, которое совпало с артефактом известной угрозы. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Артефакты угроз**
Данные последних обнаружений по узлам назначения и источника	Отображает в таблице метрики (время последнего обнаружения, количество уникальных узлов назначения, количество уникальных узлов источников, количество уникальных групп угроз, количество уникальных коллекций угроз, количество уникальных категорий угроз, количество полей, содержащих артефакт) для каждого значения поля с артефактом за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Артефакты угроз**
Статистика обнаружений по угрозам	Отображает в таблице количество событий обнаружения угроз для группы уникальных значений (категория угроз, коллекция угроз, группа угроз и поля с артефактами) за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Артефакты угроз**
События активности угроз	Отображает в таблице события обнаружения угроз за выбранный интервал времени. Включает в себя время (time), поле с артефактами (threat_match_field), значение поля с артефактом (threat_match_value), формат (threat_source_type), узел источника (src), узел назначения (dest), коллекцию угроз (threat_collection), группу угроз (threat_group), категорию угроз (threat_category). Можно применить фильтр к текущему дашборду

4.6.4.1.2 Артефакты угроз

Дашборд **Артефакты угроз** предназначен для просмотра и поиска данных об артефактах и используется при переходе из дашборда **Активность угроз** (см. п. 4.6.4.1.1).

Дашборды **Артефакты угроз** содержат подробные сведения об артефактах угроз. Они позволяют проанализировать контекст артефактов, включая информацию о связанных с ними классах угроз, группах угроз и каталогов угроз.

4.6.4.1.2.1 Вкладки

Вкладки приведены ниже (Таблица 16).

Таблица 16. Вкладки

Вкладка	Панели
Обзор артефактов	Количество угроз по источникам, Количество угроз по коллекциям и категориям, Сетевые артефакты, Артефакты конечных узлов, Артефакты электронной почты, Артефакты сертификатов
Сетевые артефакты	Оперативные данные по HTTP-артефактам, Оперативные данные по IP (Сводка), Оперативные данные по IP, Оперативные данные по Доменам (Сводка), Оперативные данные по доменам
Артефакты конечных узлов	Оперативные данные по файловым артефактам, Оперативные данные по артефактам реестра, Оперативные данные по артефактам процессов, Оперативные данные по артефактам сервисов, Оперативные данные по артефактам учётных записей
Артефакты сертификатов	Оперативные данные по артефактам сертификатов (сводка), Оперативные данные по артефактам сертификатов
Артефакты электронной почты	Оперативные данные по артефактам электронной почты

4.6.4.2 Дашборды подраздела Оперативные данные по Веб

Дашборды подраздела **Оперативные данные по Веб** предназначены для выявления атак в данных о веб-трафике.

4.6.4.2.1 Анализ категорий HTTP

Дашборд **Анализ категорий HTTP** отображает метрики веб-трафика по HTTP-категориям. Он позволяет обнаружить аномальные значения количественных показателей отдельных HTTP-категорий, что указывает на возможное использование веб-трафика вредоносным программным обеспечением, например:

- необычные или неизвестные категории веб-трафика;
- большое количество событий веб-трафика, относящегося к редко используемой категории (с небольшим количеством узлов источников);
- малое количество событий веб-трафика, относящегося к часто используемой категории (с большим количеством узлов источников).

4.6.4.2.1.1 Неизвестные категории

К неизвестным категориям на дашборде относятся те категории, которые указаны в параметрах визуализации-фильтра **SLSDL_HTTPCategoryAnalysis_Filter**. Имея права на редактирование визуализаций, можно изменить перечень HTTP-категорий, относящихся к неизвестным. Для этого необходимо выполнить следующие шаги:

1. Перейти в режим редактирования, нажав кнопку **Edit** в правом верхнем углу дашборда.
2. Нажать на значок шестерёнки в правом верхнем углу фильтра и выбрать пункт **Edit visualization**.
3. Скорректировать фильтр в URL перехода с индексом, используя закодированный в URL синтаксис Query DSL. По умолчанию к неизвестным категориям относится категории undefined и unknown
4. Применить изменение, нажав кнопку **Update** в правом нижнем углу, и сохранить изменённую визуализацию, нажав **Save and return**.

4.6.4.2.1.2 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, нажав на фильтр-ссылку (Таблица 17). Фильтры не применяются к ключевым индикаторам.

Таблица 17. Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга
Показывать только неизвестные категории	Отображает на дашборде данные по неизвестным категориям веб-трафика при выбранном значении «Да» и данные по известным категориям веб-трафика при выбранном значении «Нет»

4.6.4.2.1.3 Панели

Панели и их описание приведены ниже (Таблица 18).

Таблица 18. Панели

Панель	Описание
Ключевые индикаторы	Отображают на индикаторах ключевые метрики категорий веб-трафика за последние 24 часа. Дополнительные сведения см. в п. 4.5.4.2
Распределение HTTP-категорий	Отображает на точечной диаграмме количество событий и количество узлов источников по категориям за выбранный интервал времени. Можно применить фильтр к текущему дашборду или перейти к просмотру исходных событий в **Discover**

Панель	Описание
Статистика по HTTP-категориям	Отображает таблицу с перечнем HTTP-категорий с указанием времени последнего события, количества узлов источников, количества узлов назначения и количества событий. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти к просмотру исходных событий в **Discover**

4.6.4.2.2 Анализ HTTP User Agent

Дашборд **Анализ HTTP User Agent** показывает метрики веб-трафика по идентификационным строкам веб-клиента (HTTP User Agent). Он позволяет обнаружить необычные идентификационные строки, длина которых выходит за рамки стандартного отклонения. Такие HTTP User Agent могут указывать вредоносный веб-трафик, например:

- необычно длинные или короткие строки HTTP User Agent;
- редко используемые HTTP User Agent;
- HTTP User Agent, в которых имя браузера написано с ошибкой или номер версии указан неверно.

4.6.4.2.2.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, выбрав значение из выпадающего списка (Таблица 19). Фильтры не применяются к ключевым индикаторам.

Таблица 19. Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга
Индекс отклонения	Отображает на дашборде данные, находящиеся за рамками выбранного значения стандартного отклонения длины HTTP User Agent и соответствующего ему процента веб-событий (1(68.26 %), 2(95.45 %), 3(99.73 %), или 4(99.90 %)) При выборе большего значения стандартного отклонения будут отображаться HTTP User Agent с меньшим количеством событий

4.6.4.2.2.2 Панели

Панели и их описание приведены ниже (Таблица 20).

Таблица 20. Панели

Панель	Описание
Ключевые индикаторы	Отображают на индикаторах ключевые метрики пользовательского агента за последние 24 часа. Дополнительные сведения см. в п. 4.5.4.2

Панель	Описание
Распределение User Agent	Отображает на точечной диаграмме количество событий и длину строк по значениям идентификационных строк веб-клиента (HTTP User Agent) за выбранный интервал времени. Можно применить фильтр к текущему дашборду или перейти к просмотру исходных событий в **Discover**
Статистика по User Agent	Отображает таблицу с перечнем идентификационных строк веб-клиента (HTTP User Agent) с указанием длины строки, количества событий, количества узлов источников, количества узлов назначения и времени последнего события. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти к просмотру исходных событий в **Discover**

4.6.4.2.3 Анализ новых доменов

Дашборд **Анализ новых доменов** показывает обнаруженные в событиях веб-трафика недавно приобретённые или ранее не встречавшиеся в событиях домены веб-ресурсов. Такие домены с высокой степенью вероятности могут использоваться злоумышленниками для управления троянскими и другими вредоносными программами. При этом имена доменов часто генерируются злоумышленниками автоматически с использованием алгоритмов автоматической генерации доменных имён (Domain Generation Algorithm, DGA). Аномальный трафик к ним может указывать на наличие в сети вредоносного программного обеспечения. Например:

- необычно большое количество событий с небольшого количества узлов источников к недавно приобретённому веб-домену;
- недавно приобретённый или ранее не встречавшийся веб-домен с необычным именем;
- необычно большое количество событий к недавно приобретённому веб-домену;
- аномальное количество событий обращения к недавно зарегистрированным поддоменам доменов верхнего уровня (Top Level Domain, TLD);
- высокая активность взаимодействия с веб-доменом, не входящим в известные рейтинги популярных доменов.

4.6.4.2.3.1 Вкладки

Вкладки и их описание приведены ниже (Таблица 21).

Таблица 21. Вкладки

Вкладка	Описание
Новые зарегистрированные	Отображает данные о недавно зарегистрированных доменах
Новые в событиях	Отображает данные о доменах, встретившихся в событиях впервые недавно

4.6.4.2.3.2 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, выбрав значение из выпадающего списка (Таблица 22).

Таблица 22. Фильтр

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга

4.6.4.2.3.3 Панели

Панели и их описание приведены ниже (Таблица 23).

Таблица 23. Панели

Панель	Описание
Активность новых доменов	Отображает в таблице метрики (домен, дата регистрации, рейтинг (например, Amazon Alexa / Cisco Umbrella / Cloudflare Top 1M list), количество событий и время последнего события) для узлов назначения, взаимодействовавших с новыми доменами, за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти к просмотру исходных событий в **Discover**
Активность новых доменов по дате регистрации	Отображает на точечном графике возраст и количество событий по доменам за выбранный интервал времени. Можно перейти к просмотру исходных событий в **Discover**
Активность новых доменов по доменам верхнего уровня	Отображает на гистограмме домены верхнего уровня, для которых в событиях были обнаружены недавно зарегистрированные поддомены, и количество событий обращения к ним за выбранный интервал времени. Можно применить фильтр к текущему дашборду или перейти к просмотру исходных событий в **Discover**
Регистрационные данные	Отображает в таблице данные о регистрации доменов, обнаруженных в веб-событиях. Включает в себя имя домена (domain), дату регистрации (created), срок окончания регистрации (expires), обслуживающие домен узлы (nameservers), владелец домена (registrant) и компания, зарегистрировавшая домен (registrar). Можно применить фильтр к текущему дашборду

4.6.4.2.4 Анализ длины URL

Дашборд **Анализ длины URL** позволяет просматривать данные по веб-событиям, в которых длина URL-адреса выходит за границы выбранного диапазона стандартного отклонения. На наличие угроз могут указывать следующие данные по событиям URL необычной длины, например:

- необычное количество событий;
- аномальное количество узлов источников или узлов назначения;

- URL-запрос, содержащий подозрительные команды и скрипты, например, для SQL-инъекции, межсайтового скриптинга или других атак;
- отсутствие в событии URL источника запроса (`http_referrer`);
- незнакомые узлы отправителя или получателя.

4.6.4.2.4.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, выбрав значение из выпадающего списка (Таблица 24). Фильтры не применяются к ключевым индикаторам.

Таблица 24. Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга
Индекс отклонения	Отображает на дашборде данные, выходящие за рамки выбранной категории стандартного отклонения длины URL-адреса и соответствующего ему процента веб-событий (1(68.26 %), 2(95.45 %), 3(99.73 %), или 4(99.90 %)). При выборе большего значения стандартного отклонения будут отображаться URL-адреса с меньшим количеством событий

4.6.4.2.4.2 Панели

Панели и их описание приведены ниже (Таблица 25).

Таблица 25. Панели

Панель	Описание
Ключевые индикаторы	Отображают на индикаторах ключевые метрики URL за последние 24 часа. Дополнительные сведения см. в п. 4.5.4.2
Количество событий по времени	Отображает на графике количество событий с не пустым URL по HTTP-методам на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду или перейти к просмотру исходных событий в **Discover**
Статистика по длине URL	Отображает в таблице метрики (длину URL, количество узлов источника, количество узлов назначения, количество событий и время последнего события) для уникальных URL за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти к просмотру исходных событий в **Discover**

4.6.5 Домены

4.6.5.1 Дашборды подраздела Активы

Дашборды домена **Активы** содержат информацию о сетевых узлах и учётных записях, внесённых в Security Data Lake.

4.6.5.1.1 Центр сетевых узлов

Следует использовать дашборд **Центр сетевых узлов** для просмотра и поиска данных об узлах сети, добавленных в качестве активов в Security Data Lake. Эти данные представляют собой список наименований, IP-адресов и подсетей организации с указанием дополнительной информации об их расположении, категории и других сведений.

Данные об узлах сети не содержат временных меток, фильтр времени к ним не применим.

4.6.5.1.1.1 Панели

Панели и их описание приведены ниже (Таблица 26).

Таблица 26. Панели

Панель	Описание
Количество узлов по индексам объектов	Отображает в таблице индексы объектов мониторинга и количество узлов для каждого из них. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Количество узлов по приоритетам	Отображает на гистограмме число узлов по уровню приоритета. Можно применить фильтр к текущему дашборду
Количество узлов по подразделениям	Отображает на круговой диаграмме процентное соотношение числа узлов отдельных подразделений к общему количеству узлов. Можно применить фильтр к текущему дашборду
Количество узлов по категориям	Отображает на круговой диаграмме процентное соотношение числа узлов отдельных категорий к общему количеству узлов. Можно применить фильтр к текущему дашборду
Информация об узлах	Отображает в таблице все узлы. Включает в себя IP-адрес (ip), MAC-адрес (mac), имя операционной системы (nt_host), DNS-имя (dns), владельца (owner), приоритет (priority), город (city), страну (country), подразделение (bunit), категорию (category) указатель отслеживания наличия событий (is_expected), указатель отслеживания синхронизации времени (should_timesync), указатель отслеживания обновлений (should_update) и указатель отслеживания антивируса (requires_av). Можно применить фильтр к текущему дашборду

4.6.5.1.2 Центр учётных записей

Следует использовать дашборд **Центр учётных записей** для просмотра и поиска данных об учётных записях, добавленных в качестве активов Security Data Lake. Данные представляют собой список идентификаторов учётных записей, которые могут включать в себя полное имя, псевдоним, имя в системе и любые другие данные, однозначно идентифицирующие пользователя, а также связанную с ними дополнительную информацию. Идентификатор используется для обогащения событий и инцидентов информацией в качестве дополнительного контекста для анализа.

Данные об узлах сети не содержат временных меток, фильтр времени к ним не применим.

4.6.5.1.2.1 Панели

Панели и их описание приведены ниже (Таблица 27).

Таблица 27. Панели

Панель	Описание
Количество учётных записей по индексам объектов	Отображает в таблице индексы объектов мониторинга и количество учётных записей для каждого из них. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Количество учётных записей по приоритетам	Отображает на гистограмме число учётных записей, сгруппированных по уровню их приоритета. Можно применить фильтр к текущему дашборду
Количество учётных записей по подразделениям	Отображает на круговой диаграмме процентное соотношение числа учётных записей отдельных подразделений к общему количеству учётных записей. Можно применить фильтр к текущему дашборду
Количество учётных записей по категориям	Отображает на круговой диаграмме процентное соотношение числа учётных записей отдельных категорий к общему количеству учётных записей. Можно применить фильтр к текущему дашборду
Информация об учётных записях	Отображает в таблице все учётные записи. Включает в себя идентификатор учётной записи (identity), имя (first), фамилию (last), электронную почту (email), номер телефона (phone), учётную запись руководителя (managedBy), приоритет (priority), подразделение (bunit), категорию (category), отметку отслеживания (watchlist), дату создания учётной записи (startDate), дату удаления / блокировки учётной записи (endDate), город (work_city), страну (work_country), широту(work_lat) и долготу (work_long). Можно применить фильтр к текущему дашборду

4.6.5.1.3 Центр сетевых сессий

Дашборд **Центр сетевых сессий** предназначен для анализа активности учётных записей в сети. В нём можно отследить используемые сетевые узлы и связанные с ними атрибуты, такие как IP-адрес, MAC-адрес и имя узла. Источниками этих данных могут быть события сетевого оборудования, DHCP- или VPN-сервисов.

4.6.5.1.3.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, выбрав значение из выпадающего списка (Таблица 28).

Таблица 28.Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга

4.6.5.1.3.2 Панели

Панели и их описание приведены ниже (Таблица 29).

Таблица 29. Панели

Панель	Описание
Количество сетевых сессий по времени	Отображает на графике число сетевых сессий на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду
Информация о сетевых сессиях	Отображает в таблице сетевые сессии за выбранный интервал времени. Включает в себя время (time), идентификатор узла источника (src_values), IP-адрес узла назначения (dest_ip), MAC-адрес узла назначения (dest_mac), имя операционной системы узла назначения (dest_nt_host), DNS-имя узла назначения (dest_dns) и учётную запись (user). Идентификатор узла источника (src_values) включает в себя значение полей src_ip, src_mac, src_nt_host и src_dns. Можно применить фильтр к текущему дашборду

4.6.5.2 Дашборды подраздела Доступ

Домен **Доступ** содержит данные о событиях доступа в корпоративной сети. Дашборды подраздела **Доступ** полезны для обнаружения злонамеренных попыток аутентификации, а также для идентификации систем, к которым пользователи получили доступ авторизованным или неавторизованным образом.

4.6.5.2.1 Центр доступа

Дашборд **Центр доступа** предоставляет сводку всех событий аутентификации. Он полезен для обнаружения инцидентов, связанных с попытками доступа. Например, для выявления атак подбора учётных данных, использования паролей в открытом виде, или доступа в определённые системы в нерабочее время.

4.6.5.2.1.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, нажав на фильтр-ссылку или выбрав значение из выпадающего списка (Таблица 30). Фильтры не применяются к ключевым показателям.

Таблица 30. Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга
Действие	Отображает на дашборде данные по выбранным действиям аутентификации учётных записей
Приложение	Отображает на дашборде данные по выбранным приложениям, которые использовались учётными записями

Фильтр	Описание
Показать события:	Отображает на дашборде данные по выбранной категории событий доступа (все, привилегированного доступа или с учётными записями «по умолчанию»)

4.6.5.2.1.2 Панели

Панели и их описание приведены ниже (Таблица 31).

Таблица 31. Панели

Панель	Описание
Ключевые индикаторы	Отображают на индикаторах ключевые метрики аутентификации за последние 24 часа. Дополнительные сведения см. в п. 4.5.4.2
Количество событий доступа по действиям	Отображает на составном закрашенном графике количество событий аутентификации по действиям на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях доступа**
Количество событий доступа по приложениям	Отображает на составном закрашенном графике количество событий аутентификации по приложениям на временной шкале за выбранный интервал времени. Например, события «app: win:local» относятся к локальной аутентификации в системе Windows, а «app: ssh» относятся к удалённому доступу. Можно применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях доступа**
Количество событий доступа по узлам источников	Отображает в таблице узлы источников с наибольшим количеством событий доступа за выбранный интервал времени. Эта таблица полезна для обнаружения атак методом перебора, они будут заметны по непропорционально большому количеству запросов на аутентификацию. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях доступа**
Количество уникальных учётных записей в событиях доступа по узлам источников	Отображает в таблице узлы источников с наибольшим количеством уникальных учётных записей за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях доступа**

4.6.5.2.2 Трекер доступа

Дашборд **Трекер доступа** предназначен для проверки статусов учётных записей. Он полезен для отслеживания впервые аутентифицированных или длительное время неактивных учётных записей, а также обнаружения учётных записей, которые не были должным образом отключены или удалены, когда пользователь покинул организацию. Такие учётные записи могут быть уязвимыми перед злоумышленниками.

4.6.5.2.2.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, нажав на фильтр-ссылку или выбрав значение из выпадающего списка (Таблица 32).

Таблица 32. Фильтр

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга

4.6.5.2.2.2 Панели

Панели и их описание приведены ниже (Таблица 33).

Таблица 33. Панели

Панель	Описание
Первый вход в сеть (за последние 7 дней)	Отображает в таблице учётные записи, осуществивших впервые вход на указанный узел назначения за последние 7 дней, время первого и последнего события доступа. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях доступа**
Использование учётных записей, ранее неактивных в течение 90 дней	Отображает в таблице учётные записи, которые были не активны в течение последних 90 дней, но осуществили вход в течение последних суток. Включает в себя количество дней между предыдущим и последним входами, время первого, предыдущего и последнего входа. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях доступа**
Неактивные учётные записи (за последние 90 дней)	Отображает в таблице учётные записи, которые не аутентифицировались в сети последние 90 дней. Включает в себя данные о количестве дней с последней аутентификации, время первого и последнего события входа. Следует использовать эту панель для обнаружения учётных записей, которые следует заблокировать или удалить. Если в организации есть политика, требующая периодической смены пароля, то учётные записи, которые не осуществляли вход дольше этого периода, можно считать не используемыми. Эта панель также указывает на эффективность политики организации по приостановке или удалению учётных записей. Если здесь отображается большое количество учётных записей, то рекомендуется пересмотреть процесс. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях доступа**

Панель	Описание
Использование учётных записей с истёкшим сроком действия	Отображает в таблице учётные записи, указанные в перечне активов, срок действия которых истёк, за выбранный интервал времени. Включает в себя имя и фамилию пользователя, срок действия учётной записи и время события. Эта панель полезна для проверки того, что учётные записи с истёкшим сроком действия не используются. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях доступа**

4.6.5.2.3 Поиск в событиях доступа

Дашборд **Поиск в событиях доступа** предназначен для поиска событий аутентификации и используется при переходе из дашбордов **Центр доступа** (см. п. 4.6.5.2.1) и **Трекер доступа** (см. .п. 4.6.5.2.2).

4.6.5.2.3.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, выбрав значение из выпадающего списка (Таблица 34).

Таблица 34. Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга
Действие	Отображает на дашборде данные по выбранным действиям средств аутентификации
Приложение	Отображает на дашборде данные по выбранным приложениям, осуществляющим аутентификацию
Узел источника	Отображает на дашборде данные по выбранным IP-адресам или именам узлов источников
Узел назначения	Отображает на дашборде данные по выбранным IP-адресам или именам узлов назначения
Учётная запись	Отображает на дашборде данные по выбранным учётным записям

4.6.5.2.3.2 Панели

Панели и их описание приведены ниже (Таблица 35).

Таблица 35. Панели

Панель	Описание
Данные по событиям доступа	Отображает в таблице метрики (количество событий, количество действий, количество приложений, время последнего события) для группы уникальных значений (узел источника, имя учётной записи, инициировавшей аутентификацию, узел назначения, аутентифицируемая учётная запись) за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Количество событий по действиям	Отображает в таблице действия средств аутентификации и количество событий для каждого из них за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Количество событий по приложениям	Отображает в таблице осуществляющие аутентификацию приложения и количество событий для каждого из них за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
События доступа	Отображает в таблице исходный вид событий доступа за выбранный интервал времени. Включает в себя время (time) и события в исходном виде (source). Можно применить фильтр к текущему дашборду

4.6.5.2.4 События управления учётными записями

Дашборд **События управления учётными записями** показывает статистику действий по управлению учётными записями пользователей, таких как блокировка, создание, изменение, отключение и сброс пароля. Следует использовать этот дашборд для контроля за управлением учётными записями и назначением им привилегированных прав. Внезапное увеличение таких событий может указывать на нарушение.

4.6.5.2.4.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, нажав на фильтр-ссылку (Таблица 36).

Таблица 36. Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга
Показать события:	Отображает на дашборде данные по выбранной категории событий доступа (все, привилегированного доступа или с учётными записями «по умолчанию»)

4.6.5.2.4.2 Панели

Панели и их описание приведены ниже (Таблица 37).

Таблица 37. Панели

Панель	Описание
Количество событий управления учётными записями по времени	Отображает на графике количество событий для каждого действия по управлению учётными записями на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду или перейти к просмотру исходных событий в **Discover**
Количество блокировок учётных записей по имени	Отображает в таблице количество событий блокировок учётных записей для группы уникальных значений (узел источника, NT-домен узла источника, учётная запись) за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти к просмотру исходных событий в **Discover**
Количество событий управления учётными записями по имени инициатора	Отображает на гистограмме инициаторов действий управление учётными записями с наибольшим количеством событий управления учётными записями за выбранный интервал времени. Инициатор — это пользователь, который выполнил действие по управлению учётной записью, а не пользователь, на которого повлияло данное действие. Например, если пользователь «Ivanov_A» создаёт учётную запись «Petrov_A», то «Ivanov_A» является инициатором. Эта панель помогает выявить учётные записи, которые не должны управлять другими учётными записями, и показывает всплески количества событий управления учётными записями, например, таких, как удаление большого количества учётных записей. Можно применить фильтр к текущему дашборду или перейти к просмотру исходных событий в **Discover**
Количество событий управления учётными записями по действию	Отображает в таблице действия с наибольшим количеством событий за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти к просмотру исходных событий в **Discover**

4.6.5.2.5 Активность учётных записей «по умолчанию»

Дашборд **Активность учётных записей «по умолчанию»** показывает активность учётных записей, встроенных или активированных «по умолчанию» в программном обеспечении различных систем, например, в устройствах сетевой инфраструктуры, базах данных и операционных системах. Такие учётные записи могут быть не деактивированы должным образом при развертывании системы, иметь предустановленные и широко известные пароли и использоваться злоумышленниками для атак.

Многие политики требуют, чтобы учётные записи «по умолчанию» были отключены. В некоторых случаях может потребоваться мониторинг или расследование

использования учётной записи «по умолчанию». Важно убедиться, что пароли к учётным записям «по умолчанию» изменены. Необычное поведение учётной записи «по умолчанию» может указывать на угрозу или нарушение политики.

4.6.5.2.5.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, нажав на фильтр-ссылку (Таблица 38).

Таблица 38. Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга

4.6.5.2.5.2 Панели

Панели и их описание приведены ниже (Таблица 39).

Таблица 39. Панели

Панель	Описание
Количество событий с учётными записями «по умолчанию» по приложениям	Отображает на графике количество событий аутентификации учётных записей «по умолчанию», сгруппированных по приложениям на временной шкале, за выбранный интервал времени. Следует использовать эту панель для выявления необычной активности использования встроенных учётных записей тем или иным приложением. Для некоторых приложений такая активность может быть обычным явлением (например, ежедневным событием), а для других — указывать на компрометацию системы. Можно применить фильтр к текущему дашборду или перейти к просмотру исходных событий в **Discover**
Время последнего использования учётных записей «по умолчанию»	Отображает в таблице недавно использованные учётные записи «по умолчанию», с указанием категории учётной записи, количества узлов источника и времени последнего события за выбранный интервал времени. Эта панель помогает выявить аномальную активность встроенных учётных записей. Можно применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях доступа**

4.6.5.3 Дашборды подраздела Сеть

Домен **Сеть** включает в себя информацию о сети и сетевых устройствах, таких как маршрутизаторы, коммутаторы, межсетевые экраны и устройства обнаружения вторжений. Здесь представлена информация о сетевом трафике: объём и типы трафика, генерирующих трафик устройствах или пользователях, сетевых портах.

4.6.5.3.1 Центр трафика

Дашборд **Центр трафика** отображает общую картину сетевого трафика, помогает отслеживать изменения тренда объёма трафика, а также определить причину (например, устройство или источник) этих изменений. Увеличение трафика может быть связано с нарушением.

4.6.5.3.1.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, выбрав значение из выпадающего списка (Таблица 40).

Таблица 40. Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга
Действие	Отображает на дашборде данные по выбранному действию правила межсетевого экрана
Протокол	Отображает на дашборде данные по выбранным протоколам

4.6.5.3.1.2 Панели

Панели и их описание приведены ниже (Таблица 41).

Таблица 41. Панели

Панель	Описание
Ключевые индикаторы	Отображают на индикаторах ключевые метрики сетевого трафика за последние 24 часа. Дополнительные сведения см. в п. 4.5.4.2
Количество событий сетевого трафика по времени и действиям	Отображает на графике количество событий сетевого трафика по действиям на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях трафика**
Количество событий сетевого трафика по времени и протоколам	Отображает на графике количество событий сетевого трафика по протоколам на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях трафика**
Количество событий сетевого трафика по источникам	Отображает в таблице наиболее активные узлы источников (с которыми зарегистрировано наибольшее количество событий), с указанием количества узлов назначения за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях трафика**
Количество узлов назначения сетевого трафика по источникам	Отображает на гистограмме узлы источников с наибольшим количеством узлов назначения за выбранный интервал времени. Позволяет обнаружить активность сетевых сканеров и выявить узлы, на которых они расположены. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях трафика**

4.6.5.3.2 Поиск в событиях трафика

Дашборд **Поиск в событиях трафика** предназначен для поиска данных событий сетевого трафика и используется при переходе из дашборда **Центр трафика** (см. п. 4.6.5.3.1).

4.6.5.3.2.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, выбрав значение из выпадающего списка или указав диапазон (Таблица 42).

Таблица 42. Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга
Действие	Отображает на дашборде данные по выбранному действию правила межсетевого экрана
Узел источника	Отображает на дашборде данные по выбранным IP-адресам или именам узлов источников
Узел назначения	Отображает на дашборде данные по выбранным IP-адресам или именам узлов назначения
Протокол	Отображает на дашборде данные по выбранным протоколам
Порт узла назначения	Отображает на дашборде данные по выбранному диапазону портов узла назначения

4.6.5.3.2.2 Панели

Панели и их описание приведены ниже (Таблица 43).

Таблица 43. Панели

Панель	Описание
Данные по событиям трафика	Отображает в таблице метрики (количество действий правил межсетевого экрана, количество портов источника, время последнего события и количество событий) для группы уникальных значений (узел источника, узел назначения, протокол, порт узла назначения) за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Количество событий по действиям	Отображает в таблице действия правил межсетевого экрана и количество событий для каждого из них за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Количество событий по портам узла источника	Отображает в таблице перечень портов узлов источников и количество событий для каждого из них за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
События трафика	Отображает в таблице исходный вид событий трафика за выбранный интервал времени. Включает в себя время (time) и события сетевого трафика в исходном виде (message). Можно применить фильтр к текущему дашборду

4.6.5.3.3 Центр Веб

Следует использовать дашборд **Центр Веб** для анализа событий веб-трафика, например, поиска и устранения потенциальных угроз, связанных с чрезмерным объёмом веб-трафика, типом загруженного контента или сбоями в работе веб-сервисов.

4.6.5.3.3.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, выбрав значение из выпадающего списка или указав диапазон (Таблица 44). Фильтры не применяются к ключевым показателям.

Таблица 44. Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга

4.6.5.3.3.2 Панели

Панели и их описание приведены ниже (Таблица 45).

Таблица 45. Панели

Панель	Описание
Ключевые индикаторы	Отображают на индикаторах ключевые метрики веб-трафика за последние 24 часа. Дополнительные сведения см. в п. 4.5.4.2
Количество событий по методу	Отображает на гистограмме количество веб-событий по HTTP-методам (POST, GET, direct, referral и т. д.), на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях Веб**
Количество событий по статусу	Отображает на гистограмме количество веб-событий по статусам HTTP-ответа на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду или перейти на дашборд **Поиск в событиях Веб**
Изменение количества событий по узлам источников	Отображает на графике узлы источников с наибольшим изменением количества веб-событий за выбранный интервал времени. Эта панель полезна для обнаружения всплесков объёма веб-трафика и связанных с этим объемом узлов (например, клиентов файлообменных веб-сервисов). Можно перейти на дашборд **Поиск в событиях Веб**
Изменение количества событий по узлам назначения	Отображает на графике узлы назначений с наибольшим изменением количества веб-событий за выбранный интервал времени. Эта панель полезна для обнаружения всплесков объёма веб-трафика и связанных с этим объемом узлов (например, файлообменных веб-сервисов). Можно перейти на дашборд **Поиск в событиях Веб**

4.6.5.3.4 Поиск в событиях Веб

Дашборд **Поиск в событиях Веб** помогает искать данные в веб-событиях и используется при переходе из дашборда **Центр Веб** (см. п. 4.6.5.3.3).

4.6.5.3.5 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, выбрав значение из выпадающего списка (Таблица 46).

Таблица 46. Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга
HTTP-метод	Отображает на дашборде данные по выбранным HTTP-методам
Статус	Отображает на дашборде данные по выбранным HTTP-статус-кодам
Узел источника	Отображает на дашборде данные по выбранным IP-адресам или именам узлов источников
Узел назначения	Отображает на дашборде данные по выбранным IP-адресам или именам узлов назначения
URL	Отображает на дашборде данные по выбранным URL-адресам

4.6.5.3.5.1 Панели

Панели и их описание приведены ниже (Таблица 47).

Таблица 47. Панели

Панель	Описание
Данные по событиям Веб	Отображает в таблице метрики (количество HTTP-методов, количество статусов, время последнего события и количество событий) для группы уникальных значений (узел источника, узел назначения, URL) за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Количество событий по методу HTTP-запроса	Отображает в таблице HTTP-методы и количество событий для каждого из них за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Количество событий по статусу HTTP-ответа	Отображает в таблице HTTP-статусы и количество событий для каждого из них за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
События Веб	Отображает в таблице исходный вид событий Веб за выбранный интервал времени. Включает в себя время (time) и веб-события в исходном виде (message). Можно применить фильтр к текущему дашборду

4.6.5.4 Дашборды подраздела Конечные узлы

Домен **Конечные узлы** включает в себя информацию о событиях средств обнаружения потенциально вредоносных программ. К таким программам могут относиться, например, вирусы, сетевые черви, троянские программы, шпионское программное обеспечение, утилиты злоумышленников, рекламное программное обеспечение, потенциально нежелательным программы и другие программы, классифицируемые антивирусными средствами.

4.6.5.4.1 Центр вредоносных программ

Дашборд **Центр вредоносных программ** помогает выявлять вспышки распространения вредоносного программного обеспечения. Здесь можно отследить реакцию антивирусных средств на обнаруженный вредоносный код и статистику обнаружения новых вредоносных программ.

4.6.5.4.1.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, выбрав значение из выпадающего списка (Таблица 48).

Таблица 48. Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга
Действие	Отображает на дашборде данные по выбранному действию с вредоносной программой

4.6.5.4.1.2 Панели

Панели и их описание приведены ниже (Таблица 49).

Таблица 49. Панели

Панель	Описание
Ключевые показатели	Отображают на индикаторах ключевые метрики противодействия вредоносным программам за последние 24 часа. Дополнительные сведения см. в п. 4.5.4.2
Активность вредоносных программ по времени и действиям	Отображает на графике количество событий для каждого действия антивирусных средств на временной шкале за выбранный интервал времени. Следует использовать эту панель для выявления большого количества действий, указывающих на пропуск обнаруженных вредоносных программ. Можно применить фильтр к текущему дашборду или перейти на дашборд **Поиск по вредоносным программам**

Панель	Описание
Активность вредоносных программ по времени и сигнатуре	Отображает на графике количество событий для каждой обнаруженной сигнатуры вредоносных программ на временной шкале за выбранный интервал времени. Следует использовать эту панель, чтобы определить, какие вредоносные программы обнаруживаются чаще всего. Можно применить фильтр к текущему дашборду или перейти на дашборд **Поиск по вредоносным программам**
Количество узлов по вредоносным программам	Отображает на гистограмме часто обнаруживаемые сигнатуры вредоносных программ за выбранный интервал времени. Эта панель помогает выявить вспышки распространения отдельных сигнатур вредоносных программ. Можно применить фильтр к текущему дашборду или перейти на дашборд **Поиск по вредоносным программам**
Новые вредоносные программы за 30 дней	Отображает в таблице вредоносные программы, которые были впервые обнаружены за последние 30 дней. Для каждой сигнатуры вредоносной программы отображается время первого обнаружения и количество зараженных узлов. Впервые обнаруженные сигнатуры чаще других являются источниками вспышек распространения вредоносного программного обеспечения. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Поиск по вредоносным программам**

4.6.5.4.2 Поиск по вредоносным программам

Дашборд **Поиск по вредоносным программам** помогает искать события обнаружения вредоносных программ, и используется при переходе из дашборда **Центр вредоносных программ** (см. п. 4.6.5.4.1).

4.6.5.4.2.1 Фильтры

Фильтры используются для уточнения результатов поисковых запросов, отображаемых на панелях дашборда. Их можно применять, выбрав значение из выпадающего списка (Таблица 50).

Таблица 50. Фильтры

Фильтр	Описание
Объект	Отображает на дашборде данные по выбранным объектам мониторинга
Действие	Отображает на дашборде данные по выбранному действию с вредоносной программой
Сигнатура	Отображает на дашборде данные по выбранной сигнатуре вредоносной программы
Имя файла	Отображает на дашборде данные по выбранному имени файла
Узел назначения	Отображает на дашборде данные по выбранным узлам назначения
Учётная запись	Фильтр по наименованию учётной записи

4.6.5.4.2.2 Панели

Панели и их описание приведены ниже (Таблица 51).

Таблица 51. Панели

Панель	Описание
Количество событий по сигнатуре и узлу назначения	Отображает в таблице метрики (количество действий, количество файлов, учётную запись из последнего события, время последнего события и количество событий) для групп уникальных значений (сигнатура, узел назначения) за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Количество событий по действиям	Отображает в таблице действия антивирусных средств с вредоносными программами и количество событий за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Количество событий по имени файла	Отображает в таблице наименования заражённых файлов и количество событий за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
События вредоносных программ	Отображает в таблице события вредоносных программ. Включает в себя время (time) и события в исходном виде (_source). Можно применить фильтр к текущему дашборду

4.6.6 Аудит

4.6.6.1 Дашборды раздела Аудит

Дашборды раздела **Аудит** предназначены для контроля за выполнением основных операций в Security Data Lake. Они помогут убедиться, что осуществляется сбор данных в систему, корректно срабатывают правила корреляции, выполняются задачи по реагированию и расследованию инцидентов.

4.6.6.1.1 Аудит анализа инцидентов

Дашборд **Аудит анализа инцидентов** обеспечивает возможность проверки и оценки производительности действий по анализу и реагированию на инциденты. На дашборде отображается статистика в разрезе пользователей, владельцев инцидентов и правил корреляции, а также список недавних событий анализа инцидентов. Эта информация в первую очередь полезна руководителям подразделений.

4.6.6.1.1.1 Панели

Панели и их описание приведены ниже (Таблица 52).

Таблица 52. Панели

Панель	Описание
Количество событий изменения инцидентов по времени и учётным записям	Отображает на гистограмме количество действий для каждой учётной записи. Эта панель полезна для определения того, какие Аналитики выполняли анализ и реагирование на инциденты и как менялось общее количество анализируемых инцидентов с течением времени. Можно применить фильтр к текущему дашборду
Количество событий изменения инцидентов по учётным записям	Отображает таблицу с перечнем учётных записей, участвующих в анализе и реагировании на инциденты, включая количество инцидентов, количество событий, дату первого и последнего события. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Количество инцидентов по статусу	Отображает на гистограмме статус, количество и степень срочности незаглушенных инцидентов за выбранный интервал времени. Эта панель полезна для определения того, успевают ли Аналитики обработать инциденты и какая очередь нерассмотренных инцидентов. Можно применить фильтр к текущему дашборду или перейти на дашборд **Анализ инцидентов**
Количество инцидентов по владельцу	Отображает на гистограмме владельцев инцидентов, количество инцидентов и степень срочности для незаглушенных инцидентов за выбранный интервал времени. Эта панель полезна для понимания распределения количества и срочности инцидентов между владельцами. Можно применить фильтр к текущему дашборду или перейти на дашборд **Анализ инцидентов**
Среднее время до начала анализа инцидента по правилам корреляции	Отображает в таблице средний и максимальный интервал времени до изменения первоначального статуса инцидента по каждому правилу корреляции за выбранный интервал времени. Эта панель полезна для определения того, сколько времени проходит до начала работы над инцидентом. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Анализ инцидентов**
Среднее время до завершения анализа инцидента по правилам корреляции	Отображает в таблице средний и максимальный интервал времени до завершающего статуса инцидента по каждому правилу корреляции за выбранный интервал времени. Эта панель полезна для определения того, насколько быстро Аналитики справляются с анализом инцидентов, а также для определения того, требуется ли для некоторых типов инцидентов больше времени, чем для других. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Анализ инцидентов**
События анализа инцидентов	Отображает в таблице события по анализу и реагированию на инциденты за выбранный интервал времени. Включает в себя время (time), идентификатор события (event ID), статус (status), правило корреляции (csinfo.rule.name.ru), учётную запись (user), комментарий (comment) и владельца инцидента (owner). Можно применить фильтр к текущему дашборду

4.6.6.1.2 Аудит глушений

Дашборд **Аудит глушений** предоставляет возможность проверки результатов применения фильтров глушения ложных инцидентов. Этот дашборд показывает статистику по исключённым из обработки инцидентам и действия по настройке соответствующих фильтров. Эта информация в первую очередь полезна руководителям подразделений.

Метрики на этом дашборде позволяют определить необходимость доработки правил корреляции, применения индексов исключений или выявить ошибки фильтров глушений. На это может указывать большое количество заглушенных инцидентов.

4.6.6.1.2.1 Панели

Панели и их описание приведены ниже (Таблица 53).

Таблица 53. Панели

Панель	Описание
Количество заглушенных инцидентов по времени и правилам	Отображает на гистограмме количество инцидентов, подпадающих под включенные на данный момент фильтры глушений за выбранный интервал времени. Можно применить фильтр к текущему дашборду
История количества заглушенных инцидентов по времени и правилам	Отображает на гистограмме количество заглушенных инцидентов, в отношении которых действовали фильтры глушений за выбранный интервал времени. Факт глушения инцидента фиксируется с частотой 15 минут. Можно применить фильтр к текущему дашборду
События управления глушениями	Отображает в таблице действия по изменению и включению фильтров глушений инцидентов за выбранный интервал времени. Включает в себя время (time), идентификатор глушения (suppression_id), учётную запись (user), действие (action), результат (message), наименование (suppression_name), описание (suppression_description), запрос (search_query) и статус (active). Можно применить фильтр к текущему дашборду
Глушения с истёкшим сроком действия	Отображает в таблице перечень и фильтры глушений, у которых завершилось время действия относительно выбранного интервала времени. Можно применить фильтр к текущему дашборду
Инциденты, подпадающие под действующие глушения	Отображает в таблице исходный вид инцидентов, подпадающих под действующие фильтры глушений за выбранный интервал времени. Включает в себя время (time) и инцидент в исходном виде (source). Можно применить фильтр к текущему дашборду

4.6.6.1.3 Аудит расследований

Дашборд **Аудит расследований** обеспечивает возможность проверки и оценки производительности действий по расследованию инцидентов. На дашборде отображается статистика в разрезе пользователей и участников расследований, а также список недавних действий в расследованиях. Эта информация в первую очередь полезна руководителям подразделений.

4.6.6.1.3.1 Панели

Панели и их описание приведены ниже (Таблица 54).

Таблица 54. Панели

Панель	Описание
Количество действий в расследованиях по времени и учётным записям	Отображает на гистограмме количество действий для каждой учётной записи за выбранный интервал времени. Эта визуализация полезна для определения того, кто участвовал в расследованиях и как менялось общее количество действий в расследованиях с течением времени. Можно применить фильтр к текущему дашборду
Количество действий в расследованиях по учётным записям	Отображает в таблице перечень учётных записей, участвующих в расследованиях, за выбранный интервал времени. Включая количество действий, дату первого и последнего действия. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Количество расследований по статусу	Отображает на гистограмме статусы и количество расследований за выбранный интервал времени. Эта панель полезна для определения того, успевают ли Аналитики провести расследования и какая очередь незавершённых расследований. Можно применить фильтр к текущему дашборду или перейти на дашборд **Расследования**
Количество расследований по участникам	Отображает на гистограмме участников и количество расследований за выбранный интервал времени. Эта панель полезна для понимания распределения расследований между участниками. Можно применить фильтр к текущему дашборду или перейти на дашборд **Расследования**
Количество инцидентов по расследованиям	Отображает на гистограмме количество инцидентов в расследованиях за выбранный интервал времени. Можно применить фильтр к текущему дашборду или перейти на дашборд **Расследования**
Количество расследований по инцидентам	Отображает в таблице инциденты с наибольшим количеством расследований за выбранный интервал времени. Эта панель полезна для выявления ошибочно добавленных в расследования инцидентов. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Расследования**
Время до закрытия по расследованиям	Отображает в таблице наименование расследований, ID расследований, время до закрытия и количество текущих участников расследования в настоящее время. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду или перейти на дашборд **Расследования**

Панель	Описание
Действия в расследованиях	Отображает в таблице действия учётных записей, проводящих расследования, за выбранный интервал времени. Включает в себя время (time), идентификатор расследования (investigation ID), учётную запись (user), статус отправки уведомлений (message status), действие (name), примечание (note), статус (status), участники (collaborators) и идентификаторы инцидентов (event ID). Можно применить фильтр к текущему дашборду

4.6.6.1.4 Количество поступающих событий

Дашборд **Количество поступающих событий** предназначен для оценки скорости поступления данных в Security Data Lake. На дашборде отображается количество индексируемых событий в секунду (EPS, Events Per Second).

4.6.6.1.4.1 Панели

Панели и их описание приведены ниже (Таблица 55).

Таблица 55. Панели

Панель	Описание
Среднее значение EPS по объектам	Отображает в таблице идентификатор объекта мониторинга с указанием усреднённого значения EPS за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Среднее значение EPS по времени и объектам	Отображает на гистограмме среднее значение EPS по объектам мониторинга на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду
Количество событий по продукту	Отображает в таблице количество поступивших событий и устройств для каждого вендора, продукта и версии за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Количество событий по типу источника	Отображает в таблице количество поступивших событий и устройств для каждого типа источника с указанием наименования источника за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Среднее значение EPS по вендору	Отображает в таблице среднее значение EPS для каждого вендора за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Среднее значение EPS по вендору и времени	Отображает на графике среднее значение EPS для каждого вендора на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду
Среднее значение EPS по устройствам	Отображает в таблице устройства с наибольшими средними значениями EPS с указанием вендора и агента сбора за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду

4.6.6.1.5 Объём поступающих событий

Дашборд **Объём поступающих событий** предназначен для оценки объёмов данных, проиндексированных в Security Data Lake. Объём данных измеряется в количестве байт всех значений поступивших событий.

4.6.6.1.5.1 Панели

Панели и их описание приведены ниже (Таблица 56).

Таблица 56. Панели

Панель	Описание
Объём событий по объектам	Отображает в таблице идентификатор объекта мониторинга с указанием объёма событий за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Объём событий по времени и объектам	Отображает на гистограмме объём событий по объектам мониторинга на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду
Объём событий по продукту	Отображает в таблице объём событий и количество устройств для каждого вендора, продукта и версии за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Объём событий по типу источника	Отображает в таблице объём событий и количество устройств для каждого типа источника с указанием наименования источника за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Объём событий по вендору	Отображает в таблице объём событий для каждого вендора за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду
Объём событий по вендору и времени	Отображает на графике объём событий для каждого вендора на временной шкале за выбранный интервал времени. Можно применить фильтр к текущему дашборду
Объём событий по устройствам	Отображает в таблице устройства с наибольшим объёмом событий с указанием вендора и агента сбора за выбранный интервал времени. Можно экспортировать данные из таблицы, применить фильтр к текущему дашборду