**Управление Splunk® Enterprise Security**

**Splunk Enterprise Security 5.1.0**

Создан: 05.14.2018 11:48

Все права защищены © Компания «Splunk Inc.», 2018

[Обзор 1](#_Toc514776010)

[Управление Splunk Enterprise Security 1](#_Toc514776011)

[Анализ происшествий и расследования 3](#_Toc514776012)

[Управление анализом происшествий в Splunk Enterprise Security 3](#_Toc514776013)

[Персональная настойка анализа инцидентов в Splunk Enterprise Security 4](#_Toc514776014)

[Создание заметного события вручную в Splunk Enterprise Security 7](#_Toc514776015)

[Персональная настройка параметров заметных событий в Splunk Enterprise Security 8](#_Toc514776016)

[Расширение базовых элементов заметных событий с помощью команды expandtoken 15](#_Toc514776017)

[Управление расследованиями в Splunk Enterprise Security 17](#_Toc514776018)

[Администрирование и персональная настройка рабочей среды расследования 19](#_Toc514776019)

[Управление статусами расследования и их персональная настройка в Splunk Enterprise Security 25](#_Toc514776020)

**Поиски корреляций 28**

Обзор поиска корреляций для Splunk Enterprise Security 28

Создание поисков корреляций в Splunk Enterprise Security 28

Конфигурация поисков корреляций в Splunk Enterprise Security 29

Список поисков корреляций в Splunk Enterprise Security 33

Обновление поисков корреляций в Splunk Enterprise Security 34

Установка адаптивных ответных действий в Splunk Enterprise Security 39

Конфигурация адаптивных ответных действий для поисков корреляций в Splunk Enterprise Security 41

**Цифровые объекты и идентификаторы** 47

Добавление данных об цифровых объектах и идентификаторах в Splunk Enterprise Security 47

Сбор и извлечение данных об цифровых объектах и идентификаторах в Splunk Enterprise Security 47

Определение форматов идентификаторов в Splunk Enterprise Security 49

Форматирование списка цифровых объектов или идентификаторов в качестве справочника в Splunk Enterprise Security 50

Конфигурация нового списка цифровых объектов или идентификаторов в Splunk Enterprise Security 58

Подтвердите, что ваш цифровой объект и идентификатор были добавлены в Splunk Enterprise Security 60

Конфигурация корреляции цифровых объектов и идентификаторов в Splunk Enterprise Security 62

Как Splunk Enterprise Security обрабатывает и объединяет данные цифровых объектов и идентификаторов 63

Справочники, в которых хранятся объединенные данные цифровых объектов и идентификаторов, в Splunk Enterprise Security 65

**Цифровые объекты и идентификаторы**

Поля цифровых объектов и идентификаторов после обработки в Splunk Enterprise Security 65

Проверка процесса объединения цифровых объектов и идентификаторов в Splunk Enterprise Security 68

Персональная настройка процесса объединения цифровых объектов и идентификаторов в Splunk Enterprise Security 69

Измените справочников цифровых объектов и идентификаторов в Splunk Enterprise Security 69

Примеры методов добавления данных цифровых объектов и идентификаторов в Splunk Enterprise Security 71

**Аналитика угроз 74**

Добавление аналитики угроз в Splunk Enterprise Security 74

Поддерживаемые типы аналитики угроз в Splunk Enterprise Security 75

Конфигурация включенных источников аналитики в Splunk Enterprise Security 76

Загрузка исходных данных аналитики угроз из Интернета в Splunk Enterprise Security 79

Загрузка структурированного файла аналитики угроз STIX или OpenIOC в Splunk Enterprise Security 85

Загрузка пользовательского файла аналитики угроз CSV в Splunk Enterprise Security 88

Добавление информации об угрозах из Splunk events в Splunk Enterprise Security 89

Добавление и локальное обслуживание аналитики угроз в Splunk Enterprise Security 90

Добавление аналитики угроз с помощью пользовательского справочника в Splunk Enterprise Security 90

Подтвердите, что вы успешно добавили аналитику в Splunk Enterprise Security 92

Изменение существующей аналитики в Splunk Enterprise Security 93

Пример: добавление исходных данных угрозы программы-вымогателя в Splunk Enterprise Security 96

**Обобщенная аналитика 99**

Добавление аналитики в Splunk Enterprise Security 99

Загрузка исходных данных аналитики из Интернета в Splunk Enterprise Security 99

Использование обобщенной аналитики при поиске с помощью inputintelligence 102

Пример: добавление источника обобщенной аналитики в Splunk Enterprise Security 105

**Управление контентом 108**

Управление контентом в Splunk Enterprise Security 108

Создание моделей данных и управление ими в Splunk Enterprise Security 108

Создание поисков по ключевым показателям и управление ими в Splunk Enterprise Security 109

Создание сохраненных поисков и управление ими в Splunk Enterprise Security 111

Создание справочников на основе поиска и управление ими в Splunk Enterprise Security 112

Создание поисков по линиям событий и управление ими в Splunk Enterprise Security 115

Создание витрин и управление ими в Splunk Enterprise Security 117

Экспорт контента из Splunk Enterprise Security как приложения 118

Создание справочников и управление ими в Splunk Enterprise Security 120

Управление внутренними справочниками в Splunk Enterprise Security 122

Создание риска и редактирование объектов риска в Splunk Enterprise Security 132

**Конфигурация и устранение неполадок 133**

Конфигурация общих настроек для Splunk Enterprise Security 133

Управление учетными данными в Splunk Enterprise Security 135

Управление разрешениями в Splunk Enterprise Security 137

Персональная настройка панели меню в Splunk Enterprise Security 138

Конфигурация фильтрации на панели в Splunk Enterprise Security 145

Создание веб-сообщения Splunk в Splunk Enterprise Security 147

Устранение неполадок при ошибках сценария в Splunk Enterprise Security 148

Устранение неполадок при сообщениях о поиске в каталогах по умолчанию, выполненном ролью admin 150

Устранение неполадок загрузки аналитики в Splunk Enterprise Security 151

Устранение неполадок в панелях мониторинга в Splunk Enterprise Security 152

Таблица требований к панели мониторинга для Splunk Enterprise Security 153

**Экстремальный поиск 171**

Как Splunk Enterprise Security использует экстремальный поиск 171

Примеры экстремального поиска в Splunk Enterprise Security 177

Команды экстремального поиска 182

Обзор

Управление Splunk Enterprise Security

Администраторы Splunk Enterprise Security отвечают за конфигурирование, обслуживание, аудит и персональную настройку копии Splunk Enterprise Security. Если вы не являетесь администратором Splunk Enterprise Security, см. раздел «Использование Splunk Enterprise Security» для ознакомления с использованием этого приложения в качестве аналитика безопасности.

Используйте ссылки ниже, чтобы узнать больше об административных задачах в программе Splunk Enterprise Security.

Управление аналитическими рабочими процессами и их поддержка

Для обеспечения и индивидуальной настройки рабочих процессов для аналитиков в вашей организации, см. разделы:

* «Управление анализом происшествий в Splunk Enterprise Security»;
* «Персональная настройка анализа происшествий в Splunk Enterprise Security»;
* «Персональная настройка заметных событий в Splunk Enterprise Security»;
* «Управление расследованиями в Splunk Enterprise Security».

Наполнение Enterprise Security данными

Наполнение Splunk Enterprise Security данными об цифровых объектах и идентификаторах в вашей среды и дополнительными данными об известных угрозах.

* См. полный список задач, связанных с добавлением данных об цифровых объектах и идентификаторах и их управлением в Splunk Enterprise Security, в разделе «Добавление данных об цифровых объектах и идентификаторах в Splunk Enterprise Security».
* См. информацию обо всех задачах, связанных с управлением источниками угроз в Splunk Enterprise Security, в разделе «Добавление информации об угрозах для Splunk Enterprise Security».

Управление конфигурацией и ее персональная настройка

Для выполнения текущей конфигурации в Splunk Enterprise Security, см.:

* «Конфигурация общих настроек для Splunk Enterprise Security»;
* «Управление учетными данными ввода в Splunk Enterprise Security»;
* «Управление разрешениями в Splunk Enterprise Security».
* «Персональная настройка панели меню в Splunk Enterprise Security»;
* «Конфигурация расширенной фильтрации в Splunk Enterprise Security».

Вы можете найти дополнительную информацию о конфигурации в *Руководстве по установке и обновлению*.

* Каталоги конфигурации и запуска.
* Конфигурация пользователей и ролей.
* Конфигурация моделей данных для Splunk Enterprise Security.

Создание, управление и экспорт контента

Для создания нового контента или управления и настройки существующего контента, см.:

* «Создание поиска корреляций в Splunk Enterprise Security»;
* «Создание поиска по ключевым показателям и управление им в Splunk Enterprise Security»;
* «Создание сохраненных результатов поиска и управление ими в Splunk Enterprise Security»;
* «Создание справочников на основе поиска и управление ими в Splunk Enterprise Security»;
* «Создание поиска в историях событий и управление им в Splunk Enterprise Security»;
* «Создание показов и управление ими в Splunk Enterprise Security»;
* «Создание справочников и управление ими в Splunk Enterprise Security»;
* «Создание риска и редактирование объектов риска в Splunk Enterprise Security».

Для получения информации о том, как поделиться персональным контентом с другими копиями ES, см. раздел «Экспорт содержимого из Splunk Enterprise Security как приложения».

Панели мониторинга «Устранение неполадок»

* Советы и лучшие методы, полезные для настройки панелей мониторинга «Устранение неполадок» см. в разделе «Панели мониторинга “Устранение неполадок” в Splunk Enterprise Security».
* Информация о наборах данных модели данных, которые наполняют панели мониторинга Enterprise Security, см. «Таблица требований к панели мониторинга для Splunk Enterprise Security».
* Обзор всех панелей мониторинга в Splunk Enterprise Security см. в разделе «Введение о панелях мониторинга, доступных в Splunk Enterprise Security» в *«Использование Splunk Enterprise Security»*.

Анализ происшествий и расследования

Управление анализом происшествий в Splunk Enterprise Security

Splunk Enterprise Security обнаруживает шаблоны в ваших данных и автоматически анализирует события на предмет происшествий, связанных с безопасностью, с использованием **поиска корреляций.** При обнаружении подозрительного шаблона связанный поиск создает предупреждение, называемое **заметным событием.**

Панель мониторинга «Анализ инцидента» охватывает все заметные события и классифицирует их по потенциальной серьезности, чтобы аналитики могли быстро сортировать, назначать и отслеживать проблемы.

* Информацию о том, как аналитики используют панель мониторинга «Анализ инцидента», см. в разделе «Обзор анализа инцидентов» в *«Использование Splunk Enterprise Security»*.
* Для аудита и анализа действий аналитиков на панели мониторинга «Анализ инцидента» см. раздел «Аудит анализа инцидентов» в *«Использование Splunk Enterprise Security»*.
* Для персональной настройки отображения панели мониторинга «Анализ инцидента», а также изменения возможностей и разрешений аналитиков см. раздел «Персональная настройка анализа инцидентов в Splunk Enterprise Security».
* Для создания заметного события вручную см. раздел «Создание заметного события вручную в Splunk Enterprise Security».
* Для персональной настройки параметров заметных событий см. раздел «Персональная настройка параметров заметных событий в Splunk Enterprise Security».
* Для получения дополнительной информации о том, как заметные события наполняются и управляются моделью заметных событий, см. раздел «Модель заметных событий в Splunk Enterprise Security» на портале разработчиков Splunk.

Как оценка риска отображается в анализе инцидентов

Оценка рисков не отображается в анализе инцидентов для каждого цифрового объекта или идентификатора. В анализе инцидентов отображаются только цифровой объекты или идентификаторы (объекты риска), оценка риска и тип объекта риска которых установлен как «система» или «пользователь». Оценки риска отображаются только для следующих полей: orig\_host, dvc, src, dest, src\_user и user. Оценка риска для цифровой объекта или идентификатора может не соответствовать шкале на панели мониторинга «Анализ риска». Оценка риска – это совокупный балл для цифровой объекта или идентификатора, а не балл, характерный для конкретного имени пользователя.

* Например, если человеку присвоено имя пользователя buttercup, оценка риска которого равна 40, и адрес электронной почты buttercup@splunk.com с оценкой риска 60, и поиск идентификатора устанавливает, что buttercup и buttercup@splunk.com принадлежат одному лицу, на панели Incident Review будет отображаться оценка риска, равная 100, для учетных записей buttercup и buttercup@splunk.com.
* В качестве другого примера, если IP-адрес 10.11.36.1 имеет оценку риска 80, а IP 10.11.36.19 имеет оценку риска 30, а поиск цифрового объекта устанавливает, что диапазон IP-адресов 10.11.36.1–10.11.36.19 относится к одному цифровому объекту, на панели Incident Review будет отображаться оценка риска, равная 110, для IP-адресов« 10.11.36.1 и 10.11.36.19.

Оценки риска рассчитываются для анализа инцидентов с использованием поиска с генерацией просмотров с помощью команды **Threat – Risk Correlation – Lookup Gen.** Поиск выполняется каждые 30 минут и обновляет файл поиска risk\_correlation\_lookup. Для более частых обновлений оценок риска на панели Incident Review, обновите файл сохраненного поиска cron\_schedule.

Уведомление аналитика о несортированных заметных событиях

Вы можете использовать поиск корреляций для уведомления аналитика в случае, если заметное событие не было отсортировано.

1. Выберите команду **Configure > Content Management.**
2. Определите поиск корреляций **Untriaged Notable Events,** используя фильтры.
3. Измените поиск посредством изменения владельца заметного события или полей состояния по желанию.
4. Задайте требуемое предупреждающее действие.
5. Сохраните изменения.
6. Запустите поиск корреляций **Untriaged Notable Events.**

Персональная настойка анализа инцидентов в Splunk Enterprise Security

В качестве администратора Splunk Enterprise Security вы можете настроить способ просмотра аналитиками заметных событий и взаимодействия аналитиков с заметными событиями на панели мониторинга Incident Review.

Изменение возможностей и разрешений аналитика

Настройте, могут ли аналитики переопределить рассчитанную срочность заметного события, и выберите, требовать ли от аналитика добавления комментария при обновлении заметного события на странице **Incident Review Settings.**

1. Выберите команду **Configure > Incident Management > Incident Review Settings** для просмотра настроек анализа инцидентов.
2. Разрешите или запретите аналитикам переопределять рассчитанную срочность заметного события с помощью флажка **Allow Overriding of Urgency.** По умолчанию аналитикам разрешено переопределять срочность.
3. Установите требование к аналитикам добавлять комментарий при обновлении заметного события, установив флажок **Required** в разделе **Comments.**
4. Если вы хотите, чтобы аналитики добавляли комментарий, введите минимальное количество символов для требуемых комментариев. Количество символов по умолчанию – 20.

Настройка рекомендуемой загрузки аналитиков

Настройте рекомендуемое максимальное количество заметных событий, которые должны быть назначены одному аналитику безопасности, на странице **General Settings.**

1. Для просмотра общих настроек выберите команду **Configure > General > General Settings.**
2. Введите предпочтительное количество заметных событий, которое должно быть назначено аналитику, с помощью настройки **Incident Review Analyst Capacity.** Значение по умолчанию – 12.

Это значение используется для целей аудита и не препятствует назначению аналитику большего числа заметных событий.

Изменение столбцов таблицы анализа инцидентов

Вы можете изменить столбцы, отображаемые на панели мониторинга Incident Review.

1. Просмотрите существующие столбцы в меню **Incident Review - Table Attributes.**
2. Используйте столбец действий для редактирования, удаления или изменения порядка доступных столбцов.
3. Добавьте пользовательские столбцы, выбрав команду **Insert below** или команду **More...**, затем – команду **Insert above.**

Устранение неполадок, когда аналитики не могут успешно редактировать заметные события в обзоре инцидентов

Если аналитики не смогут успешно редактировать заметные события на панели Incident Review, причиной может быть наличие нескольких проблем.

* У аналитика может отсутствовать разрешение на изменение статуса. См. Управление статусами заметный событий.
* Аналитик может попытаться отредактировать заметное событие, которое является видимым, но не может быть успешно отредактировано из-за ограниченного количества событий, которые могут быть восстановлены из корзины.

Если поиск корреляций создает большое количество заметных событий за короткий промежуток времени, например, 1000 менее чем за пять минут, панель мониторинга Incident Review может достигнуть предела max\_events\_per\_bucket при попытке восстановления заметных событий для отображения из каталога notable.

Если аналитики не могут редактировать заметное событие по этой причине, аналитик может использовать меньший временной интервал при просмотре заметных событий на панели Incident Review. Например, временной диапазон, который сокращает количество событий на панели мониторинга Incident Review до менее чем 1000. 1000 – это значение по умолчанию для max\_events\_per\_bucket, поэтому поиск, который производит менее 1000 событий, не может выдать эту ошибку.

Чтобы это не происходило, вы можете в любое время изменить максимальное количество событий, которые могут быть восстановлены из корзины. Однако изменение этого параметра может негативно повлиять на производительность развертывания программного обеспечения Splunk.

Если вы используете Splunk Enterprise Security в Splunk Cloud, подайте заявку на поддержку для этого параметра.

1. Откройте файл limits.conf для редактирования. См. раздел «Как редактировать файл конфигурации» в *Руководстве администратора* Splunk Enterprise.
2. Установите max\_events\_per\_bucket выше 1000.
3. Сохраните.

Подробнее о настройке max\_events\_per\_bucket см. в файле limits.conf.

Добавление ссылки навигации в фильтрованное отображение панели Incident Review

Чтобы помочь аналитикам ES с их рабочими процессами, вы можете добавить в навигацию приложения ссылку, которая загружает версию панели Incident Review с применением фильтров. См. раздел «Добавление ссылки в фильтрованное отображение панели “Анализ инцидентов”».

Создание заметного события вручную в Splunk Enterprise Security

Вы можете вручную создать заметное событие из индексированного события или с нуля.

**Примечание.** По умолчанию только администраторы могут вручную создавать заметные события. Чтобы предоставить другим пользователям эту возможность, см. раздел «Настройка пользователей и ролей» в *Руководстве по установке и обновлению*.

Создание заметного события из существующего события

Вы можете создать заметное событие из любого индексированного события с помощью меню **Event Actions.** Не создавайте заметные события из заметных событий на панели мониторинга Incident Review.

1. Из события просмотрите сведения о событии и нажмите **Event Actions.**
2. Выберите команду **Create notable event.**
3. Введите заголовоксобытия в поле **Title**.
4. (Опционально) Выберите **домен/Domain** безопасности.
5. (Опционально) Выберите уровень **Urgency.**
6. (Опционально) Выберите **Owner.**
7. (Опционально) Выберите **Status.**
8. В поле **Description** введите описание события, которое объясняет, почему вы создали заметное событие или что нужно исследовать.
9. Сохраните новое заметное событие. Панель мониторинга **Incident Review** отобразится с новым заметным событием.

**Примечание.** Заметное событие, созданное таким образом, включает в себя поля отслеживания, такие как **Owner** и **Status**, но не включает уникальные поля или ссылки, которые создаются при генерации заметного события предупреждающим действием поиска корреляций.

Создание заметного события с нуля

Создайте заметное событие, основанное на наблюдениях, результатах работы системы безопасности за пределами Splunk или иных источниках.

1. Выберите **Configure > Incident Management > New Notable Event.**
2. Введите заголовоксобытия в поле **Title**.
3. (Опционально) Выберите **Domain** безопасности.
4. (Опционально) Выберите уровень **Urgency.**
5. (Опционально) Выберите **Owner.**
6. (Опционально) Выберите **Status.**
7. В поле **Description** введите описание события, которое объясняет, почему вы создали заметное событие или что нужно исследовать.
8. Сохраните новое заметное событие. Панель мониторинга **Incident Review** отобразится с новым заметным событием.

Персональная настройка параметров заметных событий в Splunk Enterprise Security

В качестве администратора Splunk Enterprise Security вы можете вносить изменения в конфигурацию заметных событий.

* Изменение полей заметных событий.
* Управление статусами заметных событий.
* Создание скрытия заметных событий и управление им.

Изменение полей заметных событий

Внесите изменения в поля, отображаемые на панели мониторинга Incident Review, для заметных событий на панели мониторинга «Настройка панели анализа инцидентов». Например, измените метку поля в данных заметного события, удалите или добавьте поле в разделе **Additional Fields** данных заметного события. Изменения, которые вы вносите для полей заметных событий, затрагивают все заметные события.

1. В строке меню Splunk Enterprise Security выберите команду **Configure > Incident Management > Incident Review Settings.**
2. Просмотрите **Incident Review – Event Attributes.**
3. Нажмите **Edit,** чтобы изменить поле или метку для определенного поля, которое появляется на панели Incident Review.
4. Нажмите **Remove,** чтобы удалить поле из данных заметных событий на панели мониторинга Incident Review.
5. Нажмите **Save,** чтобы сохранить изменения.

***Добавление поля к данным заметного события***

Поле появляется в **Additional Fields** данных заметного события, если это поле существует в результатах поиска корреляций, а панель «Анализ инцидента» может отображать это поле. Чтобы добавить поле к данным заметного события, сначала убедитесь, что результаты поиска корреляций содержат это поле, а затем убедитесь, что панель «Анализ инцидента» может отображать это поле.

1. Определите, включено ли поле, которое вы хотите видеть, в результаты поиска корреляций. Запустите поиск корреляций на странице поиска, чтобы просмотреть результат или синтаксис поиска.
   * Если поле присутствует в результатах поиска, перейдите к шагу 4.
   * Если поле отсутствует в результатах поиска, перейдите к шагу 2.
2. Измените поиск корреляций, чтобы он включал нужное поле.
   * Если вы можете редактировать поиск с помощью управляемого редактора поиска, добавьте нужное поле в виде агрегатной функции с псевдонимом. Используйте функцию **values** для возврата всех возможных значений данного поля или **latest** функции, чтобы вернуть последнее значение поля.
   * Если вы создали поиск вручную, измените поиск, чтобы извлечь поля. Убедитесь, что вы не изменяете критерии корреляции при изменении поиска.
     + Если поиск не включает статистические преобразования, добавьте | fields + newfieldname до конца поиска, где newfieldname – это имя нового поля, которое вы хотите увидеть в дополнительных данных.
     + Если поиск включает статистические преобразования, извлеките поля при выполнении статистического преобразования. Например, если ваш поиск включает поиск статистики | stats count by src | where count>5, поля src и count появятся в данных заметного события. Чтобы добавить поле dest к данным заметного события, вы можете изменить поиск на следующее: | stats values (dest) as dest, count by src.
3. Перед сохранением проверьте изменения в поиске корреляций на странице поиска.
4. Добавьте поле в список дополнительных полей.
5. В строке меню Splunk Enterprise Security выберите **Configure > Incident Management > Incident Review Settings.**
6. Нажмите **Add new entry,** чтобы добавить новое поле в раздел **Additional Fields** данных заметного события.
7. В поле **Label** ведите **ярлык**, который будет использоваться в качестве отображаемого имени поля в данных заметного события.
8. Введите **Field**, соответствующее полю, которое вы хотите отобразить в данных заметного события.
9. Нажмите **Done.**
10. Нажмите **Save.**

Управление статусами заметных событий

Аналитик назначает заметному событию статус в ходе процесса расследования. Статус согласовывается со стадиями расследования и может использоваться для обзора и отчета о ходе расследования заметных событий на панели мониторинга аудита анализа инцидентов.

Контрольная панель.

Чтобы увидеть доступные статусы для заметных событий, выберите **Configure > Incident Management > Status Configuration.**

|  |  |  |
| --- | --- | --- |
| **Ярлык** | **Описание** | **Может быть отредактирован** |
| Не назначен/Unassigned | Используется Enterprise Security, когда ошибка препятствует назначению действительного статуса заметному событию | Нет |
| Новый/New (по умолчанию) | Заметное событие не просмотрено | Нет |
| Выполняется/In progress | Расследование или реагирование на заметное событие Выполняется | Да |
| Ожидает/Pending | Закрытие заметного события ожидает действия | Да |
| Разрешен/Resolved | Заметное событие разрешено и ожидает подтверждения | Да |
| Закрыт/Closed | Заметное событие разрешено и подтверждено | Да |

Каждому заметному событию при его создании поиском корреляций по умолчанию присваивается статус **Новый/New.** Вы можете настроить заметные статусы событий в соответствии с существующим рабочим процессом в вашей организации.

***Редактирование статусов заметных событий***

Измените статусы, доступные для заметных событий, на странице **Edit Notable Event Status.**

На панели инструментов Splunk Enterprise Security выберите команду **Configure > Incident Management > Status Configuration.**

Выберите статус заметного события, чтобы открыть страницу **Edit Notable Event Status.**

(Опционально) Измените **Label** или **Description.**

Вы не можете редактировать статусы **Unassigned** и **New**, поскольку они используются по умолчанию при создании заметных событий.

***Управление историей статусов заметного события***

Заметные события связаны с пользователями, статусами и комментариями. Изменения, вносимые в наименования статусов, влияют только на наименование статуса, а не на идентификатор статуса, присвоенный заметному событию в каталоге.

При изменении наименования статуса заметного события, используемого по умолчанию, наименование изменится для заметных событий как в прошлом, так и в будущем. Например, если вы переименуете Pending на «Ожидание клиента», все заметные события со статусом Pending будут иметь статус «Ожидание клиента». Идентификатор статуса, присвоенный заметным событиям, остается неизменным.

***Переходы статуса заметного события***

Статусы представляют шаги в расследовании заметного события. Переходы статуса определяют путь расследования заметного события.

Аналитик изменяет статус заметного события по мере продвижения расследования. Чтобы изменить статус заметного события:

* аналитик должен быть членом той роли, которая имеет разрешение на изменение статуса. Возможность изменения статусов заметных событий по умолчанию доступна ролям **ess\_analyst** и **ess\_admin;**
* последующий статус должен обеспечивать переход из текущего статуса. По умолчанию каждый статус может перейти на любой другой статус. Например, аналитик может изменить статус заметного события со статусом **New** на любой другой, например **Closed.**

***Ограничение переходов статуса заметного события***

Вы можете определить рабочий поток статусов и ограничить, какие статусы аналитики могут изменять на другие, создав путь для расследования заметного события. По умолчанию любой статус заметного события может быть изменен на любой другой статус.

***Необходимые условия***

* У вас должна быть роль **ess\_admin**, или вашей роли должна быть назначена способность **Edit Statuses.** Дополнительную информацию о ролях и возможностях пользователей см. в разделе «Настройка пользователей и ролей» в *Руководстве по установке и обновлению*.
* Определите рабочий поток статусов для расследований заметных событий. Определите, какие статусы потребуются, и должны ли аналитики следовать определенной последовательности статусов для завершения рабочего процесса. Определите, могут ли какие-либо роли обойти весь рабочий процесс.

***Шаги***

На панели инструментов Splunk Enterprise Security выберите команду **Configure > Incident Management > Status Configuration.**

Выберите статус заметного события, чтобы открыть страницу **Edit Notable Event Status.**

В меню Status Transitions измените поля **To Status**. Эти поля контролируют, какие статусы аналитики могут присваивать заметному событию, если оно находится в статусе, который вы редактируете.

Чтобы определить, каким ролям разрешено перевести заметное событие в выбранный статус, выберите поле **Authorization** и добавьте или удалите роли.

Чтобы удалить переход в выбранный статус для события, выберите **Unselect All.**

Нажмите **Save.**

**Пример ограничения переходов статуса заметного события**

В этом примере показано ограничение переходов статуса для аналитиков. Ограничьте переходы состояния, чтобы аналитики должны были пройти путь от New, к In Progress или Pending, к Resolved, затем к Closed.

1. На панели инструментов Splunk Enterprise Security выберите команду **Configure > Incident Management > Status Configuration.**
2. Ограничьте переходы из статуса **New.** Выберите статус **New,** чтобы открыть страницу Edit Investigation Status.
3. В разделе **Status Transitions** выберите роли для статуса **Resolved** и снимите флажок для роли ess\_analyst.
4. Выберите роли для статуса **Closed** и снимите флажок для роли ess\_analyst.
5. Нажмите **Save,** чтобы сохранить изменения в статусе **New.**
6. Ограничьте переходы в статусах **In Progress** и **Pending,** чтобы предотвратить возможность изменения на статус **New** или **Closed** для роли ess\_analyst.
7. Выберите статус **In Progress.**
8. В разделе **Status Transitions** выберите роли для статуса **New** и снимите флажок для роли ess\_analyst. Повторите указанные действия для статуса **Closed.**
9. Нажмите **Save,** чтобы сохранить изменения в статусе **In Progress.**
10. Повторите шаги 8 и 9 для статуса **Pending.**
11. Ограничьте статус **Resolved.** Перейдите на вкладку **Investigation** и выберите статус **Resolved.**
12. В разделе **Status Transitions** выберите роли для статуса **New** и снимите флажок для роли ess\_analyst. Повторите для статусов **In Progress** и **Pending.**
13. Нажмите **Save,** чтобы сохранить изменения в статусе **Resolved.**
14. Ограничьте переходы для статуса **Closed.** Выберите статус **Closed.**
15. В разделе **Status Transitions** выберите роли для статуса **New** и снимите флажок для роли ess\_analyst. Повторите для статусов **In Progress,** **Pending** и **Resolved.**
16. Нажмите **Save,** чтобы сохранить изменения для статуса **Closed.**

***Создание статуса***

Создайте статус для рабочего потока расследования заметного события.

***Необходимые условия***

Если вы ограничиваете переходы статуса, определите, требуется ли новый статус в рабочем потоке и могут ли какие-либо роли обходить новый статус в рабочем потоке.

**Шаги**

1. На панели инструментов Splunk Enterprise Security выберите команду **Configure > Incident Management > Status Configuration.**
2. Выберите команду **Create New Status > Notable.**
3. Введите **ярлык/Label,** который представляет статус, на панели мониторинга Incident Review.

Например, «Ожидание ИТ-операций».

1. (Опционально) Введите описание, которое отображается на странице Status Configuration.

Например, «Ожидание отдела ИТ-операций».

1. (Опционально) Установите флажок **Default Status.** Установите этот флажок, если вы хотите заменить статус по умолчанию **New** статусом для вновь созданных заметных событий.
2. (Опционально) Установите флажок **End Status.** Установите этот флажок, если вы добавляете дополнительный статус **Closed** для заметных событий, таких как **False Positive.**
3. (Опционально) Снимите флажок **Enabled.** Снимите этот флажок, если вы хотите создать статус, не применяя его.
4. Обновите переходы статуса, изменив поля **To Status.** Если вы не выбираете какие-либо роли, которые могут изменить этот статус на другой, никто не сможет переместить заметное событие в другой статус после перехода заметного события к этому статусу. Если вы не ограничиваете переходы статуса, выберите все роли для каждого статуса.
5. Нажмите **Save.**

Если вы ограничиваете переходы статуса на основании ролей пользователя, измените переходы статуса для каждого статуса, который может быть изменен на новый.

Создание скрытия заметных событий и управление им

Вы можете скрыть заметные события с панели мониторинга Incident Review, создав скрытие заметных событий.

Скрытие – это фильтр поиска, который скрывает дополнительные заметные события из представления и используется снижения чрезмерного или нежелательного количества заметных событий, появляющихся на панели мониторинга Incident Review. Заметные события, которые соответствуют условиям поиска, по-прежнему создаются и добавляются в каталог. Скрытые заметные события по-прежнему учитываются в счетчике заметных событий на панели «Тип безопасности» и панели аудита.

Чтобы предотвратить появление заметных событий, которые отвечают определенным условиям, см. раздел «Регулирование количества ответных действий, созданных поиском корреляций».

Вы можете создать фильтр скрытия двумя способами.

* Создать скрытие на панели Incident Review. См. раздел «Скрытие заметного инцидента».
* Создать скрытие в меню **Configure**. См. раздел «Создание скрытия посредством меню “Скрытие заметных событий”».

***Создание скрытия посредством меню «Скрытие заметных событий»***

1. Выберите команду **Configure > Incident Management > Notable Event Suppressions.**
2. Нажмите **Create New Suppression.**
3. Введите **Name** и **Description** фильтра скрытия.
4. Введите **Search**, который будет использоваться, чтобы найти заметные события, подлежащие скрытию.
5. Установите **Expiration Time.** Это определяет временной интервал для фильтра скрытия. Если временной интервал выдержан, фильтр скрытия отключается.

***Редактирование скрытия заметных событий***

1. Выберите команду **Configure > Incident Management > Notable Event Suppressions.**
2. Выберите скрытие заметного события, чтобы открыть страницу **Edit Notable Event Suppression.**
3. Отредактируйте поля **Description** и **поиска/Search**, используемые для фильтра подавления.
4. Нажмите **Save.**

***Отключение скрытия заметных событий***

1. Выберите команду **Configure > Incident Management > Notable Event Suppressions.**

Выберите **Disable** в столбце **Status** для скрытия заметных событий.

***Удаление скрытия заметных событий***

1. На панели инструментов платформы Splunk выберите команду **Settings > Event types.**
2. Найдите событие скрытия:

notable\_suppression- <suppression\_name>.

1. Выберите **delete** в столбце **Actions** для скрытия заметных событий.

***Аудит скрытия заметных событий***

Аудит скрытия заметных событий осуществляется с помощью панели мониторинга **Suppression Audit.** См. пункт «Аудит скрытия» в разделе «*Использование Splunk Enterprise Security*».

Расширение базовых элементов заметных событий с помощью команды expandtoken

Базовые элементы в названиях и описаниях заметных событий автоматически расширяются и включают значения базовых элементов на панели мониторинга Incident Review. С помощью команды поиска expandtoken вы можете расширить базовые элементы, чтобы в результатах поиска происходила замена базовых элементов.

Описание

Расширьте поля заметных событий, содержащих базовые элементы в значениях, таких как заголовок (rule\_name) или описание (rule\_description) заметного события. Базовые элементы автоматически расширяются на панели мониторинга Incident Review, но не в поиске.

Синтаксис

... | expandtoken [field], [field1], [field2] ...

***Дополнительный аргумент***

field

**Описание:** имя поля заметного события, которое содержит базовый элемент для расширения. Не указывайте имя базового элемента. Укажите дополнительные поля через запятую. Если вы не укажете поле, все поля будут обработаны на предмет базовых элементов для расширения. Список примеров полей заметных событий см. в разделе «Использование заметных событий в поиске на портале разработчиков Splunk».

Использование

Команда expandtoken является **потоковой командой.**

Ограничения

Команда поиска не поддерживает разделители базовых элементов в середине имени поля.

Если у вас есть базовые элементы, которые зависят от расширения других базовых элементов, такие базовые элементы могут быть ненадежно расширены, поскольку нет возможности указать порядок расширения базовых элементов. Например, если у вас есть rule\_description: «В $src$ обнаружен доступ грубой силой», и drilldown\_name: «См. вспомогательные события для $rule\_description$», следующий поиск может расширить базовый элемент $src$ без расширения базового элемента $rule\_description$.

'notable' | expandtoken

Дополнительную информацию о базовых элементах см. в разделе «Использование базовых элементов в панелях мониторинга» в *Руководстве по панелям мониторинга и визуализации* Splunk Enterprise.

Примеры

***Расширение базовых элементов для всех заметных событий***

'notable' | expandtoken

rule\_title, rule\_description, drilldown\_name, drilldown\_search

***Расширение базовых элементов для определенного заметного события***

Расширьте базовые элементы для определенного заметного события на основе поля event\_id.

'notable' | where event\_id = "<event\_id>" | expandtoken rule\_title, rule\_description

Расширьте базовые элементы для определенного заметного события на основе поля короткого идентификатора.

'notable' | where notable\_xref\_id="<short ID>" | expandtoken rule\_title,rule\_description

Смотрите также

Список примеров полей заметных событий см. в разделе «Использование заметных событий в поиске на портале разработчиков Splunk».

Дополнительную информацию о базовых элементах см. в разделе «Использование базовых элементов в панелях мониторинга» в *Руководстве по панелям мониторинга и визуализации* Splunk Enterprise.

Управление расследованиями в Splunk Enterprise Security

В качестве администратора Enterprise Security вы можете управлять доступом к расследованиям безопасности и поддерживать аналитиков, устраняя проблемы с их историей действий.

Дополнительную информацию о рабочем потоке расследований аналитика см. в пункте «Расследования в Splunk Enterprise Security» раздела «*Использование Splunk Enterprise Security*».

Управление доступом к расследованиям

Пользователи с ролью **ess\_admin** по умолчанию могут создавать, просматривать расследования и управлять ими. Пользователи с ролью **ess\_analyst** могут создавать и редактировать расследования. Внесите изменения в возможности с панели мониторинга «Разрешения».

* Чтобы позволить другим пользователям создавать или редактировать расследование, добавьте функцию **«Управление своими расследованиями»** в их роль. Пользователи могут вносить изменения только в расследования, участниками которых они являются.
* Чтобы позволить другим пользователям управлять, просматривать и удалять все расследования, добавьте функцию **«Управление всеми расследованиями»** к их роли.

См. раздел «Настройка пользователей и ролей» в *Руководстве по установке и обновлению*.

Вы можете управлять тем, кто может вносить изменения в расследование, установив разрешение на запись для участников на конкретное расследование. По умолчанию у всех участников есть разрешение на запись для расследований, к которым они добавлены, но другие участники на временной шкале могут изменять эти разрешения на «только чтение». См. «Внесение изменений для участников расследования» в разделе «*Использование Splunk Enterprise Security*».

После того, как пользователь создает расследование, любой другой пользователь с возможностью **«Управление всеми расследованиями»** может просмотреть расследование, но только участники данного расследования могут редактировать расследование. Вы не можете просматривать сборники расследований KV Store в качестве справочников. Только пользователи с ролью администратора могут просматривать или изменять сборники KV Store с помощью терминала KV Store API. Подробнее об использовании терминала KV Store API см. в разделе «Описание териналов KV Store в *Справочном руководстве API Splunk Enterprise REST* Splunk Enterprise.

Источники данных для расследований

Splunk Enterprise Security хранит информацию о расследовании в нескольких сборниках KV Store. Существуют отдельные сборники для расследований на странице «Расследования», предметов, добавленных к расследованию, вложений, добавленных к п о расследовании, и артефактов, добавленных к рабочей среде расследования. См. пункт **«Расследования»** в разделе «Таблица требований к панели мониторинга для Splunk Enterprise Security».

Данные расследования из расследований, созданных в версиях, предшествующих версии Splunk Enterprise Security 4.6.0, хранятся в двух сборниках KV Store: investigative\_canvas и investigative\_canvas\_entries. Эти сборники сохранены в версии 4.6.0, но их содержимое добавлено в новые сборники KV Store.

Элементы истории действий в расследовании устранения неполадок

Когда аналитик выбирает тип истории действий для добавления к расследованию, по выбранному временному диапазону выполняется один из пяти запросов.

* Витрины панелей мониторинга – История действий
* Отслеживание поиска – История действий
* Фильтрация по панелям – История действий
* Скрытие заметных действий – История действий
* Статус заметных действий – История действий

Просмотрите результаты поиска, выполнив команду **Configure > Content Management**  и используя фильтры на странице. Если вы измените эти сохраненные поисковые запросы, элементы истории действий могут не отображаться в вашей истории действий. Чтобы исключить поиск из вашей истории действий, используйте «Справочник белых списков отслеживания поиска истории действий». См. раздел «Создание справочников и управление ими в Splunk Enterprise Security».

Администрирование и персональная настройка рабочей среды расследования

Рабочая среда расширяет существующие функции расследования в Splunk Enterprise Security, позволяя аналитикам проводить следственные действия в одном месте. Аналитики исследуют артефакты, т. е. цифровые объекты и идентификаторы, используя панели, вкладки и профили в рабочей среде. Вы можете выполнить персональную настройку рабочей среды, создав панели, вкладки и профили в помощь аналитикам. Вы также можете настроить извлечение артефактов из заметных событий для ускорения расследования, которое начинается с заметного события.

Рабочая среда представляет файл конфигурации es\_investigations.conf, который используется для управления метаданными для панелей, вкладок и профилей. Вы можете внести изменения в файловую систему, добавив станзы в файл es\_investigations.conf. См. подробнее файл es\_\_investigations.conf.spec и es\_ \_investigations.conf.example

Создание панелей и вкладок для рабочей среды расследования

Рабочая среду расследования может отображать любую готовую панель, которая имеет ссылку на рабочую среду и добавлена на вкладку рабочей среды.

Создайте или измените готовую панель. См. пункт «Создание или изменение готовой панели для рабочей среды исследования» в настоящем разделе.

Создайте панель рабочей среды, которая ссылается на готовую панель. См. пункт «Создание вкладки для рабочей среды расследований» в настоящем разделе.

Создайте вкладку рабочей среды, которая содержит панель рабочей среды. См. пункт «Создание вкладки для рабочей среды расследований» в настоящем разделе.

Пример всего указанного процесса см. в пункте «Пример преобразования панели и создания панели рабочей среды» в настоящем разделе.

***Создание или изменение готовой панели для рабочей среды исследования***

Вы можете использовать любую готовую панель в рабочей среде расследования. Вы можете создать ее специально для рабочей среды или изменить существующую панель. Вы можете создать или изменить готовую панель с помощью Splunk Enterprise Security несколькими способами:

* Создайте панель посредством меню Content Management.

В строке меню ES выберите команду **Configure > Content Management .**

Выберите команду **Create New Content > Panel.**

Введите **Prebuilt panel ID.**

Выберите **Destination App.**

Введите **Prebuilt panel XML.**

Нажмите **Save.**

* Преобразуйте панель мониторинга в готовую панель. См. пункт «Преобразование существующей панели в готовую панель» в разделе «*Панели мониторинга и визуализация*».
* Измените панель в меню Settings Splunk.

В строке меню Splunk выберите команду **Settings > User Interface.**

Нажмите **Prebuilt Panels** и выберите команду **Edit > Edit Panel** для панели, которую вы хотите изменить.

При изменении существующей готовой панели рассмотрите возможность ее клонирования до внесения изменений. Если вы клонируете панель, измените ее идентификатор, чтобы вы помнили, какая из панелей относится к рабочей среде.

* Создайте панель в меню Settings Splunk. См. пункт «Добавление панелей на панели мониторинга» в разделе «*Панели мониторинга и визуализация*».

При создании или изменении готовой панели для рабочей среды следуйте этим рекомендациям для наилучшего взаимодействия с приложением:

* Добавьте один или несколько базовых элементов на панель поиска, чтобы ограничить результаты поиска артефактами, расследуемыми в рабочей среде. Используйте несколько базовых элементов для замены более одного типа артефакта. Определите ваш базовый элемент, используя синтаксис $token$. Вы устанавливаете формат базового элемента при создании панели рабочей среды.
* Удалите имя панели в коде XML панели. Если этого не сделать, в рабочей среде отобразятся два заголовка панели. Панели рабочей среды получают название из поля **Label** при создании панели рабочей среды.
* Добавьте функцию просмотра к панели, чтобы аналитики могли добавлять артефакты с панели. Добавьте функцию просмотра, используя синтаксис <option name="drilldown">cell</option> в коде XML панели. Рабочая среда заменяет существующие функции просмотра панели, такие как пользовательские запросы, возможностью добавлять артефакты в область рабочей среды с панели.
* Обновите разрешения на панели, которая будет использоваться совместно со Splunk Enterprise Security. Убедитесь, что для панели установлены свойства **Shared in App** или **Display for: All apps.**
* Если вы сохраняете панель в специальном приложении, убедитесь, что объекты в приложении настроены на экспорт по всему миру. См. раздел «Установка разрешений для объектов в приложении Splunk» на портале разработчиков Splunk.
* Чтобы ваша панель использовала временной диапазон, отличный от установленного в рабочей среде, установите временной диапазон на панели поиска или коде XML панели.

Затем следуйте инструкциям, чтобы создать панель для рабочей среды расследования. См. пункт «Создание панели для рабочей среды расследования» в настоящем разделе.

***Создание панели для рабочей среды расследований***

Создайте панель для рабочей среды.

Выберите команду **Configure > Content Management .**

Выберите команду **Create New Content > Workbench Panel.**

В раскрывающемся списке выберите готовую панель, которую вы хотите использовать в рабочей среде.

(Опционально) Введите **Label**, чтобы заменить заголовок панели рабочей среды по умолчанию.

(Опционально) Введите **Description**, чтобы предоставить информацию о панели.

Добавьте базовый элемент, чтобы заменить базовый элемент в поиске панели. См. пункт «Пример преобразования панели и создания панели рабочей среды» в настоящем разделе или см. пункт «Определение базовых элементов для многозадачного ввода» в *Руководстве по панелям мониторинга и визуализации* Splunk Enterprise.

Нажмите **Save.**

Затем добавьте панель на вкладку, чтобы она была видна в рабочей среде.

***Создание вкладки для рабочей среды расследований***

Создайте вкладку для отображения информации, относящейся к конкретному типу данных, используемому случаю или чему-то еще.

Выберите команду **Configure > Content Management .**

Выберите команду **Create New Content > Workbench Tab.**

Введите **имя вкладки/Tab Name.** Это имя становится частью имени станзы в es\_investigations.conf и используется в качестве ярлыка, если вы не указали ярлык.

(Опционально) Введите **Label**, чтобы указать имя для пользователя для вкладки рабочей среды.

В меню **Workbench Panels** выберите панели, которые вы хотите отобразить на этой вкладке. Порядок, в котором вы выбираете панели, – это порядок, в котором они отображаются на этой вкладке рабочей среды.

(Опционально) Выберите профиль рабочей среды, с которым будет связана эта вкладка. Вы можете связать одну вкладку только с одним профилем. Профили позволяют аналитикам загружать несколько вкладок, которые относятся к сценарию использования в рабочей среде.

(Опционально) Измените выбор **Load by default.** Выберите **True,** если вы хотите, чтобы эта вкладка загружалась для всех расследований рабочей среды.

(Опционально) Введите **Description** для вкладки. Это помогает аналитикам определять, какие типы информации и контекста они могут собирать, используя панели на вкладке.

Нажмите **Save.**

Пример преобразования панели и создания панели рабочей среды

**Необходимые условия**

Необходимо установить надстройку Splunk для Blue Coat ProxySG и данные из надстройки в ваше развертывание Splunk Enterprise Security. Вы можете загрузить надстройку Splunk для Blue Coat ProxySG из Splunkbase.

Клонируйте панель и изменить поиск, чтобы использовать базовый элемент ввода в рабочей среде.

Выберите команду **Settings > User Interface.**

Нажмите **Prebuilt panels.**

Выберите команду **Edit > Clone** для actions\_by\_destination\_ip для Splunk\_TA\_bluecoat-ProxySG.

Введите идентификатор готовой панели. workbench\_actions\_by\_dest\_ip.

Удалите заголовок из кода XML, если только вы не хотите, чтобы в рабочей среде отображались два заголовка.

Измените запрос в коде XML, чтобы он включал базовый элемент, который ограничивает результаты расследуемыми артефактами цифровых объектов. sourcetype="bluecoat:proxysg:access\*" $dest\_token$ | iplocation dest | geostats count by action

Решите, следует ли удалить временной диапазон <earliest> и <latest> для панели. Этот временной диапазон имеет приоритет над временным диапазоном, установленным в рабочей среде, поэтому вы, вероятно, захотите его удалить, чтобы аналитики могли выполнять чувствительные к контексту поисковые запросы.

Нажмите **Save.**

Измените разрешения панели.

1. Найдите панель, которую вы только что создали, workbench\_actions\_by\_dest\_ip.
2. Выберите команду **Edit > Edit Permissions.**
3. Для параметра **Display for** выберите **All apps.**
4. Нажмите **Save.**

Вернитесь к Splunk Enterprise Security и настройте панель, которая будет использоваться в рабочей среде.

Выберите команду **Configure > Content Management.**

Выберите команду **Create New Content > Workbench Panel.**

Выберите **Panel Name** **workbench\_actions\_by\_dest\_ip.**

(Опционально) Введите **Label** для пользователя, который появляется в рабочей среде: **Proxy Actions by Destination.**

(Опционально) Введите описание для пользователя, отображаемое в рабочей среде: **отображает карту, которая, по возможности, отображает действия по IP-адресу назначения для конкретных расследуемых цифровых объектов.**

Нажмите **Add a Token,** чтобы добавить базовый элемент для **$dest\_token$** из поиска.

Введите **Token Name,** соответствующее базовому элементу.

**dest\_token**

Введите **Prefix (.**

Введите **Suffix ).**

Введите **Value Prefix dest = ".**

Введите **Value Suffix ".**

Снимите флажок **Is Null** для **Delimiter** и введите OR в текстовое поле. Поставьте пробелы перед и после OR.

Оставьте флажок **Is Null** для поля **Default.** Если этот флажок установлен, поиск выполняется только тогда, когда в рабочей среде выбран артефакт соответствующего типа. В этом случае поиск выполняется только в том случае, если вы изучаете цифровые объекты в рабочей среде.

Выберите **Type Artefact.**

Выберите **Field Type /Asset,** поскольку назначение – это цифровой объект, а не идентификатор.

Нажмите **Save.**

Эта панель теперь содержит поиск, который будет построен следующим образом для двух объектов, расследуемых в рабочей среде:

sourcetype="bluecoat:proxysg:access\*" (dest="<investigated\_asset\_1>" OR

dest="<investigated\_asset\_2>") | iplocation dest | geostats count by action

Добавьте новую панель на новую вкладку.

1. В меню «Управление контентом» выберите команду **Create New Content > Workbench Tab.**
2. Введите **Tab Name proxy\_data.** Это имя становится именем станзы в файле es\_investigations.conf и используется в качестве ярлыка, если ярлык не указан.
3. (Опционально) Введите **Proxy Data** в поле **Label.**
4. В меню **Workbench Panels** введите и выберите панель **Proxy Actions by Destination IP.**
5. Для поля **Load by default** оставьте флажок **False**. Выберите True, если хотите, чтобы эта вкладка загружалась для всех расследований в рабочей среде.
6. (Опционально) Введите **описание/Description** для вкладки. **Данные прокси, связанные с расследуемыми цифровыми объектами и идентификаторами.**
7. Нажмите **Save.**

Затем аналитики могут открыть рабочую среду и добавить новую вкладку, чтобы начать расследование данных прокси в рабочей среде.

Создание профиля рабочей среды

Вы можете использовать профили рабочей среды, чтобы связать несколько вкладок, которые соответствуют конкретному сценарию использования. Например, профиль расследования DDoS может включать вкладку данных брандмауэра и вкладку общих сетевых данных. Затем аналитик может добавить профиль расследования DDoS к расследованию, чтобы добавить обе эти вкладки в рабочую среду, вместо того, чтобы добавлять вкладки, соответствующие расследованию, по отдельности.

1. Выберите команду **Configure > Content Management .**
2. Выберите команду **Create New Content > Workbench Profile.**
3. Введите **Profile Name.** Это имя становится именем станзы в файле es\_investigations.conf и используется как ярлык, если ярлык не указан.
4. (Опционально) Введите **Label**, чтобы предоставить ярлык для пользователя для рабочей среды.
5. (Опционально) Введите **Description** для профиля. Это помогает аналитикам определить, какие типы информации и контекста они могут собрать, добавив профиль в свое расследование.
6. Нажмите **Save.**

После создания профиля обновите вкладки с созданным профилем. Для примера расследования DDoS отредактируйте вкладки данных брандмауэра и сетевых данных и выберите новый профиль расследования DDoS.

Установка извлечения артефактов для заметных событий

При добавлении заметного события к расследованию вы можете определить поля, которые автоматически извлекаются как идентификаторы или цифровые объекты в рабочей среде, для каждого поиска корреляций со связанным заметным событием. По умолчанию поля, которые используются для корреляции цифровых объектов и идентификаторов, – это те же поля, которые извлекаются из заметных событий, созданных включенными поисками корреляций. Вы должны добавить поля, которые нужно извлечь для любых пользовательских поисков корреляций.

|  |  |
| --- | --- |
| **Тип артефакта расследования** | **Поля, извлекаемые для расследования** |
| Цифровой объект | dest, src, dvc, orig\_host |
| Идентификатор | user, src\_user |

Если ваш поиск корреляций не использует модели данных или результаты поиска содержат разные поля, которые вы хотите извлечь, вы можете указать поля для извлечения в область расследования.

1. Выберите команду **Configure > Content Management .**
2. Выберите поиск корреляций, который вы хотите настроить, чтобы открыть его для редактирования.
3. Выберите адаптивное ответное действие на заметное событие.
4. В поле **Asset Extraction** введите имя поля из результатов поиска корреляций, которое определяет Цифровой объект. Нажмите Enter, чтобы добавить имя поля.
5. В поле **Identity Extraction** введите имя поля из результатов поиска корреляций, которое определяет идентификатор. Нажмите Enter, чтобы добавить имя поля.
6. Нажмите **Save.**

Управление статусами расследования и их персональная настройка в Splunk Enterprise Security

Начиная с версии 5.0.0, вы можете добавлять статусы к расследованиям. После обновления до этой версии расследованиям, которые не имели статуса, присваивается статус **New.**

Чтобы изменить статус расследования, аналитик должен иметь возможность transition\_reviewstatus- <x> \_to\_ <y> nt для статусов, между которым он желает осуществить переход. Роль ess\_analyst и роль ess\_admin обладают этой возможностью для всех статусов по умолчанию. Изменение переходов статуса для расследований изменяет эти возможности.

Чтобы внести изменения в статусы в качестве аналитика, вы должны иметь возможность edit\_reviewstatuses. Роль ess\_admin обладает этой возможностью по умолчанию. См. раздел «Настройка пользователей и ролей» в *Руководстве по установке и обновлению*.

Создание статуса расследования

Создайте статус, который аналитики могут выбрать при проведении расследования.

Если вы ограничиваете переходы статуса, обновите переходы статуса после создания статуса, иначе аналитики не смогут выбрать новый статус. См. пункт «Ограничение переходов статуса для расследований» в настоящем разделе.

На панели инструментов Enterprise Security выберите команду **Configure > Incident Management > Status Configuration.**

(Опционально) Перейдите на вкладку **Investigation**, чтобы просмотреть существующие статусы расследования.

Выберите команду **Create New Status > Investigation.**

Введите **ярлык/Label**, который будет отображаться как имя статуса при расследовании. Например, «Ожидание отдела настольных ИТ».

(Опционально) Введите **описание/Description**, которое отображается на странице Status Configuration для описания статуса.

Например, «Расследование ожидает проведения отделом настольных ИТ дополнительных корректирующих действий или аналитических шагов».

(Опционально) Установите флажок **Default Status,** чтобы установить этот статус как статус по умолчанию для вновь созданных расследований.

(Опционально) Установите флажок **End Status,** чтобы установить этот статус как возможный последний статус для расследования.

(Опционально) Снимите флажок **Enabled,** чтобы создать статус, не позволяя кому-либо использовать его.

Обновите роли пользователей, которые могут изменить этот новый статус расследования, например, «Ожидание отдела настольных ИТ» в другой статус, такой как **Closed.** Если вы не выбираете роли, которые могут перейти от этого статуса к другому, никто не сможет переместить расследование в другой статус после перехода расследования на этот статус.

Нажмите **Save.**

Ограничение переходов статуса для расследований

Переходы статусов, которые могут быть сделаны в отношении расследования, определяют путь исследования. По умолчанию любой статус расследование может быть изменен на любой другой статус. Например, кто-то может изменить статус расследования **New** на любой другой статус, например **Closed.**

Вы можете ограничить статусы, которые аналитики могут выбрать при расследовании. Определите, какие статусы потребуются, и должны ли аналитики следовать определенной последовательности статусов для завершения расследования. Определите, могут ли какие-либо роли обойти полную последовательность статусов.

В этом примере показано ограничение переходов статуса для аналитиков. Ограничьте переходы статусов, чтобы аналитики должны были следовать от New, к In Progress или Pending, к Resolved и затем Closed.

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **2** | **3** | **4** |
| New | In Progress  Pending | Resolved | Closed |

**Необходимые условия**

* У вас должна быть роль **ess\_admin,** или вашей роли должна быть назначена возможность **«Редактировать статусы».** Дополнительные сведения о ролях и возможностях пользователей см. в разделе «Настройка пользователей и ролей» в *Руководстве по установке и обновлению*.

1. На панели инструментов Splunk Enterprise Security выберите команду **Configure > Incident Management > Status Configuration.**
2. Выберите вкладку **Investigation.**
3. Ограничьте переходы из статуса **New.** Выберите статус **New,** чтобы открыть страницу «Изменить статус расследования».
4. В разделе **Status Transitions** выберите роли для статуса **Resolved** и снимите флажок для роли ess\_analyst.
5. Выберите роли для статуса **Closed** и снимите флажок для роли ess\_analyst.
6. Нажмите **Save,** чтобы сохранить изменения в статусе **New.**
7. Ограничьте переходы в статусах **In Progress** и **Pending,** чтобы предотвратить возможность изменения на статус **New** или **Closed** для роли ess\_analyst.
8. Выберите вкладку **Investigation** и выберите статус **In Progress.**
9. В разделе **Status Transitions** выберите роли для статуса **New** и снимите флажок для роли ess\_analyst. Повторите для статуса **Closed.**
10. Нажмите **Save,** чтобы сохранить изменения в статусе **In Progress.** Повторите указанные действия для статуса **Pending.**
11. Ограничьте статус **Resolved.** Перейдите на вкладку **Investigation** и выберите статус **Resolved.**
12. В разделе **Status Transitions** выберите роли для статуса **New** и снимите флажок для роли ess\_analyst. Повторите для статусов **In Progress** и **Pending.**
13. Нажмите **Save,** чтобы сохранить изменения в статусе **Resolved.**
14. Ограничьте переходы для статуса **Closed.** Перейдите на вкладку **Investigation** и выберите статус **Closed.**
15. В разделе **Status Transitions** выберите роли для статуса **New** и снимите флажок для роли ess\_analyst. Повторите для статусов **In Progress,** **Pending** и **Resolved.**
16. Нажмите **Save,** чтобы сохранить изменения для статуса **Closed.**

Поиски корреляций

Обзор поиска корреляций Splunk Enterprise Security

**Поиск корреляций** сканирует несколько источников данных на наличие определённого шаблона. Когда поиск находит шаблон, он выполняет **адаптивное ответное действие**.

Поиски корреляций могут искать многие типы источников данных, в том числе события из любого домена безопасности (доступ, идентификатор, конечная точка, сеть), списки устройств, списки идентификационных данных, сведения об угрозах и другие данные на платформе Splunk. Затем поиски группируют результаты начального поиска с функциями в SPL и действуют в ответ на события, которые сопоставляют условия поиска с адаптивным ответным действием.

* Чтобы создать поиск корреляций, см. «Создание поиска корреляций» в Руководстве Splunk Enterprise Security.
* Чтобы настроить или изменить поиски корреляций в вашей среде, см. [«Настройка поисков корреляций»](#bookmark6).

Примеры поисков корреляций

* Обнаружение попытки доступа из учётной записи с истёкшим сроком действия с помощью корреляции списка идентификаторов и попытки аутентификации на хосте или устройстве.
* Обнаружение большого числа хостов, зараженных конкретной вредоносной программой, или одного хоста с большим количеством вредоносных программ с помощью корреляции списка устройств с событиями из системы защиты конечных точек.
* Обнаружение шаблона с большим количеством ошибок аутентификации на одном хосте и последующей успешной аутентификацией с помощью корреляции списка профилей и попыток аутентификации на хосте или устройстве. Затем применение порогового значения в поиске, чтобы подсчитать количество попыток аутентификации.

Создание поисков корреляций в Splunk Enterprise Security

Вы можете создавать собственные поиски корреляций, чтобы создавать заметные события, изменять шкалы риска и выполнять другие адаптивные ответные действия, автоматически основанные на корреляции в событиях. Существует два способа создания поисков корреляций в Splunk Enterprise Security.

* Создайте поиск корреляции вручную, если вы хорошо владеете SPL. Вы можете просмотреть встроенные поиски корреляций для примера методологии поиска и доступных опций. Протестируйте свои идеи поиска корреляций на странице **Search** (**Поиска)** до их реализации.
* Для получения дополнительной помощи с синтаксисом поисков корреляций используйте пошаговый мастер создания поиска. Пошаговый мастер создания поиска позволяет вам создавать поиск корреляций, который использует модели данных или справочники в качестве источника данных. Мастер принимает ваши решения об источнике данных, временном диапазоне, фильтрации, агрегатных функциях, полях разделения и других условиях и строит синтаксис поиска для вас. См. «Создание поиска корреляций» в *Руководстве Splunk Enterprise Security* для пошагового руководства по созданию корреляционного поиска.

Более подробно о том, как убедиться, что дополнительные поля появляются в сведениях о заметных событиях для пользовательского поиска корреляций см. «Изменение полей заметных событий».

Смотрите также

* [Настройка поисков корреляций в Splunk Enterprise Security](#bookmark6)
* [Список поисков корреляций в Splunk Enterprise Security](#bookmark14)

Настройка поисков корреляций в Splunk Enterprise Security

Настройте поиски корреляций, чтобы включить или отключить их, обновить настройки, связанные с их запуском, изменить поисковую логику и активировать их результирующие адаптивные ответные действия. См. [Обзор поиска корреляций Splunk Enterprise Security](#bookmark1), чтобы узнать больше о [**поиске корреляций**](#bookmark1).

Включение поисков корреляций

Включите поиски корреляций, чтобы начать выполнение адаптивных ответных действий и получать заметные события. Splunk Enterprise Security устанавливается с выключенными поисками корреляций, поэтому вы можете выбрать поиски, наиболее подходящие для ваших вариантов использования безопасности.

1. В строке меню Splunk ES выберите **Configure > Content Management**.
2. Отфильтруйте страницу Content Management по типу Type поиска корреляций Correlation Search, чтобы видеть только поиски корреляций.
3. Просмотрите имена и описания поисков корреляций, чтобы определить, которые из них включить для поддержки ваших вариантов использования безопасности. Например, если скомпрометированные учётные записи являются проблемой, рассмотрите возможность включения поисков корреляций Concurrent Login Attempts Detected и Brute Force Access Behavior Detected.
4. В столбце Actions нажмите Enable, чтобы включить нужные вам поиски.

После включения поисков корреляции панели мониторинга начинают отображать важные события, шкалы риска и другие данные.

Изменение расписания поиска корреляций

Измените тип поиска корреляций по умолчанию с работающего в режиме реального времени на запланированный. Splunk Enterprise Security по умолчанию использует индексированные поиски в режиме реального времени.

1. На странице Content Management найдите поиск корреляций, который вы хотите изменить.
2. В столбце Actions нажмите Change to scheduled.

После изменения поиска на запланированный вы можете изменять настройки расписания поиска.

1. На странице Content Management нажмите имя поиска корреляций, который вы хотите изменить.
2. (Опционально) Измените расписание поиска.

Поиски корреляций могут выполняться в режиме реального времени или в непрерывном режиме. Используйте расписание в режиме реального времени, чтобы назначить приоритет текущим данным и производительности. Поиски по расписанию в режиме реального времени пропускаются, если поиск не может быть запущен в запланированное время. Поиски по расписанию в режиме реального времени не заполняют пропуски в данных, которые появляются, если поиск был пропущен. Используйте непрерывный режим, чтобы установить приоритет заполнения данных, так как поиски по непрерывному расписанию никогда не пропускаются.

1. (Опционально) Измените расписание cron, чтобы контролировать частоту запусков поиска.
2. (Опционально) Настройте окно расписания для поиска. Введите 0, чтобы не использовать окно расписания, введите auto, чтобы использовать автоматическое окно расписания, заданное планировщиком, или введите число минут, в течение которых вы хотите, чтобы окно существовало.

Если запуск большого числа запланированных отчётов установлен на одно и тоже время, настройте окно расписания, чтобы позволить планировщику поиска отложить выполнение этого поиска в пользу более приоритетных.

1. (Опционально) Настройте приоритет расписания для поиска. Измените значение по умолчанию на Higher или Highest, в зависимости от того, насколько важно, чтобы этот поиск выполнялся, и чтобы он выполняется в определенное время.

Установка приоритета расписания переопределяет настройку окна расписания, поэтому вам не нужно устанавливать оба параметра.

Информацию о приоритете расписания поиска см. в документации к платформе Splunk.

* Для Splunk Enterprise см. «Назначение приоритетности одновременно запланированным отчетам в Splunk Web» в Руководстве по отчётам Splunk Enterprise.
* Для Splunk Cloud см. «Назначение приоритетности одновременно запланированным отчетам в Splunk Web» в Руководстве по отчётам Splunk Cloud.

Редактирование поиска корреляций

Вы можете вносить изменения в поиски корреляций в соответствии с вашей средой. Например, измените пороговые значения в поиске, измените ответные действия, являющиеся результатом успешной корреляции, или измените частоту запусков поиска. Изменение поиска корреляций не влияет на существующие заметные события.

1. На странице Content Management найдите поиск корреляций, который вы хотите редактировать.
2. Нажмите на имя поиска корреляций на странице Content Management, чтобы редактировать его.
3. Измените параметры поиска, затем нажмите Save.

Если вы изменяете время начала и окончания поиска корреляций, используйте relative time modifiers. См. «Настройка модификаторов времени в вашем поиске» в Руководстве по поиску Splunk Enterprise.

*Редактирование поиска корреляций в пошаговом режиме*

Вы можете редактировать поиск корреляций в пошаговом режиме. Не все поиски корреляций поддерживают пошаговое редактирование поиска. Если поиск отображается серым цветом и имеет опцию Edit search in guided mode, то поиск был построен в пошаговом режиме и может быть отредактирован в пошаговом режиме. Если поиск можно редактировать в окне поиска, то вы не можете редактировать его в пошаговом режиме. При попытке переключиться на пошаговый режим новый поиск переписывает существующий.

1. Нажмите **Edit search in guided mode**, чтобы открыть пошаговый мастер создания поиска.
2. Просмотрите элементы поиска в поиске корреляций, при необходимости внося изменения.
3. Сохраните поиск.

Регулируйте количество ответных действий, генерируемых поиском корреляций.

Настройте регулировку, чтобы ограничить количество ответных действий, генерируемых поиском корреляций. Когда поиск корреляций соответствует событию, это вызывает ответное действие.

По умолчанию, каждый результат, возвращаемый поиском корреляции, генерирует ответное действие. Как правило, вам может понадобиться только одно оповещение определенного типа. Вы можете использовать регулировку количества ответных действий, чтобы предотвратить поиск корреляций от создания более одного оповещения в течение установленного периода. Чтобы изменить типы результатов, которые генерируют ответное действие, определите условия срабатывания. Некоторые ответные действия позволяют вам настроить максимальное число результатов в дополнение к регулировке количества ответных действий. См. [Настройка адаптивных ответных действий в Splunk Enterprise Security](#bookmark17).

1. Выберите **Configure > Content Management.**
2. Нажмите на заголовок поиска корреляций, который вы хотите редактировать.
3. Введите **Window duration**. В течение существования этого окна любое дополнительное событие, которое соответствует любому из **Fields to group by**, не будет создавать новое оповещение. После конца существования окна следующее соответствующее событие создаст новое оповещение и применит условия регулировки количества ответных действий снова.
4. Введите **Fields to group by**, чтобы указать, какие поля использовать при сопоставлении похожих событий. Если поле из этого списка совпадает со сгенерированным оповещением, поиск корреляции не создаст новое оповещение. Вы можете определить несколько полей. Доступные поля зависят от полей поиска, которые поиск корреляций возвращает.
5. Сохраните поиск корреляций.

Регулировка количества ответных действий применяется к любому типу ответного действия поиска корреляций и происходит до подавления заметного события. См. «Создание и управление подавлением заметных событий» для получения дополнительной информации о подавлении заметных событий.

Определение условий срабатывания для адаптивных ответных действий, генерируемых поиском корреляций

Вы можете изменять условия, которые определяют, когда адаптивное ответное действие генерируется поиском корреляций. Регулировка количества ответных действий отличается от определения условий срабатывания и происходит после того, как результаты поиска удовлетворяют условиям срабатывания. Когда вы определяете условия срабатывания, результаты поиска корреляций оцениваются для проверки на соответствие этим условиям. Если результаты поиска соответствуют этим условиям, правила регулировки количества ответных действий определяют, будет ли сгенерировано ответное адаптивное действие.

Вы можете установить условия срабатывания, чтобы генерировать ответные действия за каждый результат на основе количества результатов, возвращаемых поиском корреляций, в зависимости от количества хостов, количества источников или на основе пользовательских критериев. Для пользовательских критериев введите пользовательскую строку поиска, чтобы создать условие. Условия срабатывания действуют как вторичный поиск по результатам поиска корреляций.

Информацию об условиях срабатывания и настройке этих условий см. в документации к платформе Splunk.

* Для Splunk Enterprise см. «Настройка условий срабатывания оповещений» в *Руководстве по оповещениям* Splunk Enterprise.
* Для Splunk Cloud см. «Настройка условий срабатывания оповещений» в *Руководстве по оповещениям* Splunk Cloud.

Смотрите также

* [Список поисков корреляций в Splunk Enterprise Security](#bookmark14)
* [Настройка адаптивных ответных действий в Splunk Enterprise Security](#bookmark17)

Список поисков корреляций в Splunk Enterprise Security

Чтобы получить список поисков корреляций, включенных в Splunk Enterprise Security, используйте поиск REST для извлечения информации, которая нужна вам в таблице.

Например, создайте таблицу с приложением, доменом безопасности, именем и описанием всех поисков корреляции в вашей среде.

| rest splunk\_server=local count=0 /services/saved/searches | where match('action.correlationsearch.enabled' , "1|[Tt]![Tt][Rr][Uu][Ee]")|

rename eai:acl.app as app, title as csearch\_name,

action.correlationsearch.label as csearch\_label,

action.notable.param.security\_domain as security\_domain | table

csearch\_name, csearch\_label, app, security\_domain, description

В качестве другого примера создайте таблицу только с включенными поисками корреляций и адаптивными ответными действиями, связанными с этими поисками в вашей среде. Чтобы увидеть адаптивные ответные действия для всех поисков корреляций,

удалите | where disabled=0.

| rest splunk\_server=local count=0

/servicesNS/-/SplunkEnterprrseSecuritySuite/saved/searches | where match('action.correlatronsearch.enabled', "1|[Tt]|[Tt][Rr][Uu][Ee]") |

where disabled=0 | eval actions=split(actions, ",") | table

trtle,actions

Обновление поисков корреляций в Splunk Enterprise Security

Начиная с версии Splunk Enterprise Security версии 4.6.0, correlatronsearches.conf больше не используется для определения поисков корреляций. Вместо этого, savedsearches.conf уникально идентифицирует поиски корреляций, используя параметр action.correlatronsearch.enabled=l. Файл correlatronsearches.conf устарел.

*Изменения Splunk Enterprise Security при обновлении*

При обновлении до Splunk Enterprise Security 4.6.0, Splunk Enterprise Security осуществляет миграцию всех поисков корреляций в вашей среде из correlatronsearches.conf в savedsearches.conf, используя скрипт confcheck\_es\_correlatronmrgratron.py. Миграция после обновления может занять до пяти минут. В кластере Search Head миграцию выполняет Captain.

Во время обновления Splunk Enterprise Security продолжает создавать заметные события без перерывов. Это изменение не предотвращает и не задерживает появление заметных событий в Обзоре событий, так как сохраненный поиск Threat - CorrelationSearches - Lookup Gen продолжает использовать содержимое обоих correlatronsearches.conf и savedsearches.conf для заполнения хранилища данных correlatronsearches KV Store, используемого в Обзоре событий.

*Изменения, которые вы должны сделать после обновления*

После обновления до Splunk Enterprise Security 4.6.0 или более поздней версии вам необходимо внести дополнительные изменения.

* Проверьте correlationsearches.conf на наличие определений поиска, которые бы указывали на то, что миграция поиска не прошла успешно. Поиски, прошедшие миграцию, существуют только в savedsearches.conf. Если поиск не мигрировал, перенесите

записи из correlationsearches.conf вручную в savedsearches.conf, используя определения параметров ниже.

* Обновите поиски, которые вызывают конечную точку correlationsearches REST.
* Например, поиск, который отображает список поисков корреляций в вашей среде, изменится с:

| rest splunk\_server=local

/services/alerts/correlat.ionsearches | rename eai:acl.app

as app, title as csearch\_name | table app security\_domain

csearch\_name description

на:

| rest splunk\_server=local count=0 /services/saved/searches

| where match('action.correlationsearch.enabled',

"1|[Tt]|[Tt][Rr][Uu][Ee]") | rename eai:acl.app as app,

title as csearch\_name, action.correlationsearch.label as csearch\_label, action.notable.param.security\_domain as

security\_domain | table csearch\_name, csearch\_label, app, security\_domain, description

* Больше примеров обновленных поисков см. в [«Список поисков корреляций в Splunk Enterprise Security»](#bookmark14).

Макросы пользовательского поиска, которые ссылаются на коллекцию correlationsearches KV Store продолжат работать как и раньше, но все равно подумайте о том, чтобы обновить их.

*Перевод параметров* *correlationsearches.conf* *в* *savedsearches.conf*

Все параметры correlationsearches.conf теперь находятся в savedsearches.conf, а файл correlationsearches.conf устарел. Не обновляйте их напрямую, за исключением переноса определений поиска корреляций вручную.

**Идентификационные параметры для поисков корреляций**

Новые параметры определяют, является ли сохраненный поиск корреляционным, а также имя поиска корреляций.

|  |  |  |
| --- | --- | --- |
| correlationsearches.conf | savedsearches.conf **параметр**  **начиная с версии 4.6.0** |  |
| **параметр**  **в версиях до 4.6.0** | **Примечания** |
| Н/П | action.correlationsearch=0 | Это внутренний параметр, и его можно игнорировать. |
| Раздел конфигурационного файла (станза) для поиска | action.correlationsearch.enabled=l | Этот параметр идентифицирует сохраненный поиск как поиск корреляции. |
| rule\_name | action.correlationsearch.label | Этот параметр содержит имя поиска корреляции. |
| description | description | Этот параметр содержит описание поиска корреляции. |

**Параметры заметных событий для поисков корреляций**

Параметр action.notable определяет заметное событие, связанное с поиском корреляции. Параметры, описывающие дополнительные сведения, связанные с заметным событием, теперь находятся в файле savedsearches.conf.

|  |  |
| --- | --- |
| correlationsearches.conf  **параметр**  **в версиях до 4.6.0** | **savedsearches.conf** параметр  **начиная с версии 4.6.0** |
| security\_domain | action.notable.param.security\_domain |
| severity | action.notable.param.severity |
| rule\_title | action.notable.param.rule\_title |
| rule\_description | action.notable.param.rule\_description |
| nes\_fields | action.notable.param.nes\_fields |
| drilldown\_name | action.notable.param.drilldown\_name |
| drilldown\_search | action.notable.param.drilldown\_search |
| default\_status | action.notable.param.default\_status |
| default\_owner | action.notable.param.default\_owner |

**Связанные параметры поиска для поисков корреляций**

Поиски, относящиеся к поиску корреляций, такие как контекстно-генерирующие поиски, связанные с поиском корреляций, который использует экстремальный поиск, теперь являются частью параметра JSON blob action.correlationsearch.related\_searches.

|  |  |
| --- | --- |
| correlationsearches.conf  **параметр**  **в версиях до 4.6.0** | **savedsearches.conf** параметр  **начиная с версии 4.6.0** |
| related\_search\_name =  Endpoint - Emails By Source - Context Gen  related\_search\_name.0 =  Endpoint - Emails By  Destination Count - Context  Gen | action.correlationsearch.related\_searches  = [\  "Endpoint - Emails By Source - Context Gen",\  "Endpoint - Emails By Destination Count - Context Gen"\  ] |

***Примеры разделов конфигурационного файла поиска корреляций из этой версии и предыдущих версий***

Раздел конфигурационного файла для поиска корреляций savedsearches.conf начиная с версии 4.6.0 выглядит следующим образом.

[Access - Concurrent App Accesses - Rule]

action.correlationsearch = 0

action.correlationsearch.enabled = 1

action.correlationsearch.label = Concurrent Login Attempts Detected action.email.sendresults = 0

action.notable = 0

action.notable.param.security\_domain = access

action.notable.param.severity = medium

action.notable.param.rule\_title = Concurrent Access Event Detected For $user$

action.notable.param.rule\_description = Concurrent access attempts to $appl$ by $user$ from two different sources( $srcl$, $src2$ ) have been detected.

action.notable.param.nes\_fields = user

action.notable.param.drilldown\_name = View access attemps by $user$ action.notable.param.drilldown\_search = | datamodel Authentication

Authentication search | search Authentication.user="$user$"

action.risk = 1

action.risk.param,\_risk\_ob]ect = user

action.risk.param.\_risk\_object\_type = user

action.risk.param,\_risk\_score = 20

alert.suppress = 1

alert.suppress.fields = user

alert.suppress.period = 86300s

alert.track = false

cron\_schedule = 10 \* \* \* \*

description = Alerts on concurrent access attempts to an app from different hosts. These are good indicators of shared passwords and potential misuse.

disabled = True

dispatch.earliest\_time = -70m@m

dispatch.latest\_time = -5m@m

enableSched = 1

is\_visible = false

request.ui\_dispatch\_app = SplunkEnterpriseSecuritySuite

search = | tstats 'summariesonly' count from

datamodel=Authentication.Authentication by

\_time,Authentication.app,Authentication.src,Authentication.user span=ls

|'drop\_dm\_ob]ect\_name("Authentication")' | eventstats dc(src) as

src\_count by app,user | search src\_count>l | sort 0 + \_time |

streamstats current=t wmdow=2 earliest(\_time) as

previous\_time,earliest(src) as previous\_src by app,user | where

(src!=previous\_src) | eval time\_diff=abs(\_time-previous\_time) | where time\_diff<300

В предыдущих версиях Splunk Enterprise Security определения savedsearches.conf и correlationsearches.conf для одного и того же поиска корреляций выглядели следующим образом.

savedsearches.conf

|  |  |
| --- | --- |
| [Access - Concurrent App Accesses - Rule] | |
| action.email.sendresults action.risk action.risk.param.\_risk\_object action.risk.param.\_risk\_object\_type action.risk.param.\_risk\_score alert.suppress alert.suppress.fields alert.suppress.period alert.track cron\_schedule disabled dispatch.earliest\_time dispatch.latest\_time enableSched is\_visible request.ui\_dispatch\_app search | = 0 = 1 = user = user = 20 = 1 = user = 86300s = false = 10 \* \* \* \* = True = -70m@m = -5m@m = 1 = false = SplunkEnterpriseSecuritySuite = | tstats 'summariesonly' count |

from datamodel=Authentication.Authentication by

\_time,Authentication.app,Authentication.src,Authentication.user span=ls

| 'drop\_dm\_object\_name("Authentication")' | eventstats dc(src) as

src\_count by app,user | search src\_count>l | sort 0 + \_time |

streamstats current=t window=2 earliest(\_time) as

previous\_time,earliest(src) as previous\_src by app,user | where

(src!=previous\_src) | eval time\_diff=abs(\_time-previous\_time) | where

time\_diff<300

correlationsearches.conf

|  |  |
| --- | --- |
| [Access - Concurrent App Accesses - Rule] | |
| security\_domain severity rule\_name description   rule\_title rule\_description  nes\_fields drilldown\_name drilldown\_search  default\_owner default\_status | = access = medium = Concurrent Login Attempts Detected = Alerts on concurrent access attempts to an app from different hosts. These are good indicators of shared passwords and potential misuse. = Concurrent Access Event Detected For $user$ = Concurrent access attempts to $app1$ by $user$ from two different sources( $src1$, $src2$ ) have been detected. = user = View access attemps by $user$ = | datamodel Authentication Authentication search | search Authentication.user="$user$"  =  = |

Настройка адаптивных ответных действий в Splunk Enterprise Security

**Адаптивные ответные действия** позволяют собирать информацию или предпринимать другие действия в ответ на результаты поиска корреляций или детали заметного события. Splunk Enterprise Security включает несколько адаптивных ответных действий. См. раздел

Включённые адаптивные ответные действия.

Вы можете добавлять адаптивные ответные действия и действия оповещений в поиски корреляций или выполнять адаптивные ответные действия из заметных событий на Панели обзора событий. Собирайте информацию, прежде чем начать исследование, чтобы сэкономить время на сортировке, добавив адаптивные ответные действия в поиски корреляций. Во время сортировки запускайте адаптивные ответные действия из Панели обзора событий.

Добавление новых адаптивных ответных действий

Для добавления новых адаптивных ответных действий, вы можете установить надстройки с адаптивными ответными действиями или создавать свои собственные адаптивные ответные действия. См. «Создание адаптивных ответных действий» на портале разработчиков Splunk для получения информации о создании адаптивных ответных действий. См. раздел «Развертывание надстроек, включенных в Splunk Enterprise Security» в *Руководстве по установке и обновлению*.

Аудит адаптивных ответных действий

Проводите аудит адаптивных ответных действий в Центре управления адаптивными ответами.

Настройка разрешений для адаптивных ответных действий

Ограничьте определенные адаптивные ответные действия до определенных ролей, настроив разрешения для адаптивных ответных действий в диспетчере оповещений. Информацию о диспетчере оповещений можно найти в документации платформы Splunk.

* Для Splunk Enterprise см. «Использование диспетчера оповещений» в *Руководстве по оповещеням* Splunk Enterprise.
* Для Splunk Cloud см. «Использование диспетчера оповещений» в *Руководстве по оповещениям* Splunk Cloud.

Чтобы выполнить адаптивные ответные действия из Панели обзора событий, учетные данные которой хранятся в диспетчере учетных данных, вы должны иметь соответствующую возможность.

* Для платформы Splunk версии 6.5.0 и более поздних: list\_storage\_passwords.
* Для более ранних версий платформы Splunk: admin\_all\_objects.

Добавление адаптивного ответного действия в поиск корреляций

1. В строке меню Splunk Enterprise Security нажмите Configure > Content Management.
2. Выберите существующий поиск корреляций или нажмите Create New > Correlation Search.
3. Нажмите Add New Response Action и выберите ответное действие, которое вы хотите добавить.
4. Заполните поля для действия. Если вы хотите, добавьте другое ответное действие.
5. Нажмите Save, чтобы сохранить все изменения поиска корреляций.

Инструкции по настройке каждого из адаптивных ответных действий, включенных в [[Splunk Enterprise Security, см. в разделе «Настройка адаптивных ответных действий для поиска корреляций в Splunk Enterprise Security».](#bookmark24)](#bookmark24) Инструкции по настройке пользовательского адаптивного ответного действия см. в документации для приложения или надстройки, которые предоставили адаптивные ответные действия.

Устранение неполадок, из-за которых недоступен выбор адаптивного ответного действия

Невозможность выбора адаптивного ответного действия в редакторе поиска корреляций или Обзоре событий может быть вызвана несколькими причинами.

* У вас может не быть разрешений на просмотр или использование адаптивного ответного действия. См. «Использование диспетчера оповещений» в *Руководстве по оповещениям*.
* Проверьте диспетчер оповещений, чтобы определить, существуют ли адаптивные ответные действия на платформе Splunk. См. «Использование диспетчера оповещений» в *Руководстве по оповещениям*.
* Если адаптивные ответные действия из надстройки не отображаются в Splunk Enterprise Security, но отображаются в диспетчере оповещений, убедитесь, что надстройка импортируется с помощью Splunk Enterprise Security. См. «Импорт пользовательских приложений и надстроек для Splunk Enterprise Security» в *Руководстве по установке и обновлению*.
* Если вы можете выбрать адаптивное ответное действие в редакторе поиска корреляций, но не в Обзоре событий, адаптивное ответное действие может быть обычным оповещением, или ответное действие не поддерживает специальный вызов. См. «Определение того, поддерживает ли ваше действие специальный вызов» на портале разработчиков Splunk.

Настройка адаптивных ответных действий для поиска корреляций в Splunk Enterprise Security

В качестве администратора Splunk Enterprise Security вы можете настроить, какие адаптивные ответные действия запускаются поиском корреляций.

Аналитики могут запускать некоторые адаптивные ответные действия на специальной основе из Обзора событий. См. раздел «Адаптивные ответные действия, включённые в Splunk Enterprise Security» в *«Использование Splunk Enterprise Security»*.

Splunk Enterprise Security включает несколько адаптивных ответных действий, кроме того, дополнительные вы можете получить из надстроек, доступных в базе Splunk.

**Включенные адаптивные ответные действия**

Splunk Enterprise Security включает в себя несколько адаптивных ответных действий.

* Создание заметного события.
* Изменение степени риска с помощью модификатора рисков.
* Отправка электронного письма.
* Запуск скрипта.
* Запуск захвата потока с помощью приложения Splunk для Stream.
* Пинг хоста.
* Запуск Nbtstat.
* Запуск Nslookup.
* Добавление информации об угрозе.
* Создание сообщения в Splunk Web.

**Создание заметного события**

Создайте **заметное событие**, когда выполняются условия поиска корреляций.

1. В строке меню Splunk Enterprise Security нажмите **Configure** **> Content Management**.
2. Нажмите на существующий поиск корреляций либо нажмите **Create New > Correlation Search**.
3. Нажмите **Add New Response Action** и выберите **Notable**, чтобы добавить заметное событие.
4. Введите **Title** заметного события в панели **Incident Review**. Поддерживает функцию замены переменных из полей в сопоставимом событии.
5. Введите **Description** заметного события. Поддерживает функцию замены переменных из полей в сопоставимом событии.
6. В раскрывающемся списке выберите **Security Domain** заметного события.
7. В раскрывающемся списке выберите **Severity** заметного события. Степень серьезности используется для расчета **Urgency** заметного события.
8. (Опционально) Измените владельца заметного события, поменяв значение, заданное системой по умолчанию, – **не назначен (unassigned)**.
9. (Опционально) Измените статус заметного события со статуса, заданного системой по умолчанию, –**New**.
10. Введите детализированное имя для ссылки **Contributing Events** в заметном событии.
11. Введите развернутый поиск для ссылки **Contributing Events** в заметном событии.
12. В поле **Drill-down earliest offset** введите время до инициирующего события, чтобы найти связанные события для ссылки **Contributing Events** в заметном событии.

Например, **2 часа**, чтобы найти способствующие события, произошедшие за 2 часа до инициирующего события.

1. В поле **Drill-down latest offset** введите время после инициирующего события, чтобы найти связанные события для ссылки **Contributing Events** в заметном событии.

Например, **1 час**, чтобы найти способствующие события, произошедшие через 1 час после инициирующего события.

1. (Опционально) Добавьте **Investigation Profiles**, которые применяются к заметному событию. Например, добавьте профиль расследования, который подходит сценарию использования «Вредоносные программы» для событий, связанных с вредоносными программами.
2. (Опционально) Добавьте поля, содержащие цифровые объекты, в **Asset Extraction**, чтобы извлечь значения полей и добавить их в рабочую среду расследования в качестве артефактов, когда заметное событие добавляется в расследование.
3. (Опционально) Добавьте поля, содержащие идентификаторы, в **Identity Extraction**, чтобы извлечь значения полей и добавить их в рабочую среду расследования в качестве артефактов, когда заметное событие добавляется в расследование.
4. Введите для аналитика **Следующие шаги (Next Steps)**, которые нужно предпринять после сортировки заметного события. Введите текст или нажмите **Insert Adaptive Response Action** для ссылки на ответное действие в тексте для следующих шагов. В поле следующих шагов можно вводить только простой текст и ссылки на ответные действия. Используйте это поле, если хотите порекомендовать ответные действия, которые должны выполняться в определенном порядке. Например, выполнение пинга хоста, чтобы определить, активен ли он в сети. Если хост активен, необходимо увеличить степень риска на 100, в противном случае – увеличить степень риска на 50.
5. Выберите **Recommended Actions**, чтобы дополнить следующие шаги. В списке всех адаптивных ответных действий нажмите на имя действия, которое вы рекомендуете в качестве этапа сортировки или расследования для этого заметного события, чтобы добавить его в список рекомендуемых действий, которые аналитики могут предпринять в отношении этого заметного события. Можно добавить любое количество рекомендуемых действий. Используйте рекомендуемые действия, чтобы рекомендовать ответные действия, которые не нужно выполнять в определенном порядке.

Например, увеличить степень риска на хосте и запустить nslookup для поиска по доменному имени.

**Изменение степени риска с помощью модификатора рисков**

Измените степень риска в результате поиска корреляций или в ответ на детали заметного события с помощью адаптивного ответного действия **Анализ рисков** (**Risk Analysis)**. Связанное с риском адаптивное ответное действие создает событие модификатора рисков. Просмотреть события модификатора рисков можно на панели Анализ рисков (Risk Analysis) в Enterprise Security.

1. Нажмите **Add New Response Action** и выберите **Risk Analysis**.
2. Введите оценку, которую хотите присвоить объекту риска.
3. Введите поле в поиске, чтобы применить степень риска для **Risk Object Field**.

Например, введите «src», чтобы указать поле источника.

1. Выберите **Risk Object Type**, к которому будет применяться степень риска.

Другие способы изменения степени риска см. в разделе «Назначение степени риска для объекта» в документе *Использование Splunk Enterprise Security*.

**Отправка электронного письма**

Отправка электронного письма в результате обнаружения соответствия условиям поиска корреляций.

**Необходимые условия**

Перед настройкой этого ответного действия убедитесь, что на платформе Splunk настроен почтовый сервер.

* В случае Splunk Enterprise, см. раздел «Настройка параметров уведомлений по электронной почте» в *Руководстве по уведомлениям* для Splunk Enterprise.
* В случае Splunk Cloud, см. раздел «Настройка параметров уведомлений по электронной почте» в *Руководстве по уведомлениям* для Splunk Cloud.

**Шаги**

1. Нажмите **Add New Response Action** и выберите **Send email**.
2. В поле **To** перечислите через запятую адреса электронной почты, на которые хотите отправлять письмо.
3. (Опционально) Измените приоритет электронного письма. По умолчанию – **Lowest**.
4. Укажите тему электронного письма. Тема письма по умолчанию: «Splunk Alert: $name$», где $name$ – это **имя поиска** корреляций (**Search Name)**.
5. Введите сообщение, которое будет содержать основной текст письма. По умолчанию: «Запланированный запрос «$name$» был запущен» ("The scheduled report '$name$' has run").
6. Отметьте флажками поля с информацией, которую вы хотите включить в электронное письмо.
7. Выберите, следует ли отправлять электронное письмо с простым текстом или с HTML и простым текстом.

**Запуск скрипта**

Запустите скрипт, хранящийся в $SPLUNK\_HOME/bin/scripts.

1. Нажмите **Add New Response Action** и выберите **Run a script**.
2. Введите имя файла скрипта.

Более подробную информацию о заданных скриптом уведомлениях см. в документации по платформе Splunk.

* В случае Splunk Enterprise, см. раздел «Настройка заданных скриптом уведомлений» в *Руководстве по уведомлениям* для Splunk Enterprise.
* В случае Splunk Cloud, см. раздел «Настройка заданных скриптом уведомлений» в *Руководстве по уведомлениям* для Splunk Cloud.

**Запуск захвата потока с помощью приложения Splunk для Stream**

Запустите захват потока для захвата пакетов на IP-адресах выбранных протоколов за выбранный период времени. Вы можете просмотреть результаты сеанса захвата на панелях Сведения о протоколе (Protocol Intelligence).

Захват потока не будет работать, если вы не интегрируете приложение Splunk для Stream со Splunk Enterprise Security. См. раздел «Интеграция приложения Splunk для Stream со Splunk Enterprise Security».

1. Нажмите **Add New Response Action** и выберите **Stream Capture**, чтобы начать захват пакетов в ответ на совпадение в поиске корреляций.
2. Введите **Description**, чтобы описать поток, созданный в ответ на совпадение в поиске корреляций.
3. Введите **Category**, чтобы определить тип захвата потока. В приложении Splunk для Stream можно просматривать потоки по категориям.
4. Введите через запятую поля событий, чтобы найти IP-адреса для захвата потока. Для захвата используется первое поле с не нулевым значением.
5. Введите через запятую список протоколов для захвата.
6. Выберите **Capture duration**, чтобы определить продолжительность захвата пакетов.
7. Введите **Stream capture limit**, чтобы ограничить количество захватов потоков, начатых поиском корреляций.

**Проверка хоста**

Определите, активен ли хост в сети, с помощью пинга хоста.

1. Нажмите **Add New Response Action** и выберите **Ping**.
2. Введите поле события, содержащего хост, который вы хотите пинговать, в **Host Field**.
3. Введите максимальное число результатов, возвращаемых проверкой. По умолчанию – 1.

**Запуск nbtstat**

Узнайте больше о хосте и службах, которые этот хост запускает, запустил nbtstat.

1. Нажмите **Add New Response Action** и выберите **Nbtstat**.
2. Введите поле события, содержащего хост, для которого вы хотите запустить nbtstat, в **Host Field**.
3. Введите максимальное число результатов, возвращаемых nbtstat. По умолчанию – 1.

**Запуск nslookup**

Найдите доменное имя IP-адреса или IP-адрес доменного имени, запустив nslookup.

1. Нажмите **Add New Response Action** и выберите **Nslookup**.
2. Введите поле события, содержащего хост, для которого вы хотите запустить nslookup, в **Host Field**.
3. Введите максимальное число результатов, возвращаемых nslookup. По умолчанию – 1.

**Добавление информации об угрозе**

Создайте артефакты угроз в собрании угроз.

1. Нажмите **Add New Response Action** и выберите **Add Threat Intelligence**.
2. Выберите **Threat Group**, к которой необходимо отнести этот артефакт.
3. Выберите **Threat Collection**, в которое необходимо включить артефакт угроз.
4. Введите **Search Field**, содержащее значение, которое необходимо вставить в артефакт угрозы.
5. Введите **Description** артефакта угрозы.
6. Введите **Weight**, связанный со списком угроз. По умолчанию – 1.
7. Введите **Max Results**, чтобы указать количество результатов для обработки в качестве артефактов угроз. Каждое уникальное значение поля поиска считается результатом. По умолчанию – 100.

**Цифровые объекты и Идентификаторы**

**Добавление цифровых объектов и идентификаторов в Splunk Enterprise Security**

Splunk Enterprise Security использует систему цифровых объектов и идентификаторов, чтобы сопоставлять информацию об цифровых объектах и идентификаторах с событиями для обогащения и предоставления контекста к вашим данным. Эта система берет информацию из внешних источников данных для заполнения **справочников**, которые Enterprise Security сопоставляет с событиями во время поиска.

Добавьте данные об цифровых объектах и идентификаторах в Splunk Enterprise Security, чтобы пользоваться корреляцией цифровых объектов и идентификаторов.

1. Сбор и извлечение данных об цифровых объектах и идентификаторах в Splunk Enterprise Security.
2. (Опционально) Определение формата идентификаторов на странице конфигурации идентификаторов в Splunk Enterprise Security.
3. Оформление списка цифровых объектов или идентификаторов в виде справочника в Splunk Enterprise Security.
4. Настройка нового списка цифровых объектов или идентификаторов в Splunk Enterprise Security.
5. Проверка того, что данные об цифровых объектах и идентификаторах были добавлены в Splunk Enterprise Security
6. Настройка корреляции цифровых объектов и идентификаторов в Splunk Enterprise Security.

**Смотрите также**

Как Splunk Enterprise Security сопоставляет, обрабатывает и объединяет данные об цифровых объектах и идентификаторах

Справочники, в которых хранятся объединенные данные об цифровых объектах и идентификаторах

**Сбор и извлечение данных об цифровых объектах и идентификаторах в Splunk Enterprise Security**

Собирайте и извлекайте данные об цифровых объектах и идентификаторах, чтобы добавлять их в Splunk Enterprise Security. В развертывании Splunk Cloud работайте в Splunk Professional Services для разработки и внедрения решений по сбору цифровых объектов и идентификаторов. Примеры добавления данных об цифровых объектах и идентификаторах см. в разделе «Примеры способов добавления данных об цифровых объектах и идентификаторах в Splunk Enterprise Security».

1. Определите, где в вашей среде хранятся данные об цифровых объектах и идентификаторах.
2. Автоматически собирайте и обновляйте свои данные об цифровых объектах и идентификаторах, чтобы уменьшить затраты и обслуживание, требуемые для обновления вручную, и улучшить целостность данных.

* Используйте Splunk DB Connect или другую дополнительную платформу Splunk для подключения к внешней базе данных или репозиторию.
* Используйте подготовленные вводы для импорта и форматирования списков.
* Используйте события, индексированные на платформе Splunk, с помощью поиска для сбора, сортировки и экспорта данных в список.

Предлагаемые методы сбора для цифровых объектов и идентификаторов.

|  |  |  |
| --- | --- | --- |
| **Технология** | **Цифровые объекты или Идентификаторы** | **Методы сбора** |
| Active Directory | Оба | SA-ldapsearch и пользовательский поиск.  См. раздел «Примеры способов добавления данных об цифровых объектах и идентификаторах в Splunk Enterprise Security». |
| Оба | SecKit Windows Add On for ES Asset and Identities |
| LDAP | Оба | SA-ldapsearch и пользовательский поиск |
| CMDB | Цифровые объекты | DB Connect и пользовательский поиск |
| ServiceNow | Оба | Splunk Add-on for ServiceNow |
| Asset Discovery | Цифровые объекты | Splunk for Asset Discovery |
| Bit9 | Цифровые объекты | Splunk Add-on for Bit9 и пользовательский поиск |
| Cisco ISE | Оба | Splunk Add-on for Cisco ISE и пользовательский поиск |
| Microsoft SCOM | Цифровые объекты | Splunk Add-on for Microsoft SCOM и пользовательский поиск |
| Okta | Идентификаторы | Splunk Add-on for Okta и пользовательский поиск |
| Sophos | Цифровые объекты | Splunk Add-on for Sophos и пользовательский поиск |
| Symantec Endpoint Protection | Цифровые объекты | Splunk Add-on for Symantec Endpoint Protection и пользовательский поиск |
| Splunk platform | Цифровые объекты |  |

|  |  |  |
| --- | --- | --- |
|  |  | «Добавление данных об цифровых объектах из индексированных событий на платформе Splunk». |
| Amazon Web Services  (AWS) | Цифровые объекты | SecKit AWS Add On for ES Asset and Identities |
| Configuration Management Database (CMDB) | Цифровые объекты | SecKit SA Common Tools for ES Asset and Identities |

**Следующий шаг**

(Опционально) Определение формата идентификаторов в Splunk Enterprise Security

Оформление списка цифровых объектов или идентификаторов в виде справочника в Splunk Enterprise Security

**Определение формата идентификаторов в Splunk Enterprise Security**

Определите форматы идентификаторов, которые идентифицируют пользователей в вашей среде, на странице Конфигурация справочника идентификаторов (Identity Lookup Configuration). Изменения, внесенные на странице Конфигурация справочника идентификаторов (Identity Lookup Configuration) изменяют файл identityLookup.conf.

**Необходимые условия**

Сбор и извлечение данных об цифровых объектах и идентификаторах в Splunk Enterprise Security

**Шаги**

1. В строке меню Splunk ES выберите **Configure > Data Enrichment > Identity Lookup Configuration**.
2. (Опционально) Снимите выделение ячейки **Email**, если адреса электронной почты не идентифицируют пользователей в вашей среде.
3. (Опционально) Снимите выделение ячейки **Email short**, если имя пользователя адреса электронной почты не идентифицирует пользователей в вашей среде.
4. (Опционально) Отметьте ячейку **Convention**, если хотите определить условие для идентификации пользователей. Нажмите **Add a new convention**, чтобы добавить условие.

Например, идентифицируйте пользователей по первым трем буквам их имени и фамилии, используя условие first(3)last(3).

1. (Опционально) Отметьте ячейку **Case Sensitive**, чтобы требовать совпадения идентификаторов с учетом регистра. Совпадение идентификаторов с учетом регистра дает меньше результатов совпадений.
2. Нажмите **Save**.

**Следующий шаг**

Оформление списка цифровых объектов или идентификаторов в виде справочника в Splunk Enterprise Security

**Оформление списка цифровых объектов или идентификаторов в виде справочника в Splunk Enterprise Security**

Оформите собранные данные об цифровых объектах и идентификаторах в виде файла справочника, чтобы он мог обрабатываться Splunk Enterprise Security.

**Необходимые условия**

* Сбор и извлечение данных об цифровых объектах и идентификаторах в Splunk Enterprise Security
* (Опционально) Определение формата идентификаторов в Splunk Enterprise Security

**Шаги**

1. Создайте файл с обычным текстом, в формате CSV, с окончанием строки Unix и расширением .csv.
2. Используйте правильные заголовки для CSV-файла. Заголовки, ожидаемые Splunk Enterprise Security, см. в разделах «Заголовок справочника цифровых объектов» или «Заголовок справочника идентификаторов».
3. Заполните строки CSV полями цифровых объектов или идентификаторов. Для справки см. разделы «Поля справочника цифровых объектов» или «Поля справочника идентификаторов».

Пример списка цифровых объектов см. в Демонстрационном справочнике цифровых объектов.

* Найдите список в Splunk Web, нажав **Configure** > **Content Management**.
* Найдите список в файловой системе, файл demo\_assets.csv находится в каталоге SA-IdentityManagement/lookups/.

Если вы используете пользовательский поиск для генерации справочника, убедитесь, что справочник, созданный результатами поиска, содержит поля, соответствующие заголовкам.

**Следующий шаг**

Настройка нового цифровых объекта или списка идентификаторов в Splunk Enterprise Security

**Заголовок справочника цифровых объектов**

ip, mac,nt\_host, dns, owner, priority, lat, long, city, country, bunit, category, pci\_domain, is\_expected, should\_timesync, should\_update, requires\_av

**Поля справочника цифровых объектов**

Заполните следующие поля в справочнике цифровых объектов.

Чтобы добавить многосетевые хосты или устройства в список цифровых объектов, добавьте каждый IP-адрес в поле ip для хоста, разделяя адреса вертикальной линией. Поддержка многосетевых хостов ограничена, и наличие нескольких хостов с одним IP-адресом в разных сегментах сети может вызвать конфликты в процессе объединения.

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип данных** | **Описание** | **Пример** |
| ip | цифры, разделенные вертикальной линией | Список одиночных IP-адресов или диапазонов IP-адресов, разделенных вертикальной линией. Цифровой объект должен иметь запись в полях **ip**, **mac**, **nt\_host** или **dns**. Не используйте разграничение линией для более чем одного из этих полей для каждого цифрового объекта. | 2.0.0.0/8|1.2.3.4|192.168.15.9-192.169.15.27|5.6.7.8|10.11.12.13 |
| mac | строки, разделенные вертикальной линией | Список MAC-адресов, разделенных вертикальной линией. Цифровой объект должен иметь запись в полях **ip**, **mac**, **nt\_host** или **dns**. Не используйте разграничение линией для более чем одного из этих полей для каждого цифрового объекта. | 00:25:bc:42:f4:60|00:50:ef:84:f1:21|00:50:ef:84:f1:20 |
| nt\_host | строки, разделенные вертикальной линией | Список имен компьютеров Windows, разделенных вертикальной линией. | ACME-0005|SSPROCKETS-0102|COSWCOGS-013 |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Цифровой объект должен иметь запись в полях **ip**, **mac**, **nt\_host** или **dns**. Не используйте разграничение линией для более чем одного из этих полей для каждого цифрового объекта. |  |
| dns | строки, разделенные вертикальной линией | Список DNS-имен, разделенных вертикальной линией. Цифровой объект должен иметь запись в полях **ip**, **mac**, **nt\_host** или **dns**. Не используйте разграничение линией для более чем одного из этих полей для каждого цифрового объекта. | acme-0005.corp1.acmetech.org|SSPROCKETS-0102.spsp.com|COSWCOGS-013.cwcogs.com |
| owner | строка | Пользователь или отдел, связанные с устройством. | f.prefect@acmetech.org, DevOps, Bill |
| priority | строка | **Рекомендовано**. Приоритет, назначенный устройству для расчета поля **Срочность (Urgency)** для заметных событий в Анализе инцидентов (Incident Review). Приоритет «неизвестно» ("unknown") по умолчанию снижает назначенную **Срочность (Urgency)**. | неизвестно (unknown), низкий (low), средний (medium), высокий (high) или особой важности (critical) |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Дополнительные сведения см. в разделе «Как назначается срочность заметным событиям в Splunk Enterprise Security. |  |
| lat | строка | Широта цифрового объекта | 41.040855 |
| long | строка | Долгота цифрового объекта | 28.986183 |
| city | строка | Город, в котором находится цифровой объект | Chicago |
| country | строка | Страна, в которой находится цифровой объект | USA |
| bunit | строка | **Рекомендовано**. Подразделение цифрового объекта. Используется для фильтрации панелями в Splunk Enterprise Security. | EMEA, NorCal |
| category | строки, разделенные вертикальной линией | **Рекомендовано**. Список логических классификаций цифровых объектов, разделенных вертикальной линией. Используется для корреляции и категоризации цифровых объектов и идентификаторов. См. раздел «Категории цифровых объектов/ идентификаторов». | server|web\_farm|cloud |
| pci\_domain | строки, разделенные вертикальной линией | Список доменов PCI, разделенных вертикальной линией. | cardholder, trust|dmz, untrust  Если поле оставлено пустым, по умолчанию –ненадежный (untrust). |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | См. раздел «Настройка цифровых объектов в приложении Splunk для соответствия требованиям стандарта PCI» в *Руководстве по установке и конфигурации*. |  |
| is\_expected | булевские значения | Указывает, должны ли события от этого цифрового объекта ожидаться всегда. Если установлено значение «истина» («true»), поиск корреляции «От ожидаемого хоста сообщений нет» (“Expected Host Not Reporting”) осуществляет адаптивное ответное действие, когда этот цифровой объект перестает сообщать о событиях. | «истина» ("true") или пустое поле, обозначающее «ложь» ("false") |
| should\_timesync | булевские значения | Указывает, должен ли этот цифровой объект проверяться на предмет событий синхронизации времени. Если установлено значение «истина» («true»), корреляционный поиск «Если хост синхронизации времени не осуществляет синхронизацию» (Should Timesync Host Not Syncing) выполняет адаптивное ответное действие, если этот цифровой объект не сообщает о событиях синхронизации времени за последние 24 часа. | «истина» ("true") или пустое поле, обозначающее «ложь» ("false") |
| should\_update | булевские значения | Указывает, должен ли этот цифровой объект | «истина» ("true") или пустое поле, обозначающее «ложь» ("false") |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | проверяться на предмет событий обновления системы. |  |
| requires\_av | булевские значения | Указывает, должно ли на этом цифровом объекте быть установлено антивирусное программное обеспечение. | «истина» ("true") или пустое поле, обозначающее «ложь» ("false") |

**Заголовок справочника идентификаторов**

identity, prefix, nick, first, last, suffix, email, phone, phone2, managedBy, priority, bunit, category, watchlist, startDate, endDate, work\_city, work\_country, work\_lat, work\_long

**Поля справочника идентификаторов**

|  |  |  |  |
| --- | --- | --- | --- |
| **Поле** | **Тип данных** | **Описание** | **Пример** |
| identity | строки, разделенные вертикальной линией | **Обязательно.** Список строк с именами пользователя, разделенными вертикальной линией и представляющими идентификатор. После завершения процесса объединения это поле включает сгенерированные значения на основе настроек конфигурации поиска идентификатора. | a.vanhelsing|abraham.vanhelsing|a.vanhelsing@acmetech.org |
| prefix | строка | Префикс идентификатора. | Ms., Mr. |
| nick | строка | Никнейм идентификатора. | Van Helsing |
| first | строка | Имя идентификатора. | Abraham |
| last | строка | Фамилия идентификатора. | Van Helsing |
| suffix | строка |  | M.D., Ph.D |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Титул идентификатора. |  |
| email | строка | Адрес электронной почты идентификатора. | a.vanhelsing@acmetech.org |
| phone | строка | Номер телефона идентификатора. | 123-456-7890 |
| phone2 | строка | Дополнительный номер телефона идентификатора. | 012-345-6789 |
| managedBy | строка | Имя пользователя, представляющего менеджера идентификатора. | phb@acmetech.org |
| priority | строка | **Рекомендовано**. Приоритет, назначенный идентификатору для расчета поля **Срочность (Urgency)** для заметных событий в Анализе инцидентов (Incident Review). Приоритет «неизвестно» ("unknown") по умолчанию снижает назначенную **Срочность (Urgency)**. Дополнительные сведения см. в разделе «Как назначается срочность заметным событиям в Splunk Enterprise Security. | неизвестно (unknown), низкий (low), средний (medium), высокий (high) или особой важности (critical) |
| bunit | строка | **Рекомендовано**. Классификация групп или отделов для идентификаторов. | Field Reps, ITS, Products, HR |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Используется для фильтрации панелями в Splunk Enterprise Security. |  |
| category | строки, разделенные вертикальной линией | **Рекомендовано**. Список логических классификаций для идентификаторов, разделенных вертикальной линией. Используется для корреляции и категоризации цифровых объектов и идентификаторов. См. раздел «Категории цифровых объектов/ идентификаторов». | Privileged|Officer|CISO |
| watchlist | булевские значения | Помечает идентификатор для мониторинга активности. | Принимаемые значения: «истина» («true») или пустое поле. См. раздел «Мониторинг активности пользователей» в настоящем руководстве. |
| startDate | строка | Дата начала работы или найма идентификатора. | Formats: %m/%d/%Y %H:%M, %m/%d/%y %H:%M, %s |
| endDate | строка | Дата окончания работы или увольнения идентификатора. | Formats: %m/%d/%Y %H:%M, %m/%d/%y %H:%M, %s |
| work\_city | строка | Город основного места работы идентификатора |  |
| work\_country | строка | Страна основного места работы идентификатора |
| work\_lat | строка | Широта города основного места работы в десятичных градусах с направлением стрелки компаса. | 37.78N |
| work\_long | строка | Долгота города основного места работы в десятичных градусах с направлением стрелки компаса. | 122.41W |

**Настройка нового списка цифровых объектов или идентификаторов в Splunk Enterprise Security**

Настройте новый справочник цифровых объектов или идентификаторов в Splunk Enterprise Security. Этот многоступенчатый процесс добавляет справочник в Splunk Enterprise Security и определяет справочник для процесса объединения.

**Необходимые условия** Оформление списка цифровых объектов или идентификаторов в виде справочника в Splunk Enterprise Security.

**Шаги**

1. Добавление нового табличного файла справочника
2. Установка прав доступа для табличного файла справочника, чтобы поделиться им с помощью Splunk Enterprise Security
3. Добавление характеристик нового справочника
4. Установка прав доступа для характеристик справочника, чтобы поделиться ими с помощью Splunk Enterprise Security
5. Добавление входной строки для источника справочника
6. (Опционально) Принудительное объединение

**Добавление нового табличного файла справочника**

1. В строке меню Splunk выберите **Settings > Lookups > Lookup table files**.
2. Нажмите **New**.
3. Выберите **Destination App** в **SA-IdentityManagement**.
4. Выберите файл справочника для загрузки.
5. Введите **Destination filename**, которое должен иметь табличный файл справочника, в поисковом блоке. Имя должно включать в себя расширение имени файла. Например, network\_assets\_from\_CMDB.csv
6. Нажмите **Save**, чтобы сохранить табличный файл справочника и вернуться к списку табличных файлов справочников.

**Установка прав доступа для табличного файла справочника, чтобы поделиться им с помощью Splunk Enterprise Security**

1. Найдите новый табличный файл справочника в **Lookup table files** и выберите **Permissions**.
2. В поле **Object should appear in** выберите **All apps**.
3. Установите доступ для чтения **Read** для всех **Everyone**.
4. Установите доступ для записи для admin или других ролей.
5. Нажмите **Save**.

**Добавление характеристик нового справочника**

1. В строке меню Splunk выберите **Settings > Lookups > Lookup definitions**.
2. Нажмите **New**.
3. Выберите **Destination App** в **SA-IdentityManagement**.
4. Введите имя источника справочника. Это имя должно соответствовать имени, указанному далее в характеристиках входной строки на панели **Identity Management**.

Например, network\_assets\_from\_CMDB.

1. Выберите следующий **Type** в **File based**.
2. Выберите созданный табличный файл справочника.

Например, выберите network\_assets\_from\_CMDB.csv.

1. Нажмите **Save**.

**Установка прав доступа для характеристик справочника, чтобы поделиться ими с помощью Splunk Enterprise Security**

1. Найдите новые характеристики справочника в **Lookup definitions** и выберите **Permissions**.
2. В поле **Object should appear in** выберите **All apps**.
3. Установите доступ для чтения **Read** для всех **Everyone**.
4. Установите доступ для записи для admin или других ролей.
5. Нажмите **Save**.

**Добавление входной строки для источника справочника**

1. Вернитесь к Splunk Enterprise Security.
2. В строке меню Splunk ES выберите **Configure > Data Enrichment > Identity Management**.
3. Нажмите **New**.
4. Введите имя справочника.

Например, network\_assets\_from\_CMDB.

1. Введите **Category** для описания нового списка цифровых объектов или идентификаторов.

Например, CMDB\_network\_assets.

1. Введите **Description** содержимого списка.

Например, сетевые цифровые объекты из конфигурационной базы данных.

1. Введите **asset** или **identity**, чтобы определить тип списка.
2. Введите **Source**, который ссылается на имя характеристик справочника.

Например, lookup://network\_assets\_from\_CMDB.

1. Нажмите **Save**.
2. Подождите пять минут. Splunk Enterprise Security каждые пять минут объединяет списки цифровых объектов и идентификаторов с сохраненными условиями поиска. Объяснение этого процесса см. в разделе «Как Splunk Enterprise Security обрабатывает и объединяет данные об цифровых объектах и идентификаторах».

**Принудительное объединение**

Вы также можете непосредственно запустить первичные сохраненные условия поиска, чтобы незамедлительно принудительно начать объединение, не выжидая пяти минут до запуска запланированного поиска.

1. Откройте Страницу поиска (Search page).
2. Запустите первичные сохраненные условия поиска.

| from savedsearch:"Identity - Asset String Matches - Lookup Gen"

| from savedsearch:"Identity - Asset CIDR Matches - Lookup Gen"

| from savedsearch:"Identity - Identity Matches - Lookup Gen"

**Следующий шаг**

Проверка того, что данные об цифровых объектах или идентификаторах были добавлены в Splunk Enterprise Security

**Проверка того, что данные об цифровых объектах или идентификаторах были добавлены в Splunk Enterprise Security**

Убедитесь, что ваши данные об цифровых объектах или идентификаторах были добавлены в Splunk Enterprise Security с помощью поиска и просмотра панелей мониторинга.

**Необходимые условия**

Настройка нового списка цифровых объектов или идентификаторов в Splunk Enterprise Security

**Шаги**

Проверьте данные о справочнике цифровых объектов.

1. Убедитесь, что в справочнике цифровых объектов существует определенная запись об цифровом объекте.
   1. Выберите из списка цифровых объектов запись об цифровом объекте с данными в полях ip, mac, nt\_host или dns.
   2. Ищите ее в Splunk Web.

| makeresults | eval src="1.2.3.4" | 'get\_asset(src)

* Просмотрите все доступные цифровые объекты в вашем экземпляре, используя один из следующих способов. Сравните количество строк с вашими источниками данных об цифровом объекте, чтобы проверить, что количество записей об цифровых объектах соответствует вашим ожиданиям, или выборочно проверьте конкретные записи.
* Просмотрите панель Центр цифровых объектов (Asset Center). См. раздел «Панель Центр цифровых объектов (Asset Center) в документе *Использование Splunk Enterprise Security*.
* Используйте макрос цифровых объектов.

| 'assets'

* Запустите поиск модели данных.

|'datamodel("Identity\_Management", "All\_Assets")'

|'drop\_dm\_object\_name("All\_Assets")'

Проверьте данные о справочнике идентификаторов.

1. Убедитесь, что в справочнике идентификаторов существует определенная запись об идентификаторе.
   1. Выберите запись об идентификаторе с данными в поле identity.
   2. Ищите ее в Splunk Web.

| makeresults | eval user="VanHelsing" |

'get\_identity4events(user)

* Просмотрите все доступные идентификаторы в вашем экземпляре, используя один из следующих способов. Сравните количество строк с вашими источниками данных об идентификаторе, чтобы проверить, что количество записей об идентификаторах соответствует вашим ожиданиям, или выборочно проверьте конкретные записи.
* Просмотрите панель Центр идентификаторов (Identity Center). См. раздел «Панель Центр идентификаторов (Identity Center) в документе *Использование Splunk Enterprise Security*.
* Используйте макрос идентификаторов.

| 'identities'

* Запустите поиск модели данных.

|'datamodel("Identity\_Management", "All\_Identities")'

|'drop\_dm\_object\_name("All\_Identities")

**Следующий шаг**

Настройка корреляции цифровых объектов и идентификаторов в Splunk Enterprise Security

**Настройка корреляции цифровых объектов и идентификаторов в Splunk Enterprise Security**

Добавив данные о своем цифровом объекте и идентификаторе в Splunk Enterprise Security, настройте корреляцию цифровых объектов и идентификаторов в Splunk Enterprise Security.

**Необходимые условия**

Проверка того, что данные об цифровых объектах или идентификаторах были добавлены в Splunk Enterprise Security

**Шаги**

1. Выберите, следует ли включить корреляцию цифровых объектов и идентификаторов, отключить или ограничить ее, осуществляя только для выбранных типов источников. Если сомневаетесь, оставьте корреляцию цифровых объектов и идентификаторов включенной. Дополнительную информацию о том, как корреляция обогащает события во время поиска см. в разделе «Как работает корреляция цифровых объектов и идентификаторов».
2. В строке меню Splunk ES выберите **Configure > Data Enrichment > Identity Correlation**.
3. По умолчанию выбрана опция **Enable correlation**. Вы можете изменить ее на **Disable correlation** (не рекомендуется) или **Включить выборочно по типу источника (Enable selectively by sourcetype)**.
4. Если вы выбираете опцию **Включить выборочно по типу источника (Enable selectively by sourcetype)**, введите тип источника и отметьте ячейку для цифрового объекта и/или идентификатора.
5. Нажмите **Save**.

Отключение корреляции цифровых объектов и идентификаторов полностью предотвращает обогащение событий данными об цифровых объектах и идентификаторах из справочников цифровых объектов и идентификаторов. Это может помешать поиску корреляций, панелям мониторинга и другим функциям работать должным образом. Проконсультируйтесь со Splunk Professional Services или Splunk Support перед отключением корреляции цифровых объектов и идентификаторов.

**Как работает корреляция цифровых объектов и идентификаторов**

Чтобы эффективно обнаруживать вторжения в систему безопасности, организация должна иметь возможность сопоставлять события из данных журнала с конкретными цифровыми объектами и идентификаторами, которые могут быть ответственны за вторжение или затронуты им. Когда корреляция цифровых объектов и идентификаторов включена, Splunk Enterprise Security сравнивает индексированные события с данными об цифровых объектах и идентификаторах в списках цифровых объектов и идентификаторов, чтобы обеспечить обогащение данных и контекст. Процесс сравнения использует автоматический поиск. Вы можете найти информацию об автоматическом поиске в документации на платформу Splunk.

* В случае Splunk Enterprise, см. раздел «Сделать поиск автоматическим» в *Руководстве администратора базы знаний* Splunk Enterprise.
* В случае Splunk Cloud, см. раздел «Сделать поиск автоматическим» в *Руководстве администратора базы знаний* Splunk Cloud.

Корреляция цифровых объектов и идентификаторов обогащает события данными об цифровых объектах и идентификаторах во время поиска.

* Корреляция цифровых объектов сравнивает события, которые содержат данные в любом из полей src, dest или dvc с объединенными списками цифровых объектов на предмет совпадения IP-адреса, MAC-адреса, DNS-имени или имен Windows NetBIOS. Корреляция цифровых объектов больше не выполняется автоматически в отношении полей host или orig\_host.
* Корреляция идентификаторов сравнивает события, которые содержат данные в любом из полей user или src\_user, с объединенными списками идентификаторов на предмет совпадения пользователя или сеанса.
* Enterprise Security добавляет в событие совпадающие поля вывода. Например, корреляция по полю src цифрового объекта создает дополнительные поля, такие как src\_is\_expected и src\_should\_timesync.

Корреляция цифровых объектов и идентификаторов позволяет определить, могут ли несколько событий относиться к одному и тому же цифровому объекту или идентификатору. Вы также можете выполнять действия в полях идентификаторов и цифровых объектов, добавленных в события, чтобы открыть дополнительные поисковые запросы или панели, привязанные к конкретному цифровому объекту или идентификатору. Например, открыть панель Исследователь цифровых объектов (Asset Investigator) в поле src.

**Как Splunk Enterprise Security обрабатывает и объединяет данные об цифровых объектах и идентификаторах**

Splunk Enterprise Security извлекает данные об цифровых объектах и идентификаторах, которые вы добавляете в виде справочников, и генерирует файлы комбинированных справочников. Splunk Enterprise Security использует созданные файлы справочников для сопоставления данных об цифровых объектах и идентификаторах с событиями с помощью автоматических справочников.

Следующие шаги описывают этот процесс на высоком уровне.

1. Вы собираете данные об цифровых объектах и идентификаторах из источников данных, используя дополнения и пользовательский поиск или вручную с помощью CSV-файла. См. Сбор и извлечение данных об цифровых объектах и идентификаторах в Splunk Enterprise Security.
2. Вы устанавливаете любые настройки в настройках конфигурации справочника идентификаторов. См. Определение формата идентификаторов на странице конфигурации идентификаторов.
3. Модульные данные ввода диспетчера идентификаторов Splunk Enterprise Security обновляют настройки в transforms.conf, станза identity\_lookup\_expanded.
4. Вы оформляете данные в виде справочника, используя поиск, или вручную с помощью CSV-файла. См. Оформление списка цифровых объектов или идентификаторов в виде справочника.
5. Вы настраиваете список как таблицу справочника, характеристики и данные ввода. См. Настройка нового списка цифровых объектов или идентификаторов.
6. Модульные данные ввода диспетчера идентификаторов Splunk Enterprise обнаруживают две вещи:
   * Измененный контент в identity\_manager://<input\_name>.
   * Изменения в станзах данных ввода.
7. Модульные данные ввода диспетчера идентификаторов Splunk Enterprise Security обновляют макросы, используемые для идентификации источников данных ввода на основе действующих станз в inputs.conf. Например, макрос ‘generate\_identities’ динамически обновляется в зависимости от условий, указанных на странице «Конфигурация справочника идентификаторов» (Lookup Configuration page).
8. Модульные данные ввода диспетчера идентификаторов Splunk Enterprise Security осуществляют диспетчеризацию справочника, генерирующего сохраненные поисковые запросы, если обнаруживают изменения, которые требуют объединения списков цифровых объектов и идентификаторов.
9. Справочник, генерирующий сохраненные поисковые запросы, объединяет все сконфигурированные и включенные списки цифровых объектов и идентификаторов.

* Первичные сохраненные поисковые запросы объединяют таблицы справочников, на которые ссылаются данные ввода диспетчера идентификаторов, генерируют новые поля и выводят объединенные списки цифровых объектов и идентификаторов в табличные файлы целевых справочников.
* Вторичные сохраненные поисковые запросы генерируют таблицы справочников для категорий цифровых объектов, категорий идентификаторов и доменов PCI цифровых объектов (в приложении Splunk для соответствия требованиям PCI).

1. Вы проверяете, что данные выглядят так, как ожидалось. См. раздел «Проверка того, что данные об цифровых объектах или идентификаторах были добавлены в Splunk Enterprise Security».

Объединение справочников идентификаторов и цифровых объектов не подтверждает и не дедуплицирует данные ввода. Ошибки из модульных данных ввода диспетчера идентификаторов регистрируются в файле identity\_manager.log. В этом журнале не отображаются ошибки данных.

**Справочники, в которых хранятся объединенные данные об цифровых объектах и идентификаторах в Splunk Enterprise Security**

После завершения процесса объединения цифровых объектов и идентификаторов ваши данные об цифровых объектах и идентификаторах хранятся в четырех справочниках.

|  |  |  |  |
| --- | --- | --- | --- |
| **Функция** | **Имя таблицы** | **Сохраненный поиск** | **Имя справочника** |
| Корреляция цифровых объектов на основе строк | assets\_by\_str.csv | Identity – Asset String Matches – Lookup Gen | LOOKUP-zu-asset\_lookup\_by\_str-dest  LOOKUP-zu-asset\_lookup\_by\_str-dvc  LOOKUP-zu-asset\_lookup\_by\_str-src |
| Корреляция цифровых объектов на основе подсети CIDR | assets\_by\_cidr.csv | Identity – Asset CIDR Matches – Lookup Gen | LOOKUP-zv-asset\_lookup\_by\_cidr-dest  LOOKUP-zv-asset\_lookup\_by\_cidr-dvc  LOOKUP-zv-asset\_lookup\_by\_cidr-src |
| Корреляция идентификаторов на основе строк | identities\_expanded.csv | Identity – Identity Matches – Lookup Gen | LOOKUP-zy-identity\_lookup\_expanded-src\_user  LOOKUP-zy-identity\_lookup\_expanded-user |
| Корреляция полей по умолчанию | identity\_lookup\_default\_fields.csv asset\_lookup\_default\_fields.csv |  | LOOKUP-zz-asset\_identity\_lookup\_default\_fields-dest  LOOKUP-zz-asset\_identity\_lookup\_default\_fields-dvc  LOOKUP-zz-asset\_identity\_lookup\_default\_fields-src  LOOKUP-zz-asset\_identity\_lookup\_default\_fields-src\_user  LOOKUP-zz-asset\_identity\_lookup\_default\_fields-user |

Дополнительные сведения о процессе объединения цифровых объектов и идентификаторов см. в разделе «Как Splunk Enterprise Security обрабатывает и объединяет данные об цифровых объектах и идентификаторах».

**Поля цифровых объектов и идентификаторов после обработки в Splunk Enterprise Security**

В следующих таблицах описываются поля, которые присутствуют в справочниках цифровых объектов и идентификаторов после того, как Splunk Enterprise Security завершает обработку исходных файлов справочников.

Эти поля присутствуют в справочниках, в которых хранятся объединенные данные об цифровых объектах и идентификаторах. См. раздел «Справочники, в которых хранятся объединенные данные об цифровых объектах и идентификаторах в Splunk Enterprise Security».

Дополнительные сведения о процессе объединения см. в разделе «Как Splunk Enterprise Security обрабатывает и объединяет данные об цифровых объектах и идентификаторах».

**Поля цифровых объектов после обработки**

Поля цифровых объектов справочника цифровых объектов после того, как сохраненные поисковые запросы выполняют процесс объединения.

|  |  |
| --- | --- |
| **Поле** | **Действие, предпринятое ETL** |
| bunit | без изменений |
| city | без изменений |
| country | без изменений |
| dns | Принимает значения, разделенные вертикальной линией, и преобразует их в многозначное поле. |
| lat | без изменений |
| long | без изменений |
| mac | Принимает значения, разделенные вертикальной линией, и преобразует их в многозначное поле. |
| nt\_host | Принимает значения, разделенные вертикальной линией, и преобразует их в многозначное поле. |
| owner | без изменений |
| priority | без изменений |
| asset\_id | Сгенерировано из значений полей dns, ip, mac и nt\_host. |
| asset\_tag | Сгенерировано из значений полей category, pci\_domain, is\_expected, should\_timesync, should\_update, require\_av и bunit. |
| category | Добавляет «pci», если значение содержит «cardholder». Принимает значения, разделенные вертикальной линией, и преобразует их в многозначное поле. |
| ip | Проверяет и по мере необходимости разбивает поле на подсети CIDR. Принимает значения, разделенные вертикальной линией, и преобразует их в многозначное поле. |

|  |  |
| --- | --- |
| pci\_domain | Добавляет слово «надежный» («trust») или ненадежный («untrust») на основе определенных значений полей. Принимает значения, разделенные вертикальной линией, и преобразует их в многозначное поле. |
| is\_expected | Нормализуется до булева значения. |
| should\_timesync | Нормализуется до булева значения. |
| should\_update | Нормализуется до булева значения. |
| requires\_av | Нормализуется до булева значения. |
| key | Генерируется полями ip, mac, nt\_host и dns после преобразования исходных полей. |

**Поля идентификаторов после обработки**

Поля идентификаторов справочника идентификаторов после того, как сохраненные поисковый запросы выполняют процесс объединения.

|  |  |
| --- | --- |
| **Поле** | **Действие, предпринятое ETL** |
| bunit | без изменений |
| email | без изменений |
| endDate | без изменений |
| first | без изменений |
| last | без изменений |
| managedBy | без изменений |
| nick | без изменений |
| phone | без изменений |
| phone2 | без изменений |
| prefix | без изменений |
| priority | без изменений |
| startDate | без изменений |
| suffix | без изменений |
| work\_city | без изменений |
| work\_country | без изменений |
| work\_lat | без изменений |
| work\_long | без изменений |
| watchlist | Нормализуется до булева значения. |

|  |  |
| --- | --- |
| category | Добавляет «pci», если значение содержит «cardholder». Принимает значения, разделенные вертикальной линией, и преобразует их в многозначное поле. |
| identity | Создается на основе значений в строке данных ввода и условий, указанных в Конфигурации поиска идентификатора (Identity Lookup Configuration). Принимает значения, разделенные вертикальной линией, и преобразует их в многозначное поле. |
| identity\_id | Генерируется из значений полей identity, first, last и email. |
| identity\_tag | Генерируется из значений полей bunit, category и watchlist. |

**Тестирование процесса объединения цифровых объектов и идентификаторов в Splunk Enterprise Security**

Вы можете протестировать процесс объединения цифровых объектов и идентификаторов, если хотите убедиться, что данные, полученные в процессе объединения, ожидаемы и точны. Запустите сохраненные поисковые запросы, которые выполняют процесс объединения, не выводя данные в объединенные справочники, чтобы выяснить, что объединение сделает с данными, без фактического выполнения объединения. Эти шаги не являются обязательными, но могут выполняться для проверки того, что объединение данных работает надлежащим образом.

Протестируйте процесс объединения без фактического выполнения объединения и вывода данных в справочник.

1. В строке меню Splunk ES выберите **Configure > Content Management**.
2. Найдите первый из трех основных сохраненных поисковых запросов **Identity – Asset CIDR Matches – Lookup Gen**.
3. Нажмите на название поиска, чтобы открыть его.
4. Скопируйте поиск из поля **Search**.
5. Откройте страницу **Search**.
6. Вставьте поиск и удалите макрос 'output\_\*'. Например, измените | 'asset\_sources' | 'make\_assets\_cidr' | 'output\_assets("SA-IdentityManagement", "assets\_by\_cidr.csv")' на | 'asset\_sources' | 'make\_assets\_cidr'.
7. Запустите поиск.
8. Повторите шаги 2-7 для двух других поисковых запросов, **Identity – Asset String Matches – Lookup Gen** и **Identity – Identity Matches – Lookup Gen**.

**Настройка процесса объединения цифровых объектов и идентификаторов в Splunk Enterprise Security**

Вы можете изменить сохраненные поисковые запросы, которые осуществляют процесс объединения цифровых объектов и идентификаторов, для дополнительного преобразования полей или очистки данных. Добавьте любые операции, которые хотите изменить в процессе объединения, в поиск перед макросом 'output\_\*'.

Некоторые изменения сохраненных поисковых запросов не поддерживаются и могут нарушить процесс объединения или корреляцию цифровых объектов и идентификаторов.

* Не добавляйте и не удаляйте поля из данных выхода.
* Не меняйте расположение данных выхода на другую таблицу справочника или собрание KV store.
* Не заменяйте макрос 'output\_\*' командой outputlookup.

**Изменение справочников цифровых объектов и идентификаторов в Splunk Enterprise Security**

Внесите изменения в справочники цифровых объектов и идентификаторов в Splunk Enterprise Security для добавления новых цифровых объектов или идентификаторов или изменения существующих значений в таблицах справочников. Вы также можете отключить или включить существующие справочники.

**Редактирование справочников цифровых объектов и идентификаторов**

Отредактируйте справочники цифровых объектов и идентификаторов в панели мониторинга Управление идентификатором (Identity Management).

1. Выберите в Enterprise Security **Configure > Data Enrichment > Identity Management**.
2. Найдите имя списка цифровых объектов или идентификаторов, который вы хотите отредактировать, и нажмите **Source**. Список открывается в интерактивном редакторе.
3. Используйте полосы прокрутки для просмотра столбцов и строк в таблице. Дважды щелкните по ячейке для добавления, изменения или удаления ее содержимого.
4. Нажмите **Save**, когда закончите.

Изменения, внесенные в список цифровых объектов или идентификаторов, будут отражаться в результатах поиска после следующего запланированного объединения. См. раздел «Как Splunk Enterprise Security обрабатывает и объединяет данные об цифровых объектах и идентификаторах».

**Отключение или включение справочников цифровых объектов и идентификаторов**

Отключите или включите данные ввода справочника цифровых объектов и идентификаторов. Отключите ввод, чтобы предотвратить включение содержимого соответствующего списка в процесс объединения. Включите отключенный ввод, чтобы позволить связанному списку участвовать в следующем запланированном объединении данных об цифровых объектах или идентификаторах. Отключение ввода не удаляет данные из соответствующего справочника в Splunk Enterprise Security.

1. Выберите в Enterprise Security **Configure > Data Enrichment > Identity Management**.
2. Найдите справочник цифровых объектов или идентификаторов, который хотите отключить.
3. Нажмите **Отключить (Disable)** или **Включить (Enable)**.

Начиная с версии 5.0.0, ввода данных справочников цифровых объектов и идентификаторов отключен по умолчанию после установки. Локальные настройки соблюдаются после обновления.

***Отключение демо-версий справочников цифровых объектов и идентификаторов***

Демо-версии справочников цифровых объектов и идентификаторов отключены по умолчанию. Отключите демо-версии справочников цифровых объектов и идентификаторов, чтобы предотвратить добавление демо-данных к основным справочникам цифровых объектов и идентификаторов, используемых Splunk Enterprise Security для корреляции цифровых объектов и идентификаторов. После того, как вы отключите демо-данные справочников, сохраненные поисковые запросы обновят основные справочники цифровых объектов и идентификаторов и удалят из основных справочников данные из отключенных справочников.

1. Выберите в Enterprise Security **Configure > Data Enrichment > Identity Management**.
2. Найдите справочники demo\_assets и demo\_identities.
3. Нажмите **Отключить (Disable)** для каждого из них.

**Включение или исключение справочников цифровых объектов или идентификаторов из репликации пакетов**

Начиная с версии 4.7.0, исходные файлы справочников цифровых объектов и идентификаторов по умолчанию исключаются из репликации пакетов в кластере индексатора. Файлы объединенных справочников остаются включенными в репликацию пакетов для поддержки корреляции цифровых объектов и идентификаторов. См. раздел «Справочники, в которых хранятся объединенные данные об цифровых объектах и идентификаторах в Splunk Enterprise Security», для получения информации о файлах справочников, которые остаются включенными в репликацию пакетов.

Изменение значения по умолчанию для включения файлов справочников цифровых объектов и идентификаторов в репликацию пакетов может снизить производительность системы.

1. Выберите в Enterprise Security **Configure > Data Enrichment > Identity Management**.
2. Выберите справочник, который вы хотите включить или исключить из репликации пакета.
3. Установите или снимите флажок с ячейки **Черный список (Blacklist)**. Если флажок установлен, файл справочника исключается из репликации пакета.

Вы можете внести это изменение только в том случае, если для параметра «Включить автоматическое обновление генерации идентификатора» («Enable Identity Generation Autoupdate») установлено значение «истина» («true»). См. раздел «Настройка общих параметров для Splunk Enterprise Security».

**Примеры методов добавления данных об цифровых объектах и идентификаторах в Splunk Enterprise Security**

Описанные в примерах методы включают в себя некоторые распространенные способы добавления данных об цифровых объектах и идентификаторах в Splunk Enterprise Security. Вы можете обратиться к Splunk Professional Services, чтобы найти лучшее решение для вашей среды.

**Добавление данных об цифровых объектах и идентификаторах из Active Directory**

В этом примере описывается, как добавить данные об цифровых объектах и идентификаторах из Active Directory.

***Настройка Splunk Support для приложения Active Directory***

Собирайте данные об цифровых объектах и идентификаторах с помощью Splunk Support для приложения Active Directory. Информацию об установке и настройке приложения см. в разделе «Установка дополнения Splunk для Active Directory».

***Сбор данных об цифровых объектах и идентификаторах из Active Directory***

Соберите данные об цифровых объектах и идентификаторах из Active Directory, выполнив поиск данных в SA-ldapsearch.

1. Выполните шаги для настройки нового списка цифровых объектов или идентификаторов. См. раздел «Настройка нового списка цифровых объектов или идентификаторов в Splunk Enterprise Security».
2. Отключите файл справочника, который вы создали, до тех пор, пока не закончите настройку сохраненного поиска, чтобы не допустить объединения данных об цифровых объектах или идентификаторах с неполными или неточными данными. См. раздел «Отключение или включение справочников цифровых объектов и идентификаторов».
3. Создайте сохраненный поиск в SA-ldentityManagement, чтобы внести в табличный файл справочника команду idapsearch. Точный синтаксис этого поиска зависит от конфигурации вашей службы каталогов AD.

См. два примера в разделах «Пример поиска для сбора данных об идентификаторе из Active Directory» и «Пример поиска для сбора данных об цифровом объекте из Active Directory».

1. Протестируйте процесс объединения. См. раздел «Тестирование процесса объединения цифровых объектов и идентификаторов в Splunk Enterprise Security».

**Пример поиска для сбора данных об идентификаторе из Active Directory**

В этом примере поиска присваиваются статические значения для полей suffix, endDate, category, watchiist и priority. Используйте его в качестве руководства для создания и тестирования рабочего поиска, а затем замените статические значения информацией из вашей среды AD. Переименуйте справочник my.identrty.lookup, выбрав что-либо подходящее для вашей среды.

|ldapsearch domain=<domain\_name> search="(&(objectclass=user)(!(objectClass=computer)))" attrs="userAccountControl,sAMAccountName,personalTitle,displayName,givenName,sn,mail,telephoneNumber,mobile,manager,department,whenCreated,accountExpires"

|makemv userAccountControl

|search userAccountControl="NORMAL\_ACCOUNT"

|eval suffix=""

|eval priority="medium"

|eval category="normal"

|eval watchlist="false"

|eval endDate=""

|table sAMAccountName,personalTitle,displayName,givenName,sn,suffix,mail,telephoneNumber,mobile,manager,priority,department,category,watchlist,whenCreated,endDate

|rename sAMAccountName as identity, personalTitle as prefix, displayName as nick, givenName as first, sn as last, mail as email, telephoneNumber as phone, mobile as phone2, manager as managedBy, department as bunit, whenCreated as startDate

|outputlookup my\_identity\_lookup

**Пример поиска для сбора данных об идентификаторе из Active Directory**

В этом примере поиска присваиваются статические значения для нескольких полей. Используйте его в качестве руководства для создания и тестирования рабочего поиска, а затем замените статические значения информацией из вашей среды AD. Переименуйте справочник my.asset.lookup, выбрав что-либо подходящее для вашей среды.

|ldapsearch domain=<domain name> search="(&(objectClass=computer))"

|eval city=""

|eval country=""

|eval priority="medium"

|eval category="normal"

|eval dns=dNSHostName

|eval owner=managedBy

|rex field=sAMAccountName mode=sed "s/\$//g"

|eval nt\_host=sAMAccountName

|makemv delim="," dn

|rex field=dn "(OU|CN)\=(?<bunit>.+)"

|table ip,mac,nt\_host,dns,owner,priority,lat,long,city,country,bunit,category,pci\_domain,is\_expected,should\_timesync,should\_update,requires\_av

| outputlookup create\_empty=false createinapp=true my\_asset\_lookup

**Добавление данных об цифровых объектах из индексированных событий на платформе Splunk**

В этом примере показано, как идентифицировать хосты, отображающиеся в индексированных событиях, которые в настоящее время не связаны с существующими данными об цифровых объектах, и добавить эти хосты в ваш справочник цифровых объектов.

Используйте этот пример для сравнения хостов, взаимодействующих с платформой Splunk, с набором существующих данных об цифровых объектах и обзором таблицы несовпадающих хостов. Затем вы можете экспортировать таблицу как список цифровых объектов.

| `host\_eventcount`

| search host\_is\_expected=false NOT host\_asset\_id=\*

| fields - firstTime,recentTime,lastTime,\_time, host\_owner\_\*,host\_asset\_tag,host\_asset\_id

| sort -totalCount,dayDiff

| table host,ip,mac,nt\_host,dns,owner,priority,lat,long,city,country,bunit,category,pci\_domain,is\_expected,should\_timesync,should\_update,requires\_av

**Добавление новых данных об цифровых объектах или идентификаторах вручную**

Добавьте новые данные об цифровом объекте или идентификаторе в Splunk Enterprise Security вручную, отредактировав справочник цифровых объектов или идентификаторов. Например, добавьте внутренние подсети, IP-адреса, которые должны быть включены в белый список, и другие статические данные об цифровых объектах и идентификаторах.

1. В строке меню Splunk ES выберите **Configure > Content Management**.
2. Чтобы добавить данные об цифровых объектах, нажмите на справочник **Цифровых объектов (Assets)**, чтобы изменить его. Чтобы добавить данные об идентификаторе, нажмите на список **Идентификаторы (Identities)**, чтобы изменить его.
3. Используйте полосы прокрутки для просмотра столбцов и строк в таблице. Дважды щелкните по ячейке, чтобы добавить, изменить или удалить ее содержимое.
4. Сохраните изменения.

**Анализ угроз**

**Добавление анализа угроз в вашу систему Splunk Enterprise Security (ES)**

В качестве администратора системы ES вы можете коррелировать показатели подозрительной активности, известные либо потенциальные угрозы с событиями у вас, добавив анализы угроз в вашу систему Splunk Enterprise Security. Добавление анализа угроз увеличивает возможности аналитиков по мониторингу безопасности и добавляет контекстный идентификатор к их исследованиям.

Система Splunk Enterprise Security предоставляет выбор источников анализа угроз. Система Splunk Enterprise Security также поддерживает различные типы анализа угроз, что дает возможность сделать свой выбор.

Администраторы системы ES могут добавить анализ угроз в систему Splunk Enterprise Security, скачав поток из сети Интернет, загрузив структурный файл либо внедрив анализ угроз напрямую из событий системы Splunk Enterprise Security.

**Предварительные условия**

Ознакомьтесь с типами технологии анализа угроз, которые предоставляет система Splunk Enterprise Security. См. раздел Поддерживаемые типы анализа угроз в системе Splunk Enterprise Security.

**Шаги**

1. Конфигурация источников анализа угроз, включенных в систему Splunk Enterprise Security.
2. Для добавления любого дополнительного источника анализа угроз, не включенного в систему Splunk Enterprise Security следуйте правилам добавления анализа угроз, который соответствует источнику и формату анализа, который вы хотите добавить.

* Скачайте анализ угроз из сети Интернет
* Загрузите структурный файл анализа угроз STIX или OpenIOC
* Загрузите пользовательский файл анализа угроз CSV
* Добавьте анализ угроз из событий Splunk в системе Splunk Enterprise Security
* Добавьте и сохраняйте анализ угроз локально в системе Splunk Enterprise Security
* Добавьте анализ угроз с пользовательским файлом справочника в систему Splunk Enterprise Security

1. Убедитесь, что вы успешно добавили анализ угроз в систему Splunk Enterprise Security.

**См. также**

Замена существующего анализа угроз в системе Splunk Enterprise Security

Добавление анализа угроз с адаптивным ответным действием.

Упоминание интерфейса анализа угроз в *потоке протокола REST API*

Структура анализа угроз в системе Splunk ES на портале разработчика Splunk

**Поддерживаемые типы анализа угроз в системе Splunk Enterprise Security**

Система Splunk Enterprise Security поддерживает несколько типов анализа угроз. Поддерживаемые типы анализа угроз соответствуют коллекциям хранилища KV Store, где хранится анализ угроз.

Модульный ввод программы управления анализом угроз проводит анализ скачанных и загруженных файлов и задает индикаторы этим коллекциям. Файлы могут содержать любое сочетание индикаторов.

|  |  |  |  |
| --- | --- | --- | --- |
| **Группа угроз в KV Store** | **Поддерживаемые типы данных IOC** | **Локальный файл справочника** | **Необходимые заголовки в поисковом файле** |
| certificate\_intel | X509  Certificates | Local Certificate Intel | certificate\_issuer,  certificate\_subject,  certificate\_issuer\_organization,  certificate\_serial,  certificate\_issuer\_unit,  certificate\_subject\_unit,  description, weight |
| email\_intel | Email | Local Email Intel | description, scr\_user, subject, weight |
| file\_intel | Названия или хеши файлов | Local File Intel | description, src\_user, subject, weight |
| http\_intel | URLs |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | Local HTTP Intel | description, http\_referrer, http\_user\_agent, url, weight |
| ip\_intel | IP адреса | Local IP Intel | description, ip, weight |
| Домены | Local Domain Intel | description, domain, weight |
| process\_intel | Процессы | Local Process Intel | Description, process, process\_file\_name, weight |
| registry\_intel | Записи реестра | Local Registry Intel | description, registry\_path, registry\_value\_name, registry\_value\_text, weight |
| service\_intel | Сервисы | Local Service Intel | description, service, service\_file\_hash, service\_dll\_file\_hash, weight |
| user\_intel | Пользователи | Local User Intel | description, user, weight |

Файл collections.conf в подкаталоге DA-ESS-Threatntelligence содержит перечень коллекций хранилища KV Store.

**Конфигурация источника анализа, включенного в систему Splunk Enterprise Security**

Система Splunk Enterprise Security включает в себя несколько источников анализа, которые проводят выборку информации по всей сети Интернет.

Данные источники анализа по умолчанию не активны. Изучите типы анализа, предоставляемые источниками, и решите, является ли включенный анализ полезным для вашей команды перед активированием специальных источников.

**Предварительные условия**

* Ваша система Splunk Enterprise Security должна быть подключена к сети Интернет. Если система не подключена к сети Интернет, следует деактивировать данные источники либо использовать информацию из них альтернативным способом.
* Для установки правил брандмауэра для данных источников вы вероятно захотите использовать прокси сервер для получения анализа перед тем, как пересылать его в систему Splunk Enterprise

Security и позволить IP адресам прокси сервера получить доступ к системе Splunk Enterprise Security. IP адреса для данных источников могут быть изменены.

**Шаги**

1. В главном меню системы Enterprise Security выберите **Configure> Date Enrichment> Intelligence Downloads.**
2. В разделе **Description** отображаются все определенные источники анализа, в нем можно узнать больше о типах информации или индикаторах угроз, которые могут соотносится с вашими событиями.
3. Активируйте источники анализа, которые подходят вашей модели внедрения безопасности.
4. Настройте активированные источники анализа, которые подходят вашей модели внедрения безопасности, используя ссылки на вебсайты источника для обзора документации, предоставленной провайдером источника. Каждый вебсайт источника предлагает рекомендации относительно интервалов опроса и других требований конфигурации отдельно от системы Splunk Enterprise Security.

Система Splunk Enterprise Security рассчитывает получить от всех источников анализа тщательным образом отформатированные данные и ценную аналитическую информацию. Поставщики потоков несут ответственность за вредоносные данные либо ложные результаты, которые могут быть приняты в вашей среде за результат.

Если вы установили, что ваша система Splunk Enterprise Security получает данные от случайных IP адресов, используйте функцию WHOIU или nslookup, чтобы определить, соответствует ли IP адрес одному из источников анализа, установленных в вашей среде.

**Следующий шаг**

Чтобы добавить пользовательский источник анализа, см. раздел Добавление анализа угроз в вашу систему Splunk Enterprise Security и перейдите по ссылке, которая соответствует источнику, который вы хотите добавить.

После добавления источников анализа см. раздел Убедитесь, что вы успешно добавили анализ в систему Splunk Enterprise Security.

**Включенные источники анализа угроз**

Источники анализа угроз разделены по индикаторам угроз и добавлены в соответствующие коллекции хранилища KV Store.

|  |  |  |
| --- | --- | --- |
| **Источник угроз** | **Поставщик списка угроз** | **Вебсайт источника угроз** |
| Возникающие угрозы взломанного черного списка IP | Возникающие угрозы | http://rules.emergingthreats.net/blockrules |
| Возникающие угрозы правил брандмауэра IP | Возникающие угрозы | http://rules.emergingthreats.net/fwrules |
| Список вредоносных доменов | Hail a TAXII.com | http://hailataxi.com |
| iblocklist Logmein | I-blocklist | http://iblocklist.com/lists |
| iblocklist Piratebay | I-blocklist | http://iblocklist.com/lists |
| Iblocklist Proxy | I-blocklist | http://iblocklist.com/lists |
| Iblocklist Rapidshare | I-blocklist | http://iblocklist.com/lists |
| Iblocklist Spyware | I-blocklist | http://iblocklist.com/lists |
| Iblocklist Tor | I-blocklist | http://iblocklist.com/lists |
| Iblocklist Wen attacker | I-blocklist | http://iblocklist.com/lists |
| Черный список вредоносного домена | Вредоносные домены | http://mirror1.nalwaredomains.com |
| abuse.ch Palevo C&C IP черный список | abuse.ch | http://palevotracker.abuse.ch |
| Phishtank Database | Phishtank | http://www.phishtank.com |
| SANS черный список | SANS | http://isc.sans.edu |
| abuse.ch ZeuS черный список (только неверные IP) | abuse.ch | http://zeustracker.abuse.ch |
| abuse.ch ZeuS черный список (стандартный) | abuse.ch | http://zeustracker.abuse.ch |

**Включенные универсальные источники анализа**

Система Splunk Enterprise Security также включает в себя универсальный анализ, который не включен в коллекции анализа угроз хранилища KV Store, а используется для углубления информации в системе Splunk Enterprise Security.

|  |  |  |
| --- | --- | --- |
| **Список данных** | **Поставщик данных** | **Вебсайт поставщика данных** |
| Alexa Top 1 Million Sites | Alexa Internet | http://www.alexa.com/topsites |
| ICANN Top-level Domains List | IANA | http://iana.org/domains/root/db |
| MaxMind GeoIP ASN IPv4 database | MaxMind | http://dev.maxmind.com/geoip/geoip2/geoip2-anonymous-ip-csv-database |
| MaxMind GeoIP ASN IPv6 database | MaxMind | http://dev.maxmind.com/geoip/geoip2/geoip2-anonymous-ip-csv-database |
| Mozilla Public Suffix List | Mozilla | http://publicsuffix.org |

**Скачайте поток анализа угроз из сети Интернет в систему Splunk Enterprise Security**

Система Splunk Enterprise Security может периодически скачивать поток анализа угроз, доступный в сети Интернет, проводить его анализ и добавлять в соответствующие коллекции хранилища KC Store.

1. (Опционально) Конфигурация прокси для получения анализа угроз.
2. Следуйте процедуре, которая соответствует формату источника угроз:

* Добавления источника угроз на основе URL
* Добавление потока TAXII

**Конфигурация прокси для получения анализа угроз**

Если вы используете прокси сервер для отправки анализа угроз в систему Splunk Enterprise Security, установите прокси опции для такого источника угроз.

Пользователь должен соответствовать имени сохраненных учетных данных в системе безопасности Splunk в

системе управления учетными данными. Если вы удалите существующего пользователя прокси в системе редактора настроек загрузки анализа, процесс загрузки больше не будет соотносится с сохраненными учетными данными. Удаление ссылки на учетные данные не удаляет сами сохраненные данные из системы управления учётными данными. См. раздел Управление учетными данными в системе Splunk Enterprise Security.

1. В главном меню системы Enterprise Security выберите **Configure> Data Enrichment> Intelligence Downloads.**
2. Выберите источник загрузки угроз или добавьте новый источник загрузки угроз. См. раздел Добавление источника угроз на основе URL или Добавление потока TAXII.
3. Конфигурация опции прокси.
4. Введите адрес прокси сервера. Прокси сервер не может иметь вид URL. К примеру, 10.10.10.10. либо server.example.com.
5. Введите порт прокси сервера для получения доступа к адресу прокси сервера.
6. Введите данные входа пользователя прокси для прокси сервера. Поддерживаются только основные методы и дайджест-аутентификация.
7. Сохраните изменения.

**Добавление источника угроз на основе URL**

Добавьте источник анализа отличный от TAXII, доступный по ссылке URL в сети Интернет. В качестве примера добавления источника анализа угроз на основе URL см. Пример: Добавление потока угроз программ-вымогателей в систему Splunk Enterprise Security.

1. В главном меню системы Enterprise Security выберите **Configure> Data Enrichment> Intelligence Downloads.**
2. Нажмите кнопку **New** для добавления нового источника анализа.
3. Заполните поле **Name** для загрузки угрозы. Название может содержать только буквенно-цифровые символы, дефисы и подчеркивания. Название не может содержать пробелы.
4. Выберите или снимите выделение для опции **Is Threat Intelligence**.
5. (Опционально) Выберите или снимите выделение для опции **Sinkhole**. Выберите окошко для удаления загруженного файла после его обработки.
6. Заполните поле **Type** для загрузки угрозы. Тип определяет тип индикатора угрозы, содержащейся в потоке.
7. Заполните поле **Description**. Опишите индикаторы данного потока угрозы.
8. Введите значение в поле **Weight** для индикаторов угрозы. Система Splunk Enterprise Security использует значение потока угрозы для подсчета шкалы риска цифровых объектов или идентификаторов, связанных с индикатором в потоке угроз. Высокое значение указывает на повышенную необходимость или увеличенный риск для вашей среды.
9. (Опционально) Измените опцию загрузки по умолчанию **Interval** для данного потока угрозы. Значения по умолчанию: 43200 секунд либо каждые 12 часов.
10. (Опционально) Заполните поле POST аргументы для данного потока угроз.
11. (Опционально) Заполните поле **Maximum age** для определения срока хранения для данного источника угроз, определенный в относительном времени. Активируйте соответствующие сохраненные поиски, чтобы данная настройка начала действовать. См. раздел Конфигурация срока хранения источника угроз.

К примеру, - 7d. В случае если срок последнего обновления потока превышает максимальный срок, определенный данной настройкой, модульный ввод технологии анализа угроз удаляет данные из коллекции угрозы.

1. (Опционально) Если вам необходимо установить пользовательскую строку **User agent**, чтобы обойти контроль безопасности сети в вашей среде, заполните ее в таком формате <user-agent> /<version>. К примеру, Mozilla/5.0 или AppleWebkit/602.3.12. Значение этого поля должно соответствовать данному регексу: ([A-Za-z0-9\_. -1+]/([A-Za-z0-9\_.-]+). Сверьте данные с вашим администратором устройства безопасности, чтобы убедиться, что строку, которую вы вводите здесь, принимает контроль безопасности вашей сети.
2. Заполните поля **Parsing Options**, чтобы убедиться, что ваш список угроз успешно обрабатывается. Следует вводить либо ограничивающее регулярное выражение, либо извлекающее. Нельзя оставлять оба поля пустыми.

|  |  |  |
| --- | --- | --- |
| **Поле** | **Описание** | **Пример** |
| Ограничивающее регулярное выражение | Строка регулярного выражения, используемая для разделения или извлечения строк в источнике анализа. Для сложных разделителей данных используйте ограничивающее регулярное выражение. | , or: or \ t |
| Извлекающее регулярное выражение | Регулярное выражение, используемое для извлечения полей из индивидуальных строк документа источника угроз. Используется для извлечения значений в источнике угроз. | ^(\S+) \t+(S+)\t+\S+\t+\S+\t\*(\S\*) |
| Поля | Необходимы, если ваш документ содержит заданные строки. Строки полей, отделенные запятыми, извлекаются из списка угроз. Также могут быть использованы для переименования или объединения полей. Поле Description является обязательным. Дополнительные допустимые поля – это поля в соответствующей коллекции хранилища KV Store для данного анализа угроз, видимой в локальных файлах справочника или файле DA-ESS-ThreatIntelligence/collections.conf. По умолчанию установлены следующие значения: description:$1, ip:$2. | <fieldname>:$<number>, <fieldname>.$<number>  ip:$1, descriptiom:domain\_blocklist |
| Пропускающее регулярное выражение | Регулярное выражение, используемое для пропуска строк в источнике угроз. Значения по умолчанию для пропускающих пустых строк и комментариев начинается со знака #. | ^\s\*$ |
| Пропуск строк заголовка | Количество строк заголовка, которые необходимо пропустить при обработке источника угроз. | () |

|  |  |  |
| --- | --- | --- |
| Кодирование файлов анализа | Если кодирование файлов отличается от ASCII или UTF8, укажите тип кодирования здесь. Либо оставьте поле пустым. | latin1 |

1. (Опционально) Измените поля **Download Options**, чтобы убедиться, что ваш список угроз успешно скачивается.

|  |  |  |
| --- | --- | --- |
| **Поле** | **Описание** | **Пример** |
| Время до повтора | Количество секунд ожидания между повторными попытками скачивания. Перед изменением заданного времени повтора ознакомьтесь с рекомендованным интервалом опроса провайдера источника угроз. | 60 |
| Пользователь удаленной площадки | Имя пользователя, которое используется для удаленной авторизации, при необходимости. Имя пользователя, которое вы добавляете в данное поле, должно соответствовать имени учетных данных в системе Управления учетными данными. См. раздел Управление учетными данными в системе Splunk Enterprise Security. | админ |
| Повторные попытки | Максимальное количество попыток повтора | 3 |
| Тайм-аут | Количество секунд ожидания перед признанием попытки скачивания неудачной. | 30 |

1. (Опционально) Если вы используете прокси сервер, заполните поле **Proxy Options** для потока угроз. См. раздел Конфигурация прокси для получения анализа угроз.
2. Сохраните изменения.

**Следующий шаг**

Чтобы добавить еще один пользовательский источник угроз, см. раздел Добавление анализа угроз в систему Splunk Enterprise Security и перейдите по ссылке, которая соответствует источнику, который вы хотите добавить.  
После добавления источников анализа угроз см. раздел Удостоверьтесь, что вы успешно добавили анализ угроз в систему Splunk Enterprise Security.

**Добавление потока TAXII**

Добавьте анализу угроз, предоставляемый в качестве потока TAXII в систему Splunk Enterprise Security.

**Предварительные условия**

Определите, требует ли поток TAXII проверки подлинности сертификата. Если требует, добавьте сертификат и ключи в тот же раздел приложения, в который вы определили

поток TAXII. К примеру, DA-ESS-ThreatIntelligence.

1. Следуйте инструкциям по добавлению нового сертификата в систему Splunk Enterprise Security, чтобы добавить сертификат и файлы закрытого ключа. См. раздел Управление учетными данными в системе Splunk Enterprise Security.
2. Следуйте инструкциям по добавлению потока TAXII в систему Splunk Enterprise Security, используя параметры POST cert\_file и key\_file для обозначения файловых имен сертификата и файла закрытого ключа.

**Шаги**

1. В главном меню системы Enterprise Security выберите **Configure> Data Enrichment> Intelligence Downloads.**
2. Нажмите кнопку **New** для добавления нового потока TAXII.
3. Заполните поле **Name** для потока анализа угроз.
4. Отметьте опцию **Is Threat Intelligence**.
5. (Опционально) Выберите или снимите выделение для опции **Sinkhole**. Выберите окошко для удаления загруженного файла после его обработки.
6. Заполните поле **Type** of **taxii**.
7. Заполните поле **Description** для потока анализа угроз.
8. Введите ссылку URL для загрузки потока TAXII.
9. (Опционально) Измените значение по умолчанию в поле **Weight** для потока анализа угроз. Увеличьте значение, если угрозы в потоке угроз представляют собой высокодостоверные и вредоносные угрозы, которые увеличивают шкалу риска для цифровых объектов или идентификаторов, которые взаимодействуют с индикаторами из источника угроз.
10. (Опционально) Измените интервал загрузки анализа угроз. Значение по умолчанию: 43200 секунд либо дважды в день.
11. Введите **POST параметры** с разделителями-пробелами, заданные для TAXII, для потока анализа угроз.

<Post argument>=”<POST argument value>”

|  |  |  |
| --- | --- | --- |
| **Пример параметра POST** | **Описание** | **Пример** |
| collection | Имя коллекции данных из потока TAXII. | collection=”A\_TAXII\_Feed\_Name” |
| earliest | Первичные данные угроз, которые необходимо получить из потока TAXII. | Earliest=”-ly” |
| Taxi\_username | Дополнительный способ обеспечения имени пользователя потока TAXII. | taxi\_username=”user” |

|  |  |  |
| --- | --- | --- |
| taxi\_password | Дополнительный способ обеспечения пароля потока TAXII. Если вы предоставляете имя пользователя без предоставления пароля, модульный ввод анализа угроз попытается найти пароль в системе управления учетными данными. См. раздел Управление учетными данными в системе Splunk Enterprise Security. | taxii\_password=”password” |
| cert\_file | Добавьте имя сертификата файла, если поток TAXII использует проверку подлинности сертификата. Имя файла должно точно соответствовать, оно чувствительно к регистру. | cert\_file=”cert.crt” |
| key\_file | Добавьте имя ключевого файла для сертификата, если поток TAXII использует проверку подлинности сертификата. Имя файла должно точно соответствовать, оно чувствительно к регистру. | key\_file=”cert.key” |

1. Поток TAXII не использует настройку **Maximum age**. Для настройки хранения файлов TAXII см. раздел Конфигурация срока хранения файла угроз.
2. Поток TAXII не использует настройку **User agent**.
3. Поток TAXII не использует настройку **Parsing Options**.
4. (Опционально) Измените настройки **Download Options**.
5. (Опционально) Измените настройки **Proxy Options**. См. раздел Конфигурация прокси для получения анализа угроз.
6. Сохраните изменения.

Вы не можете воспользоваться аутентифицированным прокси с потоком TAXII, поскольку библиотека libtaxii, используемая системой Enterprise Security, не поддерживает такие аутентифицированные прокси. При возможности, взамен используйте неаутентифицированный прокси.

**Следующий шаг**

Чтобы добавить еще один пользовательский источник угроз, см. раздел Добавление анализа угроз в систему Splunk Enterprise Security и перейдите по ссылке, которая соответствует источнику, который вы хотите добавить.

После добавления источников анализа угроз см. раздел Удостоверьтесь, что вы успешно добавили анализ угроз в систему Splunk Enterprise Security.

**Загрузите структурный файл анализа угроз STIX или OpenIOC в систему Splunk Enterprise Security**

Загрузите анализ угроз в файле STIX или OpenIOC в систему Splunk Enterprise Security, используя один из указанных способов:

* Загрузка файла STIX или OpenIOC, используя интерфейс системы Splunk Enterprise Security
* Добавление файла STIX или OpenIOC, используя протокол REST API
* Добавление файла STIX или OpenIOC, используя файловую систему

**Загрузка файла STIX или OpenIOC, используя интерфейс системы Splunk Enterprise Security**

Система Splunk Enterprise Security поддерживает добавление файлов типа OpenIOC, STIX и CSV напрямую в интерфейс системы Splunk Enterprise Security.

1. В главном меню системы Enterprise Security выберите **Configure> Data Enrichment> Threat Intelligence Uploads.**
2. Введите имя файла для файла, который вы хотите загрузить. Имя файла, которое вы вводите будет задано в качестве имени файла, сохраненного в $SPLUNK\_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat\_intel.

Имя файла не может содержать пробелы или специальные символы.

1. Загрузите файлы формата OpenIOC или STIX.
2. Заполните поле **Weight** для файла анализа угроз. Значение файла анализа угроз увеличивает шкалу риска объектов, связанных с анализом угроз в данном списке.
3. (Опционально) Заполните поле **Threat Category**. Если вы оставите поле незаполненным, а категория определена в файле OpenIOC или STIX, система Splunk Enterprise Security будет использовать категорию, которая указана в файле.
4. (Опционально) Заполните поле **Threat Group**. Если вы оставите поле незаполненным, а группа определена в файле OpenIOC или STIX, система Splunk Enterprise Security будет использовать группу, которая указана в файле.
5. (Опционально) Отметьте опцию **Overwrite**. Если вы ранее загружали файл с таким же именем, выберите эту опцию, чтобы заменить предыдущую версию файла.
6. (Опционально) Отметьте опцию **Sinkhole**. Данная опция позволяет удалить файл после обработки анализа.
7. Нажмите кнопку **Save**.

**Следующий шаг**

Чтобы добавить еще один пользовательский источник угроз, см. раздел Добавление анализа угроз в систему Splunk Enterprise Security и перейдите по ссылке, которая соответствует источнику, который вы хотите добавить.

После добавления источников анализа угроз см. раздел Удостоверьтесь, что вы успешно добавили анализ угроз в систему Splunk Enterprise Security.

**Добавление файла STIX или OpenIOC, используя протокол REST API**

Протокол REST API системы Splunk Enterprise Security поддерживает загрузку файлов анализа угроз в формате OpenIOC, STIX или CSV. См. раздел Справочная информация о протоколе API технологии анализа угроз.

**Следующий шаг**

Чтобы добавить еще один пользовательский источник угроз, см. раздел Добавление анализа угроз в систему Splunk Enterprise Security и перейдите по ссылке, которая соответствует источнику, который вы хотите добавить.

После добавления источников анализа угроз см. раздел Удостоверьтесь, что вы успешно добавили анализ угроз в систему Splunk Enterprise Security.

**Добавление файла STIX или OpenIOC, используя файловую систему**

Вы также можете добавить анализ угроз в систему Splunk Enterprise Security, добавив должным образом отформатированный файл в папку системного файла.

1. Добавьте файл формата STIX с расширение .xml либо файл OpenIOC с расширением .ioc в

папку $SPLUNK\_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat\_intel для поискового блока в вашей системе Splunk Enterprise Security либо предоставьте доступ к данной директории файла в общем доступе подключенной локальной сети.

1. По умолчанию, модульный ввод da\_ess\_threat\_local обрабатывает такие файлы и места обнаружения анализа угроз в соответствующих коллекциях хранилища KV Store.
2. По умолчанию, после обработки анализа в файлах, модульный ввод удаляет файлы, поскольку включена опция Sinkhole.

***Изменение исходных настроек da\_ess\_threat\_local***

1. В главном меню системы Enterprise Security выберите **Configure> Data Enrichment> Threat Intelligence Management.**
2. Нажмите на модульный ввод da\_ess\_threat\_local.
3. Проверьте или измените настройки по желанию.

Не меняйте исходные данные da\_ess\_threat\_default.

***Настройка пользовательской папки и контроль вводных данных для источников угроз***

Вы также можете добавить анализ угроз в систему Splunk Enterprise Security, добавив должным образом отформатированный файл в директорию пользовательского файла. Директория файлов должна соответствовать пути $SPLUNK\_HOME/etc/apps/<app\_name>/local/data/<directory\_name>, вы также должны создать контроль вводных данных, чтобы контролировать эту файловую директорию для анализа угроз.

Создайте контроль вводных данных для источников угроз, чтобы добавить анализ угроз в папку, которая не контролируется модульным вводом **da\_ess\_threat\_local**.

1. В главном меню системы Enterprise Security выберите **Configure> Data Enrichment> Threat Intelligence Management.**
2. Нажмите кнопку **New**.
3. Введите подробное имя для модульного ввода. Имя не может содержать пробелы.
4. Задайте путь для хранилища файлов. Файловое хранилище должно быть указано в таком формате

$SPLUNK\_HOME/etc/apps/<app\_name>/local/data/<directory\_name>

1. (Опционально) Задайте максимальный размер файла в байтах.
2. (Опционально) Отметьте опцию **Sinkhole**. При выборе данной опции модульный ввод удаляет каждый файл в директории после его обработки.
3. (Опционально) Выберите опцию **Remove Unusable**. При выборе данной опции модульный ввод удаляет файл после его обработки, если он не актуальный для анализа угроз.
4. (Опционально) Введите число, которое будет использоваться как значение по умолчанию для всех документов анализа угроз, использованных в данной директории.

**Следующий шаг**

Чтобы добавить еще один пользовательский источник угроз, см. раздел Добавление анализа угроз в систему Splunk Enterprise Security и перейдите по ссылке, которая соответствует источнику, который вы хотите добавить.

После добавления источников анализа угроз см. раздел Удостоверьтесь, что вы успешно добавили анализ угроз в систему Splunk Enterprise Security.

**Загрузка пользовательского файла анализа угроз в формате CSV в систему Splunk Enterprise Security**

Вы можете добавить пользовательский файл анализа угроз в систему Splunk Enterprise Security.

**Предварительные условия**

Отформатируйте пользовательский файл CSV, добавив заголовки для каждого типа анализа в файле. Пользовательский файл может содержать различные типы анализа, но вам необходимо включить заголовки для каждой колонки в файле CSV. См. раздел Поддерживаемые типы анализа угроз в системе Splunk Enterprise Security для заголовков, соответствующих каждому типу анализа угроз.

Добавьте пользовательский файл в систему Splunk Enterprise Security.

1. В главном меню системы Enterprise Security выберите **Configure> Data Enrichment> Threat Intelligence Uploads.**
2. Задайте имя файла для файла, который вы хотите загрузить. Имя файла, которое вы вводите присваивается файлу, который хранится по пути

$SPLUNK\_HOME/etc/apps/DA-ESS-ThreatIntelligence/local/data/threat\_intel.

Имя файла не может содержать пробелы или специальные символы.

1. Загрузите файл формата CSV.
2. Заполните поле **Weight** для списка угроз. Значение файла угроз увеличивает шкалу риска объектов, связанных с анализом угроз в списке.
3. (Опционально) Заполните поле **Threat Category**.
4. (Опционально) Заполните поле **Threat Group**.
5. (Опционально) Выберите опцию **Overwrite**. Если ранее вы загружали файл с таким же именем, выберите эту опцию для перезаписи

предыдущей версии файла.

1. (Опционально) Выберите опцию **Sinkhole**. Данная опция позволяет удалить файл после обработки анализа с него.
2. Нажмите кнопку **Save**.

**Следующий шаг**

Чтобы добавить еще один пользовательский источник угроз, см. раздел Добавление анализа угроз в систему Splunk Enterprise Security и перейдите по ссылке, которая соответствует источнику, который вы хотите добавить.

После добавления источников анализа угроз см. раздел Удостоверьтесь, что вы успешно добавили анализ угроз в систему Splunk Enterprise Security.

**Добавление анализа угроз с событий Splunk в систему Splunk Enterprise Security**

Вы можете добавить анализ угроз с событий Splunk в локальные справочники анализа угроз.

1. Задайте поиск, который находит индикаторы угроз.
2. Добавьте в конец поиска | outputlookup local\_<threat intelligence type>\_intel append=t.

К примеру, задайте поиск, который находит список IP адресов, которые тестируют веб сервер на предмет степени защищенности и добавьте их в поиск local\_ip\_intel для обработки модульным вводом и которые включены в коллекцию KV Store ip\_intel.

**Следующий шаг**

Чтобы добавить еще один пользовательский источник угроз, см. раздел Добавление анализа угроз в систему Splunk Enterprise Security и перейдите по ссылке, которая соответствует источнику, который вы хотите добавить.

После добавления источников анализа угроз см. раздел Удостоверьтесь, что вы успешно добавили анализ угроз в систему Splunk Enterprise Security.

**Добавление и мониторинг анализа угроз локально в системе Splunk Enterprise Security**

В каждой коллекции анализа угроз есть локальный файл справочника, который можно использовать для добавления анализа угроз вручную.

1. В главном меню системы Enterprise Security выберите **Configure> Content Management.**
2. Найдите файл справочника, который соответствует типу индикатора угроз, который вы хотите добавить. К примеру, **Local Certificate intel** для добавления информации и вредоносных или ложных сертификатов.
3. Нажмите на имя справочника для его редактирования.
4. Добавьте индикаторы в справочник. Нажмите правую кнопку мыши и выберите поле **Insert Row Below** для добавления новых строк, при необходимости.
5. (Опционально) Задайте цифровое значение для поля **Weight**, чтобы изменить шкалу риска для объектов, связанных с индикаторами для данного источника анализа угроз.
6. Нажмите кнопку **Save**.

**Следующий шаг**

Чтобы добавить еще один пользовательский источник угроз, см. раздел Добавление анализа угроз в систему Splunk Enterprise Security и перейдите по ссылке, которая соответствует источнику, который вы хотите добавить.

После добавления источников анализа угроз см. раздел Удостоверьтесь, что вы успешно добавили анализ угроз в систему Splunk Enterprise Security.

**Добавление анализа угроз с пользовательским файлом справочника в систему Splunk Enterprise Security**

Можно добавить анализ угроз в систему Splunk Enterprise Security в качестве пользовательского файла справочника. Добавьте файл справочника данным способом, если вы хотите отредактировать файл справочника в системе Splunk Enterprise Security. Если вы хотите добавить файл справочника, чтобы извлечь из него анализ единожды, взамен загрузите файл формата CSV. См. раздел Загрузка пользовательского файла анализа угроз в формате CSV в систему Splunk Enterprise Security.

Источник угроз на основании поиска может добавлять данные в любой из поддерживаемых типов анализа угроз, таких как файл или анализ IP. См. раздел Поддерживаемые типы анализа угроз в системе Splunk Enterprise Security.

**Предварительные условия**

Создайте пользовательский файл CSV. Пользовательский файл может содержать различные типы анализа, однако, вы можете включить заголовки для каждой колонки в CVS файле. См. раздел Поддерживаемые типы анализа угроз в системе Splunk Enterprise Security для заголовков, относящихся к каждому типу анализа угроз.

**Шаги**

Для начала, добавьте справочник в систему Splunk Enterprise Security.

1. Выберите поле **Configure> Content Management**.
2. Выберите поле **Create New Content> Lookup**.
3. Нажмите кнопку **Create New**.
4. Выберите поисковый файл для загрузки.
5. Выберите **App of SA-ThreatIntelligence**.
6. (Опционально) Измените имя файла. К примеру, задайте имя

threatindicatorszerodayattack.csv.

1. (Опционально) Измените имя определения. К примеру, задайте имя

zero\_day\_attack\_threat\_indicators\_list.

1. Оставьте тип справочника по умолчанию **Manual editing**.
2. Создайте ярлык для справочника. Ярлык отображается как имя для справочника на странице управления контентом. К примеру, Zero Day Threat Indicators.
3. Заполните описание для справочника. К примеру, индикаторы угроз, основанные на файлах от вредоносных атак нулевого дня.
4. Сохраните изменения.

Далее, добавьте вводную строку файла конфигурации источника угроз, которая соответствует файлу справочника, чтобы система ES могла провести анализ угроз.

1. Выберите **Configure> Data Enrichment> Intelligence Downloads**.
2. Нажмите кнопку **New**.
3. Заполните поле **Name**. Имя не может содержать пробелы. К примеру, zero\_day\_attack\_indicators.
4. Заполните поле **Type**. К примеру, zero\_day\_IOCs.
5. Заполните поле **Description**. К примеру, индикаторы угроз, основанные на файлах от вредоносных атак нулевого дня.
6. Введите URL, который относится к определению справочника, которое вы задали. К примеру, lookup://zero\_day\_attack\_threat\_indicators\_list.
7. (Опционально) Измените значение поля **Weight** по умолчанию для данных угроз.
8. (Опционально) Измените значение поле **Retry interval** по умолчанию для справочника.
9. Если ваш справочник содержит различные типы анализа угроз, введите заголовки в разделе **Fields**.
10. Сохраните изменения.

**Следующий шаг**

Чтобы добавить еще один пользовательский источник угроз, см. раздел Добавление анализа угроз в систему Splunk Enterprise Security и перейдите по ссылке, которая соответствует источнику, который вы хотите добавить.

После добавления источников анализа угроз см. раздел Удостоверьтесь, что вы успешно добавили анализ угроз в систему Splunk Enterprise Security.

**Удостоверьтесь, что вы успешно добавили анализ угроз в систему Splunk Enterprise Security**

После добавления новых источников анализа или конфигурации уже включенных источников анализа, удостоверьтесь, что анализ проводится успешно и что индикаторы угроз были добавлены в коллекции анализа угроз хранилища KV Store. Модульный ввод, ответственный за проведение анализа, срабатывает каждые 60 секунд.

Удостоверьтесь, что скачивание источника анализа началось

Данная процедура проверки актуальна только для источников на основе URL и потоков TAXII.

1. Из главного меню системы Enterprise Security выберите раздел **Audit> Threat Intelligence Audit**.
2. Найдите источник анализа и убедитесь, что в колонке **download\_status** указано **threat list downloaded**.
3. Проверьте раздел **Intelligence Audit Events**, чтобы убедиться в отсутствии ошибок, связанных с названием справочника.

Если попытка скачивания провалилась, попробуйте скачать напрямую из терминала сервера Splunk, используя утилиту curl или wget. Если источник анализа можно успешно скачать, используя одну из этих утилитов, но не удается скачать из системы Splunk Enterprise Security, обратитесь к вашему системному администратору, возможно, вам нужно указать пользовательскую строку пользователя для обхода средств контроля безопасности сети в вашей среде. См. шаг 10 в разделе Добавление источника угроз на основе URL.

**Удостоверьтесь, что индикаторы угроз существуют в коллекциях угроз**

Что касается источников анализа угроз, следует убедиться, что анализ угроз успешно проводится, а индикаторы угроз находятся в коллекциях угроз.

1. Выберите раздел **Security Intelligence> Threat Intelligence> Threat Artifacts**.
2. Введите в поиск имя источника в поле **Intel Source ID.**
3. Убедитесь, что для данного источника угроз определены индикаторы угроз.

**Устранение ошибок анализа**

Проверьте нижеуказанные файлы журнала, чтобы устранить ошибки, которые могут возникнуть при проведении анализа источников анализа с целью добавления их в систему Enterprise Security.

|  |  |
| --- | --- |
| **Проблема** | **Решение** |
| Вопросы, связанные со скачиванием источников анализа. | Проверьте табло Intelligence Audit Events на панели Threat Intelligence Audit. Необходимо найти события из файла threatlist.log исходным типом threatintel:download. |
| Вопросы, связанные с проведением анализа или обработкой. | Проверьте табло Intelligence Audit Events на панели. Threat Intelligence Audit. Необходимо найти события из файла threat\_intelligence\_manager.log исходным типом threatintel:manager. |
| Ошибки, связанные с загрузкой файла. | Проверьте файл threat\_intel\_file\_upload\_rest\_handler.log. |
| Другие ошибки, связанные с проведением анализа. | Убедитесь, что модульные вводы функционируют корректно. Проверьте файл python\_modular\_input.log на предмет ошибок, связанных с неудачными попытками модульного ввода. |

**Изменение существующего анализа в системе Splunk Enterprise Security**

После добавления анализа в систему Splunk Enterprise Security вы можете изменить настройки, чтобы убедиться, что анализ, который вы коррелируете с событиями, приносит пользу.

**Деактивация источника анализа**

Деактивируйте источник анализа, чтобы остановить скачивание информации из источника.

Новые индикаторы угроз перестанут добавляться в коллекции анализа угроз.

1. В главном меню систему Enterprise Security выберите **Configure> Data Enrichment> Intelligence Downloads**.
2. Найдите источник анализа.
3. Под строкой **Status** нажмите кнопку **Disable**.

**Деактивация персональных выходных файлов угроз**

Для того, чтобы персональные выходные файлы угроз не создавали значимых событий при соответствии с вашей средой, деактивируйте опцию персональных выходных файлов угроз. Если у вас есть доступ командной строки к заголовку поиска в системе Splunk Enterprise Security, вы можете деактивировать выходные файлы угроз, используя протокол REST API. См. справочную информацию о протоколе API анализа угроз в системе Splunk Enterprise Security *СПРАВОЧНАЯ ИНФОРМАЦИЯ О ПРОТОКОЛЕ* *REST API.*

**Редактирование источника анализа**

Измените информацию о существующем источнике анализа, такую как срок хранения или интервал скачивания для данного источника.

1. В главном меню систему Enterprise Security выберите **Configure> Data Enrichment> Intelligence Downloads**.
2. Нажмите на имя источника анализа, который вы хотите редактировать.
3. Внесите изменения в необходимые поля.
4. Сохраните изменения.

По умолчанию, редактировать источники анализа могут только администраторы. Для того, чтобы пользователи, не являющиеся администраторами, могли редактировать источники анализа, см. Добавление возможностей роли в разделе Руководство по установке и обновлению.

**Настройка срока хранения источника угроз**

Удалите анализу угроз из коллекции хранилища KV Store в системе Splunk Enterprise Security согласно дате, когда анализ угроз была добавлена в систему Splunk Enterprise Security.

1. Если источник анализа угроз не является потоком TAXII, определите ее максимальный срок хранения. Данное поле не заполняется для потоков TAXII.
2. В главном меню системы Enterprise Security выберите **Configure> Data Enrichment> Intelligence Downloads**.
3. Выберите источник анализа.
4. Измените настройку **Maximum age**, используя спецификатор относительного времени. К примеру, -7d или -30d.
5. Активируйте срок хранения поиска для коллекции.
6. В главном меню платформы Splunk, выберите **Settings** и нажмите поле **Searches, reports, and alerts**.
7. Используя поисковый фильтр задайте в поиск слово “срок хранения”.
8. Активируйте срок хранения поиска для коллекции, в которой располагается источник угроз. По умолчанию все сроки хранения поиска неактивны.

**Настройка срока хранения файла анализа угроз**

Определите, как долго должны храниться файлы в системе Splunk Enterprise Security после обработки. Модульные вводы, настроенные на странице Управление анализом угроз, занимаются разборкой файлов источников анализа. Измените настройки локальных модульных вводов, чтобы управлять суммарным сроком хранения файлов для источников анализа, либо измените персональные настройки для каждого скачивания или загрузки для более регулярного контроля срока хранения файлов.

Используйте нижеприведенную таблицу, чтобы определить условия, при которых система Splunk Enterprise Security будет удалять файлы после обработки. Для файлов, которые были добавлены в директорию при помощи скрипта, используйте опцию sinkhole модульного ввода.

|  |  |  |
| --- | --- | --- |
| **Опция sinkhole, заданная для модульного ввода** | **Опция sinkhole, заданная для персонального файла** | **Результат** |
| Неактивна | Неактивна | Файл не удален. |
| Неактивна | Активна | Файл удален. |
| Активна | Активна | Файл удален. |
| Активна | Неактивна | Файл удален. |

***Удаление файлов, управляемых особым модульным вводом***

Используйте опцию sinkhole или удалить неиспользуемые настройки, чтобы избирательно удалять файлы, управляемые модульным вводом.

1. В главном меню системы Enterprise Security выберите **Configure> Data Enrichment> Threat Intelligence Management**.
2. Выберите модульный ввод для настроек срока хранения файлов, который вы хотите изменить.
3. Для скачанных файлов выберите модульный ввод sa\_threat\_local.
4. Для загруженных файлов выберите модульный ввод da\_ess\_threat\_local.
5. Отметьте опцию **Sinkhole** для того, чтобы модульный ввод удалял каждый файл в директории после обработки.
6. Отметьте опцию **Remove Unusable**, чтобы модульный ввод удалял файл после обработки, если он не актуален для анализа.
7. Сохраните изменения.

***Удаление файлов, связанных с отдельными скачиваниями***

Используйте опцию sinkhole для удаления файлов, связанных со скачиванием анализа угроз.

1. В главном меню системы Enterprise Security выберите **Configure> Data Enrichment> Intelligence Downloads**.
2. Определите местоположение скачивания анализа угроз.
3. Отметьте опцию **Sinkhole**.
4. Сохраните изменения.

***Удаление файлов, связанных с отдельными загрузками***

При загрузке файлов выберите опцию sinkhole для их удаления после обработки.

* См. раздел Загрузка структурного файла анализа угроз формата STIX или OpenIOC в систему Splunk Enterprise Security.
* См. раздел Загрузка пользовательского файла анализа угроз формата CSV в систему Splunk Enterprise Security.

**Пример: Добавление вредоносного потока угроз в систему Splunk Enterprise Security.**

На данном примере показано, как добавлять список заблокированных доменов, в которых могут находиться вредоносные программы для системы Splunk Enterprise Security, чтобы лучше подготовить вашу организацию к атакам программ-вредителей. Поток, приведенный в примере, был взят с abuse.ch.

1. В главном меню системы Enterprise Security выберите **Configure> Data Enrichment> Intelligence Downloads**.
2. Нажмите кнопку **New**, чтобы добавить новый источник анализа угроз.
3. Заполните поле **Name of ransomware\_tracker**, чтобы описать источник скачивания угроз.
4. Заполните поле **Type of domain**, чтобы определить тип анализа угроз, содержащийся в данном источнике угроз.
5. Заполните поле **Description of Blocked domains that could host ransomware**.
6. В поле **URL** введите следующий адрес

http://ransomwaretracker.abuse.ch/downloads/RW\_DOMBL.txt.

1. (Опционально) Измените значение поля **Weight** по умолчанию с 1 на **2**, поскольку вредоносные программы представляют собой серьезную угрозу и вам понадобится экстра умножитель шкалы риска для активов либо идентификаторов, связанных с заблокированными вредоносными доменами.
2. Значение поля **Interval** оставьте по умолчанию 43200 секунд или каждые 12 часов.
3. Оставьте поле **POST arguments** незаполненным, поскольку данный тип потока не принимает аргументы POST.
4. Решите, стоит ли определять значение в поле **Maximum age** для анализа угроз. В соответствии с сайтом-трекером вредоносных программ, позиции в черном списке остаются в нем в течение 30 дней. Чтобы удалить позиции из черного списка в системе Enterprise Security раньше, установите максимальный срок хранения менее 30 дней. Введите значение в формате -7d.
5. Решите, стоит ли определять значение в строке User agent из-за средств контроля безопасности в вашей среде. Если нет, оставьте поле пустым.
6. Заполните поле **Delimiting regular expression** : по умолчанию, чтобы вы могли пополнить индикаторы угроз, добавив поля.
7. Оставьте поле **Extracting regular expression** пустым, поскольку нет необходимости извлекать доменные имена, поскольку они ограничены строками.
8. В поле **Fields** введите следующее domain:$1, description:ransomware\_domain\_blocklist для определения полей в данном черном списке.
9. (Опционально) В поле **Ignoring regular expression** оставьте отмеченным по умолчанию.
10. Измените значение поля **Skip header lines** на 0, поскольку опция пропуска регулярного выражения пропускает комментарии в верху потока.
11. Оставьте значение поля **Retry interval** по умолчанию 60 секунд.
12. (Опционально) Оставьте поле **Remote site user** пустым, поскольку данный поток не требует никакой аутентификации.
13. Оставьте значение поля **Retries** по умолчанию **3**.
14. Оставьте значение поля **Timeout** по умолчанию 30 секунд.
15. Пропустите раздел **Proxy Options**, если вы не используете прокси сервер для добавления анализа угроз в систему Splunk Enterprise Security.
16. Нажмите кнопку Save.
17. В главном меню платформы Splunk выберите **Apps> Enterprise Security**, чтобы вернуться в систему Splunk Enterprise Security.
18. В главном меню системы Enterprise Security выберите **Audit> Threat Intelligence Audit.**
19. Найдите станзу файла конфигурации ransomware\_tracker на панели **Threat Intelligence Downloads** и убедитесь, что в поле **status** указан статус **threat list downloaded.**
20. В главном меню системы Enterprise Security выберите **Security Intelligence> Threat Intelligence> Threat Artifacts.**
21. Заполните поле **Intel Source ID of ransomware\_tracker** для поиска доменов, добавленных в систему Splunk Enterprise Security из нового потока угроз.
22. Нажмите кнопку **Submit** для начала поиска.
23. Перейдите во вкладку Network и проверьте панель Domain Intelligence, чтобы убедиться, что в ней появилась анализ угроз из источника угроз ransomware\_tracker.

**Общий анализ**

**Добавление анализа в систему Splunk Enterprise Security**

В качестве администратора системы ES вы можете использовать платформу анализа угроз в системе Splunk Enterprise Security, чтобы скачать и проанализировать другие формы анализа, которые вы можете использовать для корреляции с событиями либо для пополнения панелей, используя поиск. Добавление таких общих форм анализа увеличивает возможности мониторинга безопасности ваших аналитиков и добавляет контекстный идентификатор в их расследования.

Система Splunk Enterprise Security включает в себя несколько источников анализа. Также система Splunk Enterprise Security поддерживает возможность добавления других общих источников анализа.

Администраторы ES могут добавить общий анализ в систему Splunk Enterprise Security, скачав поток из сети Интернет.

1. Конфигурация источников анализа, включенных в систему Splunk Enterprise Security.
2. Скачивание потока анализа из сети Интернет.
3. Убедитесь, что вы успешно добавили анализ в систему Splunk Enterprise Security.
4. Использование общего анализа в поиске вместе с вводом анализа.

**Скачивание потока анализа из сети Интернет в систему Splunk Enterprise Security**

Система Splunk Enterprise Security может периодически скачивать поток анализа, доступный в сети Интернет и хранить его в директории $SPLUNK\_DB/modinput/threatlist. Затем вы можете использовать команду поиска inputintelligence, чтобы использовать анализ в отчетах, поиске или панелях. См. раздел Пример: Добавление источника общего анализа в систему Splunk Enterprise Security.

1. (Опционально) Конфигурация прокси для получения анализа.
2. Добавление источника анализа на основе URL.

**Конфигурация прокси для получения анализа**

Если вы используете прокси сервер для отправки анализа в систему Splunk Enterprise Security, настройте опции прокси для источника анализа.

Имя пользователя должно соответствовать имени сохраненных учетных данных безопасности Splunk в системе управления учетными данными. Если вы удалите существующего пользователя прокси и пароль в редакторе настроек скачивания анализа, процесс скачивания больше не будет относится к сохраненным учетным данным. Более подробную информацию см. в разделе Управление учетными данными в системе Splunk Enterprise Security.

1. В главном меню Enterprise Security выберите **Configure> Data Enrichment> Intelligence Downloads.**
2. Выберите источник скачивания.
3. Настройте опции прокси.
4. Введите адрес прокси сервера. Поле **Proxy Server** не может содержать ссылку URL. К примеру, 10.10.10.10 или server.example.com.
5. Введите порт прокси сервера для получения доступа к адресу прокси сервера.
6. Введите учетные данные пользователя прокси для прокси сервера. Поддерживаются только основные и цифровые методы аутентификации.
7. Сохраните изменения.

**Добавление источника анализа на основе URL**

Добавьте источник анализа, отличающегося от TAXII, доступный по ссылке URL в сети Интернет. В качестве примера добавления общего источника анализа на основе URL, см. раздел Пример: Добавление общего источника анализа в систему Splunk Enterprise Security.

1. В главном меню Enterprise Security выберите **Configure> Data Enrichment> Intelligence Downloads.**
2. Заполните поле **Name** для скачивания. Имя может содержать только буквенно-цифровые значения, дефисы и подчеркивания. Имя не может содержать пробелы.
3. Нажмите кнопку **New** для добавления нового источника анализа.
4. Не отмечайте опцию **Sinkhole**.
5. Уберите выделение опции **Is Threat Intelligence**.
6. Заполните поле **Type** для скачивания. Поле тип определяет тип информации, содержащейся в потоке.
7. Заполните поле **Description**. Опишите информацию в потоке.
8. Оставьте значение в поле **Weight** без изменений, поскольку данное поле не имеет значения для источника общего анализа.
9. (Опционально) Измените значение по умолчанию поля **Interval** скачивания для потока. Значения по умолчанию: 43200 секунд или каждые 12 часов.
10. (Опционально) Заполните поле POST arguments для потока.
11. Не используйте настройку **Maximum age**.
12. (Опционально) Если вам необходимо определить пользовательскую строку **User agent**, чтобы обойти средства контроля безопасности сети в вашей среде, задайте значение следующего формата <user-agent> /<version>. К примеру, Mozilla/5.0 либо

AppleWebKit/602.3.12. Значение данного поля должно соответствовать регексу:

([A-Za-z0-9\_.-]+)/([A-Za-z0-9.-]+). Уточните у администратора вашего устройства безопасности, принимает ли система контроля безопасности сети строку, которую вы здесь вводите.

1. Заполните поля **Parsing Options**, чтобы убедиться, что ваш список успешно анализируется. Вам следует либо заполнить ограничивающее регулярное выражение, либо извлекающее регулярное выражение. Нельзя оставлять оба поля пустыми.

|  |  |  |
| --- | --- | --- |
| **Поле** | **Описание** | **Пример** |
| Ограничивающее регулярное выражение | Строка регулярного выражения, используемая для разделения или извлечения строк в источнике анализа. Для сложных разделителей данных используйте ограничивающее регулярное выражение. | , or: or \ t |
| Извлекающее регулярное выражение | Регулярное выражение, используемое для извлечения полей из индивидуальных строк документа источника угроз. Используется для извлечения значений в источнике угроз. | ^(\S+) \t+(S+)\t+\S+\t+\S+t\*(\S\*) |
| Поля | Необходимы, если ваш документ содержит заданные строки. Строки полей, отделенные запятыми, извлекаются из списка угроз. Также могут быть использованы для переименования или объединения полей. Поле Description является обязательным. Дополнительные допустимые поля – это поля в соответствующей коллекции хранилища KV Store для данной анализа угроз, видимой в локальных файлах справочника или файле DA-ESS-ThreatIntelligence/collections.conf. По умолчанию установлены следующие значения: description:$1, ip:$2. | <fieldname>:$<number>, <fieldname>.$<number>  ip:$1, descriptiom:domain\_blocklist |
| Пропускающее регулярное выражение | Регулярное выражение, используемое для пропуска строк в источнике угроз. Значения по умолчанию для пропускающих пустых строк и комментариев начинается со знака #. | ^\s\*$ |
| Пропуск строк заголовка | Количество строк заголовка, которые необходимо пропустить при обработке источника угроз. | () |
| Кодирование файлов анализа | Если кодирование файлов отличается от ASCII или UTF8, укажите тип кодирования здесь. Либо оставьте пустым. | latin1 |

1. (Опционально) Измените значение полей **Download Options**, чтобы убедиться, что ваш список скачивается успешно.

|  |  |  |
| --- | --- | --- |
| **Поле** | **Описание** | **Пример** |
| Время до повтора | Количество секунд ожидания между повторными попытками загрузки. Перед изменением заданного времени повтора ознакомьтесь с рекомендованным | 60 |

|  |  |  |
| --- | --- | --- |
|  | интервалом опроса провайдера источника угроз. |  |
| Пользователь удаленной площадки | Имя пользователя, которое используется для удаленной авторизации, при необходимости. Имя пользователя, которое вы добавляете в данное поле, должно соответствовать имени учетных данных в системе Управления учетными данными. См. раздел Управление учетными данными в системе Splunk Enterprise Security. | админ |
| Повторные попытки | Максимальное количество попыток повтора | 3 |
| Тайм-аут | Количество секунд ожидания перед признанием попытки загрузки неудачной. | 30 |

1. (Опционально) Если вы используете прокси сервер, заполните поле **Proxy Options** для потока. См. раздел Конфигурация прокси для получения анализа.
2. Сохраните изменения.

После окончания добавления источников анализа см. раздел Убедитесь, что вы успешно добавили анализ в систему Splunk Enterprise Security.

**Использование общего анализа для поиска при помощи команды inputintelligence**

После добавления общего анализа в систему Splunk Enterprise Security, вы можете использовать команду inputintelligence, чтобы использовать анализ. См. раздел Добавление общего анализа в систему Splunk Enterprise Security.

**Описание**

Используйте команду inputintelligence, чтобы добавить анализ из директории списка угроз к вашим результатам поиска. После скачивания общая аналитика разбирается и хранится в директории $SPLUNK\_DB/modinputs/threatlist$.

**Синтаксическая структура**

|inputintelligence <threatlist\_stanza\_name> [fields=<string>]

[delim\_regex=<string>][extract\_regex=<string>] [ignore\_regex=<string>]

[skip\_header-lines=<int>] [include\_raw=<bool>] [append=<bool>]

[no\_parse=<bool>]

***Необходимые аргументы***

**threatlist\_stanza\_name**

**Синтаксическая структура**: <string>

**Описание**: Станза скачивания анализа. Соответствует полю **Name** на странице Скачивания анализа. Вы можете включить различные названия станз в ваш поиск. См. раздел Скачивание потока анализа из сети Интернет в систему Splunk Enterprise Security.

***Дополнительные аргументы***

fields

**Синтаксическая структура**: <string>

**Описание**: Переопределяет настройки полей по умолчанию для скачивания анализа, определенные на странице Скачивание анализа. Необходимо, если ваш документ ограничен строками. Список полей, отделенный запятыми, который необходимо выделить из списка анализа. Может также использоваться для переименования или объединения полей. Поле Description обязательно для заполнения. Дополнительные подходящие поля– это поля в соответствующей коллекции хранилища KV Store для анализа угроз, видимые в локальных файлах справочника или файле DA-ESS-Threatintelligence/collections.conf. Значение по умолчанию для поля Description: $1, ip:$2.

**delim\_regex**

**Синтаксическая структура**: <string>

**Описание**: Переопределяет настройки по умолчанию ограничивающего регулярного выражения для скачивания анализа, определенные на странице скачивания анализа. Строка регулярного выражения используется для разделения или ограничения линий в источнике анализа. Для сложных ограничителей используйте извлекающее регулярное выражение.

**extract\_regex**

**Синтаксическая структура**: <string>

**Описание**: Переопределяет настройки по умолчанию извлекающего регулярного выражения для скачивания анализа, определенные на странице скачивания анализа. Регулярное выражение, используемое для извлечения полей из индивидуальных линий в документе источника анализа. Используйте извлекающие значения в источнике анализа.

**ignore\_regex**

**Синтаксическая структура**: <string>

**Описание**: Переопределяет настройки параметров по умолчанию игнорирования регулярного выражения для скачивания анализа, определенные на странице скачивания анализа. Регулярное выражение, используемое для игнорирования строк в источнике анализа. Параметры по умолчанию для игнорирования пустых строк и комментариев, которые начинаются с #.

**skip\_header\_lines**

**Синтаксическая структура**: <int>

**Описание**: Переопределяет настройки значения по умолчанию для пропуска строк заголовка для скачивания анализа, определенные на странице скачивание анализа. Количество строк заголовка, которые необходимо пропустить при обработке источника анализа.

**Значение по умолчанию**: 0

**include\_raw**

**Синтаксическая структура**: <bool>

**Описание**: Если указано значение 1, t или true, добавляется оригинальный контент строки к дополнительной колонке, которая называется исходной.

**Значение по умолчанию**: 0

**append**

**Синтаксическая структура**: <bool>

**Описание**: Если указано значение 1, t или true, добавляются результаты команды inputintelligence к существующему набору результатов поиска вместо их замещения.

**Значение по умолчанию:** 0

**no\_parse**

**Синтаксическая структура**: <bool>

**Описание**: Если указано значение 1, t или true, все другие опции игнорируются, а файл анализа исходного контента возвращается одна линия на ряд.

**Значение по умолчанию**: 0

**Применение**

Команда inputintelligence является командой transforming command.

**Примеры**

***1. Рассмотрите сайты the top one million***

Рассмотрите сайты the top one million согласно данным Alexa.

inputintelligence alexa\_top\_one\_million\_sites

***2. Другие примеры***

См. раздел Примеры: Добавление источника основного анализа в систему Splunk Enterprise Security.

**Смотрите также**

Справочник ввода данных

**Пример: Добавление источника основного анализа в систему Splunk Enterprise Security.**

В качестве аналитик безопасности, вы захотите сравнить хост-системы вашей сети с хост-системами, связанными с предупреждениями Spotify, которые могут оценить риск, который согласно Spotify Free, каждый рабочий день угрожает вашей сети. хост-системы, связанные с предупреждениями Spotify, не являются вредоносными, и вам не понадобится добавлять их в систему Splunk Enterprise Security в качестве анализа угроз. Взамен, вы можете добавить их как общий анализ.

**Скачивание общего анализа**

Для начала создайте конфигурацию скачивания для списка.

1. Выберите **Configure> Data Enrichment> Intelligence Downloads.**
2. Нажмите кнопку **New**.
3. В поле **Name** введите spotify\_ads.
4. Уберите отметку в поле **Is Threat Intelligence**.
5. В поле **Type** введите spotify\_ads.
6. В поле **Description** укажите имена хост-машин, в которых размещены Spotify ads.
7. Укажите ссылку URL

http://raw.githubusercontent.com/FadeMind/hosts.extras/master/Spotify-Ad-free/hosts.

1. (Опционально) Измените значение по умолчанию поля **Weight**.
2. (Опционально) Измените значение по умолчанию поля **Interval**.
3. Задайте ограничивающее регулярное выражение \s.
4. В поле **Fields** введите url:$2.
5. В поле **Ignoring regular expression** введите (^# | ^ \s\*$).
6. Сохраните изменения.

**Убедитесь, что анализ скачивается успешно**

Используя поиск, убедитесь, что модульный ввод скачивает информацию из источника.

| inputintelligence no\_parse= 1 spotify\_ads

**Убедитесь, что анализ проводится корректно**

Используйте пользовательскую команду поиска inputintelligence, чтобы убедиться, что анализ проводится корректно.

| inputintelligence spotify\_ads

Если вам кажется, что анализ проводится некорректно, проверьте search.log на предмет сообщений об ошибках. Дополнительно, вы можете изменить настройки проведения анализа для скачивания, используя дополнительные аргументы для команды inputintelligence, чтобы задать правильные настройки. См. раздел Использование общего анализа для поиска при помощи команды inputintelligence.

**Использование нового источника анализа при поиске**

Вы можете использовать новый источник анализа разными способами при поиске.

***Использование Spotify ads для субпоиска.***

Для возвращения 100 URLs, используемых Spotify ads в списке со следующим субпоиском:

| search [ | inputintelligence spotify\_ads, | return 100 url ]

***Использование Spotify ads при команде join***

Объедините хост-системы в источнике анализа Spotify ads с другим набором данных при помощи команды join:

. . . | join url [ | inputintelligence spotify\_ads | eval

spotify\_ad=”true”] | search spotify\_ad=”true”

***Добавление Spotify ads в файл таблицы справочника***

Добавьте хост-системы из Spotify ads в файл таблицы справочника, используя порождающий поиск справочника:

| inputintelligence spotify\_ads | eval spotify\_ad=”true” | outputlookup spotify\_ads.csv

После создания справочника, используйте его для поиска со следующим примерным поиском:

. . . | lookup spotify\_ads.csv url OUTPUT spotify\_ad | search spotify\_ad=”true”

**Управление содержанием**

**Управление содержанием в Splunk Enterprise Security**

Как администратор Splunk Enterprise Security, вы можете использовать страницу управления содержанием (Content Management) для отображения, создания, конфигурации и редактирования содержания, уникального для Splunk Enterprise Security, такого как поиск корреляций, поиск по ключевым показателям, сохраненный поиск и поиск по событийным линиям.

* Создание поиска корреляций в Splunk Enterprise Security
* Создание моделей данных и управление ими в [Splunk Enterprise Security](#page1)
* [Создание поиска по ключевым показателям и управление им в Splunk Enterprise Security](#page2)
* [Создание справочников и управление ими в Splunk Enterprise Security](#page13)
* [Создание сохраненных поисков и управление ими в Splunk Enterprise Security](#page4)
* [Создание справочников на основе поиска и управление ими в Splunk Enterprise Security](#page5)
* [Создание поиска по событийным линиям и управление ими в Splunk Enterprise Security](#page8)
* [Создание витрин и управление ими в Splunk Enterprise Security](#page13)
* [Экспорт содержимого из Splunk Enterprise Security как](#page11) приложения

**См. также**

• Создание и редактирование объектов риска в Splunk Enterprise Security

**Создание моделей данных и управление ими в Splunk Enterprise Security**

Создавайте модели данных и управляйте ими с помощью страницы управления содержанием в Splunk Enterprise Security.

* Проверить список моделей данных в Splunk Enterprise Security.
* Проверить следующее время по графику, статус ускорения, выбрать, нужно ли ускорять модель данных.
* Нажать на название модели данных для редактирования модели данных.

**Создать модель данных**

1. В меню Enterprise Security выбрать **Configure > Content** **Management**.
2. Нажать **Create New Content** и выбрать **Data Model**.
3. Создать модель данных, следуя инструкциям документации платформы Splunk.

* Для Splunk Enterprise, см. раздел «Создание модели данных в Splunk Enterprise» в *Руководстве администратора базы знаний.*
* Для Splunk Cloud, см. раздел «Создание модели данных в Splunk Cloud» в *Руководстве администратора базы знаний.*

**Создание поиска по ключевым показателям и управление им в Splunk Enterprise Security**

Конфигурируйте поиск по ключевым показателям на странице управления содержанием в Splunk Enterprise Security. Используйте фильтры для выбора типа ключевого показателя для просмотра только поиска по ключевым показателям.

**Создание пользовательского поиска по ключевым показателям**

Создайте поиск ключевого показателя для создания ключевого показателя, который вы сможете добавить на панель или в систему «стеклянный стол» как показатель безопасности.

1. В меню Enterprise Security выбрать **Configure > Content** **Management**.
2. Нажать **Create New Content** и выбрать **Key Indicator Search**.
3. Ввести название ключевого показателя.

Чтобы отобразить ключевой показатель в списке показателей безопасности в системе «стеклянный стол», ввести категорию или область системы безопасности перед названием ключевого показателя, затем ввести дефис. Например, **APT - Example Key**

**Indicator** или **Access - Sample Key Indicator**.

1. Ввести поиск и прочие данные.

Ключевые показатели, встроенные в Enterprise Security, используют модели данных для ускорения получения результатов.

1. (Опционально) Выбрать **Schedule**, чтобы использовать ускорение модели данных для вашего пользовательского ключевого показателя.
2. Ввести название поля, которое соответствует значению ключевого показателя в поле **Value**.
3. Ввести название поля, которое соответствует изменению ключевого показателя в поле **Delta**.
4. (Опционально) Ввести **Threshold** для ключевого показателя. Данное пороговое значение контролирует, изменяет ли цвет ключевой показатель. Вы также можете установить пороговое значение в панелях и системе «стеклянный стол».
5. Ввести **Value Suffix**, для обозначения единиц или других слов, которые будут идти после ключевого показателя.
6. Выбрать графу **Invert**, чтобы инвертировать цвета ключевого показателя. Выбрать эту графу, чтобы указать, что высокое значение является положительным, а низкое значение является плохим значением.
7. Нажать **Save**.

**Планирование поиска по ключевым показателям**

Ключевые показатели, включенные в Splunk Enterprise Security, используют ускорение модели данных. Активируйте ускорение и запланируйте поиск для запуска как **запланированный отчет** (**scheduled report)**. Результаты запланированного отчета кэшируются, что позволяет показателю более быстро отображать результаты на панели.

1. Выбрать **Configure > Content Management**.
2. Указать поиск ключевого показателя, который вы хотите ускорить.
3. Нажать **Accelerate** в столбце **Actions**.
4. В окне **Edit Acceleration** выбрать графу **Accelerate**.
5. Выбрать **Refresh Frequency**, чтобы указать, как часто Enterprise Security должна обновлять кэшированные результаты.
6. Нажать **Save**.

После ускорения ключевого показателя **Next Scheduled Time** заполняет страницу **Content Management**, значок молнии для этого показателя меняется с серого на желтый.

**Редактирование поиска по ключевому показателю**

Вносите изменения в поиск по ключевому показателю.

1. В меню ES выбрать **Configure > Content Management**
2. Выбрать поиск по ключевому показателю.
3. (Опционально) Изменить название поиска.
4. (Опционально) Изменить целевое приложение, где будет храниться поиск.
5. (Опционально) Изменить заголовок ключевого показателя. Заголовок появляется над ключевым показателем на панели или рядом с показателем безопасности в системе «стеклянный стол».
6. (Опционально) Изменить подзаголовок ключевого показателя, который используется для описания типа функции ключевого показателя на панелях.
7. (Опционально) Изменить цепочку поиска, которая заполняет ключевой показатель.
8. (Опционально) Добавить URL для детализации, такой как пользовательский поиск или ссылка на панель для обхода детализации по умолчанию. По умолчанию детализация ключевого показателя открывает результаты поиска, по которым было получено значение ключевого показателя. Для ключевых показателей вы можете установить пользовательскую детализацию, когда добавляете ключевой показатель в систему «стеклянный стол».

1. (Опционально) Выбрать графу **Schedule**, чтобы активировать ускорение для ключевого показателя и обеспечить ускоренную загрузку в панели.
2. (Опционально) Изменить частоту **Cron Schedule**, используя стандартное обозначение крон.
3. (Опционально) Изменить параметры **Threshold**, чтобы определить цвет, выбранный для показателя значения. По умолчанию, отсутствие порогового значения обозначается показателем значения черного цвета, пороговое значение выше показателя значения обозначается зеленым цветом, пороговое значение ниже показателя значения обозначается красным цветом.
4. (Опционально) Добавить **Value suffix**, чтобы описать показатель значения. Например, указать единицы. На панелях суффикс значения появляется между показателем значения и показателем тренда.
5. (Опционально) Выбрать графу **Invert**, чтобы изменить цвета, установленные по умолчанию для порогового значения показателя тренда. Если выбрана данная графа, пороговое значение выше показателя значения обозначается красным цветом, пороговое значение ниже показателя значения обозначается зеленым цветом.
6. Нажать **Save**.

**Создание сохраненных поисков и управление ими в Splunk Enterprise Security**

Выбрать сохраненный поиск, также называемый запланированным отчетом, в Splunk Enterprise Security.

1. В меню Enterprise Security выбрать **Configure > Content** **Management**.
2. Нажать **Create New Content** и выбрать **Saved Search**.
3. Создать выбранный поиск, также называемый запланированным отчетом, следуя инструкциям в документации платформы Splunk.
   * Для Splunk Enterprise, см. раздел «Создание нового отчета в Splunk Enterprise» в *Инструкциях по отчетности.*
   * Для Splunk Cloud, см. раздел «Создание нового отчета в Splunk Cloud» в *Инструкциях по отчетности.*
4. Изменяйте разрешения в отчете, чтобы передать его в Enterprise Security, чтобы вы смогли просматривать поиск и управлять им в Enterprise Security, следуя инструкциям в документации платформы Splunk.
   * Для Splunk Enterprise, см. раздел «Установить разрешения отчета в Splunk Enterprise» в *Инструкциях по отчетности.*
   * Для Splunk Cloud, см. ee раздел «Установить разрешения отчета в Splunk Cloud» в *Инструкциях по отчетности.*

**Создание справочников на основе поиска и управление ими в Splunk Enterprise Security**

Справочник на основе поиска позволяет вам создавать справочник, основанный на результатах поиска, который будет выполняться через регулярные установленные интервалы. Поиск может выполняться только по данным, хранящимся в моделях данных, или в существующем справочнике. Справочники, созданные как справочники на основе поиска, исключаются из копирования специальных пакетов и не направляются в индексаторы.

**Когда использовать справочники на основе поиска**

Создавайте справочник на основе поиска, если вы хотите знать, когда происходит что-то новое в вашей среде, или если вам требуется постоянно обновлять справочник на основании изменения информации из модели данных или другого справочника.

Справочник на основе поиска собирает и хранит информацию из модели данных или других справочников. Данные, которые хранятся в справочнике, представляют историческую сводку выбранных полей, собранную по событиям. Вы можете просматривать изменения на панели или использовать поиск корреляций, чтобы сравнивать данные из справочника на основе поиска с новыми событиями и получать уведомления в случае совпадений. Например, чтобы узнать, когда на веб-сервер заходит новый пользователь.

1. Выполнить поиск данных о пользователе в модели данных «Аутентификация» и отфильтровать по имени хоста веб-сервера с помощью команды where.
2. Убедиться, что результаты поиска соответствуют известным хостам и пользователям в вашей среде.
3. Создать управляемый справочник на основе поиска, чтобы собрать и хранить информацию по регулярному графику о пользователях, заходящих на веб-серверы.
4. Создать поиск корреляций, который будет уведомлять вас, когда пользователь заходит на один из веб-серверов, куда ранее не заходил, на основании исторической информации в справочнике на основе поиска.

**Создание справочника на основе поиска**

Создайте справочник на основе поиска.

1. В меню Splunk Enterprise Security выбрать **Configure >** **Content Management**.
2. Нажать **Create New Content** и выбрать **Справочник на основе поиска**.
3. (Опционально) Выбрать **App**. Приложением, используемым по умолчанию, является SplunkEnterpriseSecuritySuite. Вы можете создать справочник в особом приложении, таком как SA-NetworkProtection, или в пользовательском приложении. Вы не можете изменить приложение после того, как сохранили справочник на основе поиска.
4. (Опционально) Ввести описание для поиска.
5. Ввести ярлык для справочника. Это название справочника на основе поиска, которое появляется на странице **Content Management**.
6. Ввести название для справочника. После сохранения справочника название менять нельзя.
7. Ввести график крон, чтобы определить, как часто вы хотите запускать поиск.
8. Выбрать для поиска планирование в реальном времени или постоянное планирование. Планирование в реальном времени определяет приоритетом выполнение поиска, а постоянное планирование определяет приоритетом целостность данных.
9. Ввести **Search Name**, чтобы определить название сохраненного поиска. После сохранения справочника название изменить нельзя.
10. Выбрать режим **Guided**, чтобы создать поиск без необходимости прописывания синтаксиса поиска, или выбрать **Manual**, чтобы прописать ваш собственный поиск. См. пример для создания поиска с помощью редактора управляемого поиска.
11. Если вы создаете поиск в ручном режиме, введите поиск.
12. Нажать **Save**, чтобы сохранить поиск.

**Пример справочника на основе поиска**

В данном примере справочника на основе поиска, включенном в Splunk Enterprise Security, вы хотите отслеживать атаки, идентифицируемые вашей системой обнаружения сетевых атак (IDS). После этого вы сможете получать уведомления о новых атаках с поиском корреляций или определять, является ли атака новой для вашей среды. Панель центра обнаружения сетевых атак (Intrusion Center) использует данный справочник на основе поиска для панели «Новые атаки – Последние 30 дней». См. панель Intrusion Center.

1. В меню Splunk Enterprise Security выбрать **Configure >** **Content Management**.
2. Нажать **Create New Content** и выбрать **Search-Driven Lookup**.
3. (Опционально) Выбрать **App** SA-NetworkProtection. Вы не сможете изменить приложение после сохранения справочника на основе поиска.
4. Ввести описание «Ведение списка атак, определенных IDS, и время первого и последнего обнаружения атак».
5. Ввести ярлык **IDS Attack Tracker Example** для справочника. Это название для справочника на основе поиска, которое появляется на странице **Content Management**.
6. Ввести уникальное и описательное название для справочника

**ids\_attack\_tracker\_example**. После сохранения справочника название изменить нельзя.

1. Ввести график крона, чтобы определить, как часто вы хотите запускать поиск. Если ваша система IDS часто собирает данные, введите график крона 25 \* \* \* \*, чтобы запускать поиск каждые 25 минут, каждый час, каждый день.
2. Выбрать Continuous Schedule, так как справочник должен постоянно отслеживать все точки ввода данных.
3. Ввести **Search Name** в витрине **Network - IDS Attack Tracker - Example** **Lookup Gen**.
4. Выбрать управляемый режим, чтобы использовать редактор управляемого поиска для создания поиска.
5. Нажать **Open guided search editor**, чтобы начать создание поиска.
6. Выбрать источник данных как **Data Model**, так как данные по атакам системы IDS хранятся в модели данных.
7. Выбрать модель данных **Intrusion\_Detection** и набор данных модели данных **IDS\_Attacks**.
8. Выбрать **Yes**, чтобы поле агрегированных данных выполняло только поиск по данным в ускоренной модели данных.
9. Выбрать диапазон времени, который использует относительное время, которое начинается самое раннее 70 минут назад, начиная с начала минуты, и заканчивается сейчас. Нажать **Apply**, чтобы сохранить диапазон времени.
10. Нажать **Next**.
11. (Опционально) Ввести условие where, чтобы отфильтровать данные из модели данных только по данным от конкретного поставщика IDS и нажать **Next**.
12. Добавить агрегированные значения для отслеживания определенной статистики по данным и сохранить эту информацию в справочнике. Требуется как минимум одно агрегированное значение.
    * 1. Чтобы отследить, когда в первый раз в вашей среде была обнаружена атака IDS, необходимо добавить новое агрегированное значение с функцией **min** и полем **\_time** и сохранить его как **firstTime**.
      2. Чтобы отследить, когда в последний раз в вашей среде была обнаружена атака, необходимо добавить еще одно агрегированное значение с функцией **max** и полем **\_time** и сохранить его как **lastTime**. В результате в справочнике будет создано два столбца, firstTime иlastTime.
13. Добавить условия разбивки, чтобы отслеживать больше точек ввода данных в справочнике. Все условия разбивки появляются как столбцы в справочнике.
    * 1. Добавить условие разбивки в витрине **IDS\_Attacks.ids\_type** и переименовать его как **ids\_type** для отражения типа атаки IDS в справочнике.
      2. Добавить условие разбивки, чтобы переименовать IDS\_Attacks.signature как **signature**.
      3. Добавить условие разбивки, чтобы переименовать IDS\_Attacks.vendor\_product как **vendor\_product**.
14. Нажать **Next**.
15. Выбрать период сохранения, чтобы определить срок данных, которые будут храниться в справочнике. Например, вам необходимо хранить данные по атакам IDS за 5 лет в данном справочнике. Выбрать поле времени **lastTime**, чтобы указать время сохранения на основе последнего времени выявления атаки IDS. Введите самое раннее время как **-5y** и укажите формат времени, которое вы ввели: **%s**. Вы можете найти руководство по формату времени в документации платформы Splunk.
    * Для Splunk Enterprise см. раздел «Переменные форматы даты и времени в Splunk Enterprise» в *Руководстве по поиску*.
    * Для Splunk Cloud см. раздел «Переменные форматы даты и времени в Splunk Cloud» в *Руководстве по поиску*.
16. Нажать **Next**.
17. Проверить поиск, созданный в мастере настройки, и нажать **Done**, чтобы завершить использование редактора управляемого поиска.
18. Нажать **Save**, чтобы сохранить поиск.

**Изменение справочника на основе поиска**

1. В меню Splunk Enterprise Security выбрать **Configure >** **Content Management**.
2. Выбрать **Type** как **Search-Driven Lookup**.
3. Нажать на поиск, который вы хотите редактировать.
4. Внести изменения и нажать **Save**.

**Активация или отключение поиска, заполняющего справочник на основе поиска**

Вы можете активировать или отключать поиск справочника на основе поиска, чтобы поиск не обновлял справочник. Если вы отключаете поиск, который заполняет справочник на основе поиска, поиск прекращает обновлять справочник, данные в справочнике не будут обновляться. Поиски корреляций и панели, которые используют данные справочника, будут устаревшими.

1. Выбрать **Configure > Content Management**.
2. Отфильтровать по типу справочника на основе поиска и открыть справочник на основе поиска, который вы хотите активировать или отключить.
3. Найти **Search name** справочника на основе поиска.
4. В меню платформы Splunk выбрать **Settings > Searches, reports,** **alerts**.
5. Выбрать поиск и активировать или отключить его.

**Создание поиска по событийным линиям и управление им в Splunk Enterprise Security**

Создайте поиск по событийным линиям для поиска по событийным линиям, который вы можете добавить на панель Asset Investigator или Identity Investigator. Событийные линии на панелях изучения помогают вам составить профиль действий по определенным объектам или показателям в течение периода времени.

1. В меню Enterprise Security выбрать **Configure > Content** **Management**.
2. Нажать **Create New Content** и выбрать **Swim Lane Search**.
3. Ввести **Search name**.
4. Выбрать **Destination App**.
5. Ввести **Title** для событийной линии, который появится на панели.
6. Ввести **Search**, который заполняет событийная линия.
7. Ввести **Drilldown Search**, который запускается, когда пользователь нажимает объект событийной линии. По умолчанию детализация объектов событийной линии показывает необработанные события.
8. Выбрать цвет.
9. Выбрать **Entity Type** для **Asset** или **Identity**.
10. Ввести **Constraint Fields**. Ввести поле для указания ограничений по поиску. Ваш поиск должен содержать where $constraints$, чтобы использовать эти поля ограничений в поиске. Только определенные ограничения действительны для каждого типа поиска по событийным линиям.

Например, поиск по событийной линии Asset Investigator, использующий модель данных Malware и набор данных модели данных Malware\_Attacks, может указывать в качестве ограничения поле Malware\_Attacks.user.

11. Нажать **Save**.

**Пример**

Например, создать событийную линию для выявления всех событий аутентификации, включающих определенный объект.

1. Ввести **Search name** как **Authentication by Asset - Example**
2. Выбрать **Destination App** как **DA-ESS-AccessProtection**.
3. Ввести **Title** для событийной линии, который отображается на панели. **All** **Authentication**.
4. Ввести **Search**, который заполняет событийная линия.

| tstats 'summariesonly' values(Authentication.action) as action,values(Authentication.app) as app,values(Authentication.src) as src,values(Authentication.dest) as dest,values(Authentication.user) as user,count from datamodel=Authentication.Authentication where $constraints$ by \_time span=$span$

1. Ввести **Drilldown Search**.

| 'datamodel("Authentication","Authentication")' | search $constraints$

1. Выбрать цвет **Purple**.
2. Выбрать тип предприятия **Asset**, так как вы хотите изучать все события аутентификации по объекту и иметь возможность добавлять событийную линию на панель Asset Investigator.

После указания этих значений все ограничения, указанные как поля ограничений, выполняют обратный просмотр по другим полям, которые определяют объект.

1. Ввести поля ограничений **Authentication.src** и **Authentication.dest**, чтобы определить аутентификации, происходящие из определенного объекта или направленные на него.

Для ввода справочника по объекту с IP-адресом 1.2.3.4, dns с server.example.com, и nt\_host server1, поиск для данной событийной линии ищет все события аутентификации, где источником или целью события аутентификации является 1.2.3.4, server.example.com, или server1.

... Authentication.src=1.2.3.4 OR Authentication.src=server.example.com OR Authentication.src=server1 OR Authentication.dest=1.2.3.4 OR Authentication.dest=server.example.com OR Authentication.dest=server1

**Создание витрин и управление ими в Splunk Enterprise Security**

Создайте новую витрину или панель с помощью Simple XML на странице Content Management.

**Предварительное условие**

Создание новых витрин и панелей через Content Management требует знания Simple XML. Смотрите обзор создания и редактирования панелей, включая работу с Simple XML, в документации платформы Splunk.

* Для Splunk Enterprise см. раздел «Обзор панелей в Splunk Enterprise» в *Панелях и визуализации.*
* Для Splunk Cloud см. раздел «Обзор панелей в Splunk Cloud» в *Панелях и визуализации.*

**Задача**

1. В меню Enterprise Security выбрать **Configure > Content** **Management**.
2. Нажать **Create New Content** и выбрать **View**.
3. Создать новую панель с помощью Simple XML.
4. Изменить разрешения для передачи новой витрины в Enterprise Security, чтобы вы смогли просматривать ее и управлять ей в Enterprise Security.
   1. В меню Splunk выбрать **Settings > User interface > Views**.
   2. Указать **View name**, который вы создали.
5. Нажать **Permissions** и изменить разрешения, чтобы передать витрину в Enterprise Security.
6. Нажать **Save**.

Вы также можете создать новую панель с помощью редактора интерактивной панели. Выбрать **Search > Dashboards**, чтобы открыть страницу панелей. Вы можете найти информацию о Редакторе панелей в документации платформы Splunk.

* Для Splunk Enterprise см. раздел «Открыть Редактор панелей в Splunk Enterprise» в *Панелях и визуализации.*
* Для Splunk Cloud см. раздел «Открыть Редактор панелей в Splunk Cloud» в *Панелях и визуализации.*

Использовать редактор Навигации, чтобы изменить, какие панели будут видны в меню в вашей развертке. Смотрите дальнейшую информацию в разделе «Настройка меню» в Splunk Enterprise Security.

**Экспорт содержимого из Splunk Enterprise Security как приложения**

Экспортируйте содержимое из Splunk Enterprise Security как приложение со страницы Content Management. Используйте опцию экспорта для передачи пользовательского содержимого в другие копии ES, например, миграция пользовательских поисков из среды разработки или тестирования в производство. Вы можете экспортировать любой тип содержимого на странице Content Management, например, поиск корреляций, система «стеклянный стол», модели данных и витрины.

По умолчанию, только пользователи-администраторы могут экспортировать содержимое. Чтобы добавить возможность экспорта для другой роли, см. раздел «Добавление возможностей для роли" в *Инструкциях по установке и обновлению.*

1. В меню ES выбрать **Configure > Content Management**.
2. Выбрать графы с содержимым, которое вы хотите экспортировать.
3. Нажать **Edit Выбратьion** и выбрать **Export**.
4. Ввести **App name**. Это будет название приложения в файловой системе. Например, SOC\_custom.
5. Выбрать **App name prefix**. Если вы хотите импортировать содержимое обратно в Splunk Enterprise Security без изменения характеристик импорта приложения по умолчанию, выбрать **DA-ESS-**. В противном случае, выбрать **No Prefix**.
6. Ввести **Label**. Это название приложения. Например, Custom SOC app.
7. Ввести **Version** и **Build number** для вашего приложения.
8. Нажать **Export**.
9. Нажать **Download app now,** чтобы загрузить пакет приложения в поисковый блок, расположенный в

$SPLUNK\_HOME/etc/apps/SA-Utils/local/data/appmaker/\*.

1. Нажать **Close**, чтобы вернуться на страницу **Content Management**.

**Ограничения по экспортируемому содержанию**

Экспортируемое содержание может не работать в более старых версиях Enterprise Security. Следующие позиции включены или не включены в экспортируемое содержание.

|  |  |  |
| --- | --- | --- |
| **Экспортируемая позиция** | **Включена в экспорт** | **Не включена в экспорт** |
| Модели данных | datamodels.conf и определение JSON модели данных. | Не применимо |
| Сохраненные поиски, включая поиски корреляций, поиск по ключевым показателям и событийным линиям | savedsearches.conf  governance.conf  Действия по предупреждению и меры реагирования, включая назначение риска, название скрипта и адрес электронной почты | Макрос, скрипт-файлы, справочники, или любые бинарные файлы, на которые ссылается объект поиска. Объекты экстремального поиска, такие как поиск, генерирующий контекст, контексты или концепции, на которые ссылается объект поиска. |
| Справочники на основе поиска | savedsearches.conf  governance.conf  managed\_configurations.conf  collections.conf  transforms.conf | Макрос, скрипт-файлы, справочники, или любые бинарные файлы, на которые ссылается объект поиска. |
| Управляемые справочники | CSV-файл справочника managed\_configurations.conf  collections.conf transforms.conf | Не применимо |
| Витрины | Файлы XML или HTML, CSS, и JS files для витрины. | Не применимо |

**Создание справочников и управление ими в Splunk Enterprise Security**

Splunk Enterprise Security предоставляет **lookups** для управления корреляциями объектов и идентификации с событиями, соотношения показателей угрозы с событиями и внесения информации в панели и блоки.

Как администратор, вы можете добавлять справочники в Splunk Enterprise Security. После добавления справочников в Splunk Enterprise Security, вы можете использовать справочники в поиске, редактировать их, добавлять описания и экспортировать их.

**Добавление справочника в Splunk Enterprise Security**

Загрузить и создать справочник в Splunk Enterprise Security.

1. Выбрать **Configure > Content Management**.
2. Нажать **Create New Content > Managed Lookup**.
3. Нажать **Create New**.
4. Выбрать файл справочника для загрузки.
5. (Опционально) Изменить **App** по умолчанию для файла.
6. (Опционально) Изменить название файла.
7. (Опционально) Изменить название определения.
8. (Опционально) Изменить тип справочника по умолчанию.
9. Ввести ярлык для справочника. Ярлык появляется как название для справочника на странице **Content Management**.
10. Ввести описание для справочника.
11. (Опционально) Изменить опцию, чтобы разрешить редактирование файла справочника.
12. Нажать **Save**.

**Добавление существующего справочника в Splunk Enterprise Security**

Если файл справочника и определение уже существуют в платформе Splunk, вы можете добавить его в Splunk Enterprise Security, чтобы вы смогли его редактировать.

1. Выбрать **Configure > Content Management**.
2. Нажать **Create New Content > Managed Lookup**.
3. Нажать **Select Existing**.
4. Выбрать определение справочника из выпадающего списка.
5. (Опционально) Изменить тип справочника.
6. Ввести ярлык для справочника. Ярлык появляется как имя справочника на странице **Content Management**.
7. Ввести описание для справочника.
8. (Опционально) Изменить опцию для разрешения редактирования файла справочника.
9. Нажать **Save**.

**Проверка успешного добавления справочника**

Убедитесь, что вы успешно добавили файл справочника, используя команду поиска inputlookup для отображения списка. Например, для проверки справочника протоколов приложения:

| inputlookup append=T application\_protocol\_lookup

**Редактирование справочника в Splunk Enterprise Security**

Только пользователи с соответствующими разрешениями могут редактировать справочники. См. раздел «Управление разрешениями» в Splunk Enterprise Security. Справочники не принимают обычных выражений, редактор справочника не проверяет точность ваших записей. Вы не можете сохранить файл справочника с пустыми полями заголовков.

**Прекращение управления справочником**

Вы можете прекратить управление справочником на странице Content Management, нажав **Stop managing**. Когда вы прекращаете управлять справочником, вы больше не сможете редактировать справочник из Splunk Web, но справочник не удаляется.

**Экспорт справочника в Splunk Enterprise Security**

1. На странице Content Management укажите справочник, который вы хотите экспортировать.
2. В столбце Actions нажать **Export**, чтобы экспортировать копию файла в формате CSV.

Вы можете экспортировать несколько файлов справочника и прочие объекты знаний как часть приложения. См. раздел «Экспорт содержимого» в *Администрировании* *Splunk Enterprise Security.*

**Проверка изменений, произведенных в справочниках**

Чтобы просмотреть, когда последний раз и кем редактировался справочник, используйте строку поиска. Например:

index=\_internal

uri\_path="/splunk-es/en-US/app/SplunkEnterpriseSecuritySuite/ess\_lookups\_edit"

**Управление внутренними справочниками в Splunk Enterprise Security**

Splunk Enterprise Security обеспечивает и обслуживает внутренние справочники для поддержки панели мониторинга, поисковых запросов и других внутренних процессов.

Эти справочники создаются несколькими способами.

* Путем заполнения данными из статического справочника
* Путем заполнения данными по результатам поисковых запросов, такой справочник также называется справочником по поиску (search-driven lookup)
* Путем заполнения информацией, полученной из сети Интернет

Внутренние справочники, заполненные информацией из сети Интернет, используются некоторыми корреляционными поисками для установления хостов, которые признаны вредоносными или подозрительными в соответствии с различными онлайнами, такими как Институт SANS. Если Splunk Enterprise Security не подключен к сети Интернет, то справочники не обновляются, соответственно поиск корреляции на основании таких справочников может работать некорректно. Большинство внутренних справочников, заполненных информацией из сети Интернет, являются источниками распознавания угроз. См. раздел настоящего руководства Настройка источников распознавания угроз в Splunk Enterprise Security.

Выберите **Configure > Content Management,** чтобы отобразить существующие справочники, которые вы можете редактировать в программе Splunk Enterprise Security.

Splunk Enterprise Security использует различного рода внутренние справочники.

|  |  |  |
| --- | --- | --- |
| **Тип справочника** | **Описание** | **Пример** |
| Список | Небольшие, относительно статические списки, используемые для наполнения панели мониторингаов. | Категории |
| Список ресурсов или идентификационных данных | Поддерживается модульным вводом и поисковыми запросами. См. раздел Как Splunk Enterprise Security обрабатывает и объединяет ресурсы или идентификационные данные. | Ресурсы |
| Сбор данных об источниках распознавания угроз | Поддерживается несколькими модульными вводами и поисковыми запросами. См. раздел Структура распознавания угроз в Splunk Enterprise Security на портале разработчика Splunk. | Локальный сертификат  Intel |
| Трекер | Справочники по поиску, используемые для обеспечения данными секций панели мониторинга. | Трекер вредоносных программ |
| Фильтр справочников по секциям | Используется для ведения списка посекционных фильтров для конкретных  панели мониторинга. | Фильтр анализа категорий HTTP |

**Внутренние справочники, которые можно редактировать**

Некоторые справочники заполняются данными по результатам поисковых запросов (справочники по поиску), некоторые можно редактировать вручную. В таблице ниже представлен список справочников, которые может потребоваться редактировать в Splunk Enterprise Security.

|  |  |  |  |
| --- | --- | --- | --- |
| **Название справочника** | **Описание** | **Пример** | **Подробности применения** |
| Рекомендательный список отслеживания истории действий с поисковыми запросами | Список | Добавляйте поисковые запросы в данный рекомендательный список, чтобы они не создавали элементы истории действий для последующего исследования. | Укажите 1 для **start\_time,** чтобы добавить поисковой запрос в рекомендательный список.Укажите **start\_time** и  **end\_time,** чтобы добавить поисковой запрос в рекомендательный список на определенный период времени. |
| Административные идентификационные данные | Список | Вы можете использовать данный справочник, чтобы разделить идентификационные данные на данные с особым статусом и административные данные на соответствующих панелях мониторинга, таких как панель мониторинга Центра Доступа и панель мониторинга Управления Аккаунтами. | Измените колонку **category,** чтобы обозначить особый статус аккаунта. Установите особый статус для аккаунтов по умолчанию с помощью функции  default|privileged, или укажите privileged для аккаунтов с особым статусом, которые не являются особыми по умолчанию, или default для аккаунтов, которые не являются особыми по умолчанию. |
| Протоколы приложений | Список | Используется панелью мониторинга Порт и протокол. | См. раздел Протоколы приложений |
| Категории ресурсов/идентификационных данных | Список | Вы можете использовать данную таблицу, чтобы установить категории для упорядочения ресурсов и идентификационных данных.  Общепринятые категории для ресурсов содержат стандарты соответствия и безопасности, такие как  PCI или функциональные категории, такие как сервер и web\_farm. Общепринятые категории для идентификационных данных содержат должности и роли. | См. раздел Ресурсы/Идентификационные данные |
| Ресурсы | Список ресурсов | Вы можете вручную добавить ресурсы в ваш справочник, чтобы он был включен в справочник, используемый для поиска корреляции ресурсов. | См. раздел Добавить ресурсы/идентификационные данные вручную |
| Демонстрационные ресурсы | Список ресурсов | Предоставляет образец ресурсов, который можно использовать в качестве примера или для демонстрации. | Отключите функцию использования справочника в производственной среде. См. раздел Отключить функцию демонстрации ресурсов и идентификационных данных в справочнике. |
| Демонстрационные идентификационные данные | Список идентификационных данных | Предоставляет образец идентификационных данных, который можно использовать в качестве примера или для демонстрации. | Отключите функцию использования справочника в производственной среде. См. раздел Отключить функцию демонстрации ресурсов и идентификационных данных в справочнике. |
| Настройка фильтра состояния Enterprise Security | Фильтр справочников по секциям | Посекционная фильтрация для настройки панели мониторинга о состоянии Enterprise Security. | См. раздел Настройка посекционного фильтра  в Splunk  Enterprise Security. |
| Ожидаемые просмотры | Список | Составляет список просмотров Enterprise  Security для аналитиков с целью регулярного мониторинга. | См. раздел Ожидаемые просмотры. |
| Фильтр анализа категорий HTTP | Фильтр справочников по секциям | Посекционная фильтрация панели мониторинга с Анализом категорий HTTP | См. раздел Настройка посекционного фильтра  в Splunk  Enterprise Security. |
| Анализ агента пользователя HTTP | Фильтр справочников по секциям | Посекционная фильтрация панели мониторинга с Анализом агента пользователя HTTP | См. раздел Настройка посекционного фильтра  в Splunk  Enterprise Security. |
| Идентификационные данные | Список идентификационных данных | Вы можете вручную редактировать данный справочник и добавлять идентификационные данные в справочник, используемый для поиска корреляции идентификационных данных. | См. раздел Добавить ресурсы/идентификационные данные вручную |
| Справочник идентификационных номеров эмитентов (ИНЭ) | Список | Статический список идентификационных номеров эмитентов (ИНЭ), используемый для определения подходящих номеров кредитных карт в событийных данных. | Используется для установления персонально-идентифицируемой информации по вашему событию. |
| Значимые порты | Список | Используется корреляционными поисками для определения портов, релевантных политике безопасности вашей сети. | См. раздел Значимые порты |
| Значимые процессы | Список | Используется корреляционными поисками для определения процессов, релевантных политике безопасности вашей сети. | См. раздел Значимые процессы |
| Значимые сервисы | Список | Используется корреляционными поисками для определения сервисов, релевантных политике безопасности вашей сети. | См. раздел Значимые сервисы |
| Локальный \* Intel | Справочник распознавания угроз | Используется для ручного ввода распознавания угроз. | См. раздел Добавление и поддержка распознавания угроз локально в Splunk Enterprise Security. |
| Категории модульных действий | Список | Используется для категоризации типов адаптивных действий реагирования, доступных для выбора. | Добавьте настраиваемую категорию, чтобы классифицировать настраиваемое действие адаптивного ответа на проверку инцидентов или на редактор поиска корреляции. |
| Анализ нового домена | Фильтр справочников по секциям | Посекционная фильтрация панели мониторинга с Анализом нового домена | См. раздел Настройка посекционного фильтра  в Splunk Enterprise Security. |
| Справочник домена PCI | Список идентификационных данных | Используется приложением Splunk  App для соответствия требованиям PCI с целью наполнения данными поля pci\_domain.  Содержит домены PCI, соответствующие стандарту PCI. | См. раздел Установка категорий ресурсов. |
| Первичные функции | Список | Определяет первичный процесс или сервис, запущенный на хосте.  Используется для поиска корреляции. | См. раздел Первичные функции. |
| Запрещенный трафик | Список | Определяет процесс и трафик, запрещенный в вашем окружении.  Используется для поиска корреляции. | См. раздел Запрещенный трафик. |
| Типы объектов риска | Список | Доступные типы объектов риска. | Отредактируйте справочник для создания настраиваемого типа объекта риска. Затем вы можете фильтровать новый тип рискового объекта или добавить новую запись о рисках на панеле мониторинга Анализа рисков.  См. раздел Создать риск и редактировать объект риска в Splunk Enterprise Security. |
| Домены безопасности | Список | Составляет список доменов безопасности, которые вы можете использовать для классификации значимых событий и во время разбора инцидентов. | Редактируйте справочник и добавляйте настраиваемый домен безопасности. |
| Фильтр угроз | Фильтр справочников по секциям | Посекционная фильтрация панели мониторинга с Анализом угроз. | См. раздел Настройка посекционного фильтра  в Splunk Enterprise Security. |
| Анализ объема трафика | Фильтр справочников по секциям | Посекционная фильтрация панели мониторинга с Анализом объема трафика. | См. раздел Настройка посекционного фильтра  в Splunk Enterprise Security. |
| Уровни срочности | Список | Данная таблица комбинирует приоритетность и строгость, которые определяют срочность значимых событий. | См. раздел Как значимым обытиям присваивается срочность в Splunk Enterprise Security в документе *Использование Splunk*  *Enterprise Security*. |
| Анализ длины URL | Фильтр справочников по секциям | Посекционная фильтрация панели мониторинга с Анализом длины URL. | См. раздел Настройка посекционного фильтра  в Splunk Enterprise Security. |

**Протоколы приложений**

Список протоколов приложений - это список комбинаций портов и протоколов и их статус в вашей организации. Этот список используется панелью мониторинга Трекер порта и протокола. См. панель мониторинга Трекер порта и протокола.

В этом файле доступны следующие поля.

|  |  |
| --- | --- |
| **Поле** | **Описание** |
| dest\_port | Номер порта назначения. Должен быть номер от 0 до 65535. |
| transport | Протокол сетевого трафика. Например, icmp, tcp или udp. |
| app | Имя приложения, использующего порт. |

**Категории Ресурсы/Идентификационные данные**

Список категорий может содержать любой набор категорий, которые вы выбираете для упорядочения ресурсов или идентификационных данных. Категория - это логическая классификация или группировка, используемая для ресурсов или идентификационных данных. Общепринятые категории для ресурсов содержат стандарты соответствия и безопасности, такие как PCI или функциональные категории, такие как сервер и web\_farm. Общепринятые категории для идентификационных данных содержат должности и роли. Дополнительные примеры см. в разделе «Редактирование ресурса или идентификационных данных в виде справочника в Splunk Enterprise Security».

Чтобы наполнить события данными о корреляции в категории ресурсов или идентификационных данных, вы должны поддерживать поле category в списках ресурсов или идентификационных данных, а не в списке категорий Ресурсы / Идентификационные данные. См. раздел «Редактирование ресурса или идентификационных данных в виде справочника в Splunk Enterprise Security».

Существует два способа поддержки списка категорий Ресурсы / Идентификационные данные.

***Запуск сохраненного поискового запроса для поддержки списка категорий.***

Splunk Enterprise Security включает в себя сохраненный поисковой запрос, который выбирает категории, определенные в списках ресурсов или идентификационных данных, и добавляет их в список категорий Ресурсы / Идентификационные данные.

По умолчанию поисковый запрос не запланирован.

1. В строке меню платформы Splunk выберите **Settings > Searches, reports, alerts**.
2. Определите местоположение сохраненного поискового запроса Identity - Make Categories - Lookup Gen.
3. Нажмите **Edit > Enable**.

***Ручная поддержка списка категорий***

Ведите список категорий вручную, напрямую добавляя категории в справочник.

По умолчанию вы должны вести список вручную.

1. Выберите **Configure >Content Management**.
2. Нажмите на список **Asset/Identity Categories**.
3. Добавьте новые категории в список.
4. Нажмите **Save**.

***Ожидаемые витрины***

Список ожидаемых витрин определяет перечень витрин Splunk Enterprise Security, мониторинг по которым проводится на регулярной основе. Панель мониторинга «Проверка витрины» использует этот справочник. Дополнительную информацию о справочнике можно найти в разделе «Проверка витрины».

Таблица ниже описывает поля, содержащиеся в этом файле.

|  |  |
| --- | --- |
| **Поле** | **Описание** |
| app | Приложение, содержащее витрину. Обычно оно устанавливается в SplunkEnterpriseSecuritySuite. |
| is\_expected | Истина или Ложь. Если иное не определено, Splunk Enterprise Security принимает по умолчанию, что витрины не подлежат мониторингу. |
| view | Название витрины. Доступно в URL или в панеле мониторинга Управление контентом. |

Чтобы найти название просмотра:

1. Перейдите к витрине в Enterprise Security.
2. Обратите внимание на последний сегмент URL-адреса, чтобы найти название витрины.

Например, просмотр в следующем URL-адресе называется incident\_review:

<https://127.0.0.1:8000/en-US/app/SplunkEnterpriseSecuritySuite/incident_review>

**Значимые порты**

Значимые порты содержат список портов TCP и UDP, которые считаются необходимыми, запрещенными или небезопасными по вашему расположению. Администраторы могут устанавливать политику, определяющую разрешенные и запрещенные порты, и изменять справочники в соответствии с этой политикой. Чтобы получать предупреждения, когда эти порты замечены в вашем окружении, включите поиск корреляции, который вызывает предупреждение для этих портов, например, «Обнаружена активность запрещенного порта».

Таблица ниже описывает поля, содержащиеся в этом файле.

|  |  |  |
| --- | --- | --- |
| **Поле** | **Описание** | **Пример** |
| app | Имя приложения или сервиса, использующего порт. | Win32Time |
| dest | Хост назначения для сервиса сети. Используйте подстановочный знак \* для соответствия всем хостам. | DARTH\*,  10.10.1.100,  my\_host. |
| dest\_pci\_domain | Дополнительный домен PCI. Принимает подстановочный знак. | trust, untrust |
| dest\_port | Номер порта назначения. Принимает подстановочный знак. | 443, 3389, 5900 |
| transport | Транспортный протокол. Принимает подстановочный знак. | tcp or udp |
| is\_required | Если необходимо, чтобы сервис работал, и вы хотите, чтобы корреляционный поиск создавал предупреждение в случае если он не запущен, установите значение true. | true or false |
| is\_prohibited | Если вы не хотите, чтобы порт использовался в вашей сети, и хотите, чтобы корреляционный поиск создавал предупреждение, в случае если он используется, установите значение true. | true or false |
| is\_secure | Если трафик, отправленный через порт, безопасен, установите значение true. | true or false |
| note | Описывает сервис с использованием порта и приводит пояснения по политике порта. | Нешифрованные службы telnet небезопасны. |

**Значимые процессы**

Значимые процессы содержат список процессов, по которому вы определяете, необходим ли процесс, запрещен ли он, либо безопасен для работы в вашей среде. Splunk Enterprise Security использует этот список при поиске корреляций в Обнаруженных запрещенных процессах.

Таблица ниже описывает поля, содержащиеся в этом файле.

|  |  |
| --- | --- |
| **Поле** | **Описание** |
| app | Название приложения |
| dest | Назначение процесса |
| dest\_pci\_domain | Домен PCI, в случае если доступен |
| is\_required | Если процесс должен выполняться на хосте назначения, установите значение true. Возможные значения: true или false. |
| is\_prohibited | Если процесс безопасен, установите значение true. Возможные значения: true или false. |
| is\_secure | Если процесс запрещен на хосте назначения, установите значение true. Возможные значения: true или false. |
| note | Опишите любую дополнительную информацию об этом процессе. Например, приложение telnet запрещено из-за небезопасной аутентификации. |

**Значимые сервисы**

Значимые сервисы содержат список сервисов по месту вашего расположения. Поиск корреляций в Обнаруженных запрещенных процессах использует данный справочник, чтобы определить, считать ли сервис необходимым, запрещенным или небезопасным.

Таблица ниже описывает поля, содержащиеся в этом файле.

|  |  |
| --- | --- |
| **Поле** | **Описание** |
| app | Название приложения |
| dest | Хост назначения, на котором работает сервис. |
| dest\_pci\_domain | Домен PCI, в случае если доступен |
| is\_required | Если процесс должен выполняться на хосте назначения, установите значение true. Возможные значения: true или false. |
| is\_prohibited | Если процесс запрещен на хосте назначения, установите значение true. Возможные значения: true или false. |
| is\_secure | Если процесс безопасен, установите значение true. Возможные значения: true или false. |
| note | Опишите любую дополнительную информацию об этом процессе. |

**Первичные функции**

Первичные функции содержат список первичных процессов, сервисов и их функции по вашему расположению. Используйте этот список, чтобы определить, какие службы являются первичными, а также порт и транспорт, которые будут использоваться сервисами. Этот справочник используется при поиске корреляций по нескольким обнаруженным первичным функциям.

Таблица ниже описывает поля, содержащиеся в этом файле.

|  |  |
| --- | --- |
| **Поле** | **Описание** |
| process | Название процесса |
| service | Название сервиса |
| dest\_pci\_domain | Домен PCI, в случае если доступен |
| transport | Протокол, используемый процессом для транспортировки. Возможные значения: tcp или udp. |
| port | Номер порта, используемый процессом. |
| is\_primary | Если процесс является первичным процессом на хосте назначения, установите значение true. Возможные значения: true или false. |
| function | Функция, которую выполняет процесс. Например, прокси, аутентификация, база данных, доменное имя сервиса (DNS), веб, или почтовый сервис. |

**Запрещенный трафик**

Запрещенный трафик группирует процессы, которые, если они видны в вашем сетевом трафике, могут показывать вредоносное поведение. Этот список используется панелью мониторинга Системный Центр и полезен для обнаружения программного обеспечения, которое запрещено вашей политикой безопасности, например, IRC, инструменты для уничтожения данных, программное обеспечение для передачи файлов, или известное вредоносное программное обеспечение, например, вредоносное ПО, которое стало распространяться относительно недавно.

Таблица ниже описывает поля, содержащиеся в этом файле.

|  |  |
| --- | --- |
| **Поле** | **Описание** |
| app | Название процесса (например, echo, chargen,и т.д.) |
| is\_prohibited | Если процесс запрещен в вашем окружении, установите значение true. Возможные значения: true или false. |
| note | Добавьте описание, почему этот процесс запрещен. |

**Создание риска и редактирование объектов риска в SplunkEnterprise Security**

Как администратор Enterprise Security, вы можете создавать и редактировать объекты риска.

**Создание нового объекта риска**

1. Из меню Enterprise Security выберите **Configure > Data Enrichment > Lists and Lookups** и выберите список **Risk Object Types**.
2. Выделите последнюю ячейку в таблице **risk\_object\_type** и вызовите редактор таблицы правой кнопкой мыши.
3. Добавьте новый ряд в таблицу.
4. Чтобы редактировать новый ряд, два раза щелкните по нему мышью, затем добавьте имя новому типу объекта.
5. Сохраните изменения.

**Редактирование существующего объекта риска**

1. В меню Enterprise Security выберите **Configure > Data Enrichment > Lists and Lookups**
2. Выберите список **Risk Object Types**.
3. Выделите тип объекта риска и измените имя.
4. Сохраните изменения.

**Конфигурация и Устранение неполадок**

**Конфигурация общих настроек для Splunk Enterprise Security**

В качестве администратора Splunk Enterprise вы можете изменять конфигурацию в вашей установке Splunk Enterprise Security. Измените пороговые значения, макроопределения, фильтры поиска и другие, как правило, заменяемые значения на странице общих настроек General Settings.

|  |  |
| --- | --- |
| В меню Enterprise Security, выбрать **Configure > General > General Settings.** | |
| **Настройка** | **Описание** |
| Asset Sources | Макрос поиска, который перечисляет таблицы просмотра, содержащие информационные ресурсы, используемые для корреляции ресурсов. |
| Auto Pause | Определяет время в секундах, до момента, когда детальный поиск будет приостановлен. |
| Default Watchlist Search | Определяет наблюдаемые события для поиска корреляций 'Watchlisted Events' (события списков просмотров). |
| Domain Analysis | Включает либо отключает WHOIS отслеживание для веб-доменов. |
| Domain From URL Extraction Regex | Обычное выражение, используемое чтобы извлечь домен (url\_domain) из URL. |
| Enable Identity  Generation  Autoupdate | Если «верно», позволяет Identity Manager автоматически обновить макросы asset\_sources, identity\_sources и generate\_identities. Верно по умолчанию. |
| Generic Error Search | Фильтр поиска для определения событий, указывающих на возникновение ошибки. |
| HTTP Category Analysis Sparkline Earliest | Установка времени запуска спарклайнов, отображенных на панели **HTTP User Category Analysis (Анализ категорий пользователя HTTP).** |
| HTTP Category Analysis Sparkline Span | Установка временного диапазона для спарклайнов, отображенных на панели **HTTP User Category Analysis (Анализ категорий пользователя HTTP).** |
| HTTP User Agent Analysis Sparkline  Earliest | Установка времени запуска для спарклайнов, отображенных на панели **HTTP User Agent Analysis** **(Анализ агента пользователя HTTP)**. |

|  |
| --- |
|  |

|  |  |
| --- | --- |
| HTTP User Agent Analysis Sparkline Span | Установка временного диапазона для спарклайнов, отображенных на панели **HTTP User Agent Analysis (Анализ агента пользователя HTTP)**. |
| IRT Disk Sync Delay | Устанавливает количество секунд для Enterprise Security, необходимых для ожидания завершения очистки диска. Относится к индексируемым поискам в реальном времени. |
| Identity Generation | Определяет изменения, необходимые для нормализации идентификационной информации. См. раздел «Как Splunk Enterprise Security обрабатывает и объединяет ресурсы и идентификационные данные». |
| Identity Generation Timeout | Количество секунд, которое ожидает Identity Manager, прежде чем предупредить о медленном завершении поиска в identity\_manager.log. |
| Identity Sources | Перечисляет исходные таблицы просмотров, содержащие идентификационную информацию. |
| Incident Review Analyst Capacity | Ожидаемый максимальный объем заметных событий, отведенных анализатору.  Относительная единица измерения рабочей нагрузки анализатора. |
| Indexed Realtime | Включает либо отключает указанный режим реального времени для поиска. |
| Large Email Threshold | Электронное сообщение, которое превышает данный размер в байтах, считается большим. |
| Licensing Event Count Rilter | Определяет перечень указателей для исключения из реферирования "Events Per Day" («события в день»). |
| Maximum Documents Per Batch Save (kvstore) | Максимальное количество документов, которое может быть сохранено одним пакетом в коллекции KV Store. |
| New Domain Analysis Sparkline Span | Установка временного диапазона для спарклайнов, отображенных на панели **New Domain Analysis (Анализ нового домена)**. |
| Notable Modalert Pipeline | SPL для ответного действия на заметные события. |
| Override Email Alert Action | Отменяет настройки почтового оповещения об опасности и позволяет пользователям отправлять заметные события по электронной почте путем адаптивных ответных действий на панели Incident Review (Оценка инцидентов). |
| Risk Modalert Pipeline | SPL для ответного действия преобразователя рисков. |
| Search Disk Quota  (admin) | Устанавливает максимальный объем дискового пространства в Mбайт, который  пользователь-администратор может использовать для хранения результатов поиска. |
| Search Jobs Quota (admin) | Установка максимального количества параллельных поисков, разрешенных пользователям-администраторам. |
| Search Jobs Quota (power) | Установка максимального количества параллельных поисков для опытных пользователей. |
| Short Lived Account Length | Запись по созданию и удалению аккаунта, которая превышает данный порог, является отклоняющейся от нормы. |
| TSTATS Allow Old Summaries | Включает либо отключает поиск ускорений моделей данных, содержащих поля, не соответствующие текущей конфигурации модели данных. |
| TSTATS Local | Определяет, будет ли распределен TSTATS макрос. |
| TSTATS Summaries Only | Определяет, будет ли TSTATS или макрос summariesonly искать только ускоренные события. |
| Use Other | Включает либо отключает понятие OTHER в схемах, превышающих границы серий по умолчанию. |
| Website Watchlist Search | Перечень наблюдаемых веб-сайтов, используемых поиском корреляции «События списка просмотра». |

**См. также**

Управление учетными данными ввода в Splunk Enterprise Security

Управление разрешениями в Splunk Enterprise Security

Персональная настройка панели меню в Splunk Enterprise Security

Конфигурация фильтра в панелях Splunk Enterprise Security

**Управление учетными данными в Splunk Enterprise Security**

Используйте страницу управления учетными данными **Credential Management**, чтобы хранить учетные данные для модульного ввода либо ввода по сценарию. Конфигурации ввода, отражающие учетные данные, используют учетные данные, сохраненные в Credential Management. Вы можете хранить учетные данные, такие как имя пользователя и пароль, или сертификаты, используемые для аутентификации сторонними системами. Не используйте данную страницу для управления сертификатами, используемыми для кодирования сообщений между серверами.

Ваша роль должна иметь соответствующие возможности для добавления, изменения и просмотра учетных данных и сертификатов. См. раздел «Конфигурация пользователей и ролей» в *Руководстве по Установке и Обновлению.*

**Добавление новых учетных данных для ввода**

1. В меню Enterprise Security выбрать **Configure > General > Credential Management.**
2. Нажать **New Credential** для добавления учетных данных нового пользователя.
3. Ввести имя пользователя **Name.**
4. (Опционально) Заполнить поле **Realm** для разграничения между многочисленными учетными данными, имеющими одинаковое имя пользователя.
5. Ввести пароль **Password** для учетных данных и повторно вписать его в поле **Confirm password.**
6. Выбрать the **App** для учетных данных.
7. Нажать **Save.**

**Редактирование существующих учетных данных ввода**

Вы можете редактировать пароли для существующих учетных данных ввода.

1. В менюEnterprise Security, выбрать **Configure > General > Credential Management.**
2. В столбце учетных данных **Action** нажать **Edit.**
3. Ввести новый пароль **Password** для учетных данных и вписать его повторно в поле **Confirm password.**
4. Нажать **Save.**

**Добавление нового сертификата**

Вы не можете добавить новый сертификат при помощи Credential Management на кластере search head cluster (SHC). Для добавления нового сертификата в Splunk Enterprise Security на кластере SHC, добавьте сертификат в $spLUNK\_HOME/etc/apps/<app\_name>/auth в установщике и укажите сертификат для членов SHC.

1. В менюEnterprise Security выбрать **Configure > General > Credential Management.**
2. Нажать **New Certificate** для добавления нового сертификата.
3. Ввести **File name** для сертификата. Это имя файла, под которым Сертификат сохранен в каталоге $SPLUNK\_HOME/etc/apps/<app\_name>/auth.
4. Добавить **Certificate text** для сертификата. Вставить сюда содержание существующего

файла сертификата для добавления сертификата в Splunk Enterprise Security.

1. Выбрать **App**, чтобы сохранить сертификат.
2. Нажать **Save.**

**Редактирование существующего сертификата**

Вы можете редактировать текст существующих сертификатов в Credential Management. Нельзя редактировать сертификаты на кластере search head cluster.

1. В меню Enterprise Security, выбрать **Configure > General > Credential Management.**
2. В столбце сертификата **Action** нажать **Edit.**
3. Ввести новый **Certificate text** для сертификата.
4. Нажать **Save.**

**Удаление существующих учетных данных ввода или сертификата**

Вы не можете удалить сертификаты на кластере search head cluster.

* + 1. В меню Enterprise Security выбрать **Configure > General > Credential Management.**
    2. В столбце **Action** учетных данных или сертификата нажать **Delete.**
    3. Нажать **OK** для подтверждения.

**Управление разрешениями в Splunk Enterprise Security**

Используйте Permissions page для просмотра и присвоения возможностей Enterprise Security ролям без прав администратора.

1. В меню Enterprise Security выбрать **Configure > General > Permissions.**
2. Выбрать окошко метки для роли и разрешения для данной роли.
3. Нажать **Save.**

Для получения дополнительной информации о возможностях ES см. раздел «Конфигурация пользователей и ролей» в *Руководстве по Установке и Обновлению*.

**Персональная настройка панели меню в Splunk Enterprise Security**

Настройте панель меню в Splunk Enterprise Security при помощи представления Edit Navigation (Редактирование навигации). Добавляйте новые **панели мониторинга,** уведомления, **представления,** ссылки на отфильтрованныепанели, либо ссылки на сеть в вашу панель меню. Необходимо обладать правами администратора Enterprise Security для внесения изменений в навигацию панели меню.

Вы можете добавлять представления в панель меню как часть коллекции, которая группирует несколько представлений вместе, либо как отдельный пункт в панели меню. Например, Incident Review – это отдельная панель мониторинга в меню, а Audit – это коллекция панелей контроля.

Splunk Enterprise Security сохраняет ваши настройки навигации с предыдущих версий.

**Проверка обновленных представлений**

Новые, обновленные Представления и коллекции, либо которые не были рекомендованы в версию приложения, которое вы установили, выделены маленькими значками, указывающими соответствующие изменения.

После установки новой версии Splunk Enterprise Security или новой версии приложения, которое предоставляет представления и коллекции для использования в Enterprise Security, посетите представление Edit Navigation для проверки обновлений в данных представлениях и коллекциях.

1. В меню Enterprise Security выбрать **Configure > General > Navigation.**
2. Если контент был обновлен, на вершине навигационного редактора появится сообщение "Some content updates available" («Доступны обновления контента»).
3. Найти значки представлений на панели редактора для определения контента, который был добавлен, обновлен либо не рекомендован. Те же самые значки также появляются в меню **Add a New View** и **Add a New Collection**.

**Установление представления по умолчанию для Splunk Enterprise Security**

Для просмотра определенного представления или ссылки, когда вы или другой пользователь открывает Splunk Enterprise Security, установите представление по умолчанию.

1. В меню Enterprise Security выбрать **Configure > General > Navigation.**
2. Разместить представление или ссылку, которые вы хотите установить по умолчанию.
3. Нажать значок галочки, который появляется, когда вы наводите мышь над представлением, чтобы установить его по умолчанию («**Set this as the default view**») .



1. Нажать **Save** для сохранения изменений.
2. Нажать **OK** для обновления страницы и отображения ваших изменений.

**Редактирование существующей навигации панели меню**

1. В меню Enterprise Security выбрать **Configure > General > Navigation**.
2. Нажать и перетащить представления или коллекции представлений для изменения расположения представления или коллекции представлений в меню.
3. Нажать **X** рядом с представлением или коллекцией для их удаления из меню.
4. Нажать , значок для редактирования имени коллекции.
5. Нажать - значок для добавления делителя и визуального разделения пунктов в коллекции.
6. Нажать **Save** для сохранения изменений.
7. Нажать **OK** для обновления страницы и отображения ваших изменений.

**Добавление отдельного представления на панель меню**

Вы можете добавить новое представление на панель меню, не добавляя его в коллекцию.

1. В меню Enterprise Security выбрать **Configure > General > Navigation**.
2. Нажать **Add a New View**.
3. Оставить **View Options set** по умолчанию.
4. Нажать **Select a View** в разделе **Unused Views**.
5. Выбрать панель или представление из списка.
6. Нажать **Save**. Панель появится в редакторе навигации.
7. Когда закончите добавлять позиции в меню, нажать **Save** для сохранения изменений.
8. Нажать **OK** для обновления страницы и отображения ваших изменений.

**Добавление коллекции на панель меню**

Используйте коллекцию, чтобы объединить несколько представлений или ссылок вместе в панели меню.

1. В меню Enterprise Security выбрать **Configure > General > Navigation**.
2. Нажать **Add a New Collection**.
3. Ввести имя **Name**. Например, **Audit**.
4. Нажать **Save**. Коллекция появится в редакторе навигации.

Вы должны добавить представление или ссылку на коллекцию, прежде чем они появятся в навигации меню.

**Добавление представления к существующей коллекции**

Добавьте представления к существующей коллекции.

1. В меню Enterprise Security выбрать **Configure > General > Navigation**.
2. Разместить коллекциию, к которой вы хотите добавить представления.
3. Нажать значок.
4. Оставить **View Options** по умолчанию.
5. Нажать **Select a View** в разделе **Unused Views**.
6. Выбрать представление из списка.
7. Нажать **Save**. Представление появляется в редакторе навигации.
8. Когда закончите добавлять позиции в меню, нажать **Save** для сохранения изменений.
9. Нажать **OK** для обновления страницы и отображения ваших изменений.

**Добавление ссылки на панель меню**

Вы можете добавить ссылку на панель меню Splunk Enterprise Security.Например, добавить ссылку на специально-отфильтрованное представление Incident Review или к внешней системе тикетов.

***Создание ссылки в меню к внешней системе или веб-странице***

1. В меню Enterprise Security выбрать **Configure > General > Navigation**.
2. Нажать **Add a New View**, чтобы добавить его в меню, или разместить существующую коллекцию и нажать значок, чтобы добавить ссылку на существующую коллекцию представлений.
3. Выбрать **Link** в разделе **View Options**.
4. Ввести имя **Name**, которое появится в меню Splunk Enterprise Security. Например, Splunk Answers.
5. Вписать ссылку. Например, https://answers.splunk.com/
6. Нажать **Save**.
7. Когда вы закончите добавлять позиции в меню, нажать **Save**, чтобы сохранить ваши изменения.
8. Нажать **OK** для обновления страницы и отображения ваших изменений.

***Добавление ссылки на фильтрованное представление Incident Review (Оценка инцидентов)***

Обычной ссылкой для добавления на панель меню является фильтрованное представление Incident Review.

1. Отфильтровать Incident Review при помощи желаемых вами фильтров. Когда вы фильтруете панель, URL обновляется в соответствии с запрашиваемыми параметрами ваших фильтров.
2. В адресной строке веб-браузера скопировать часть URL, которая начинается с

/арр/spiunkEnterprisesecuritySuite/ и вставить ее в простой текстовый файл для сравнения.

Например, если вы отфильтровали панель для показа только наиболее важных заметных событий, часть URL, которую вы копируете, выглядит как /app/SplunkEnterpriseSecuritySuite/incident\_review?form.selected\_urgency=critical

1. В меню Enterprise Security выбрать **Configure** > **General** >

**Navigation.**

1. Нажать **Add a New View**,чтобы добавить его в меню или разместить существующую коллекцию, и нажать **Add View,** чтобы добавить ссылку на существующую коллекцию представлений.
2. Выбрать **Link** в разделе **View Options.**
3. Ввести имя **Name**, которое появится в меню Splunk Enterprise Security. Например, **IR** - **Critical.**
4. В поле **Link** вставить часть URL. Например,

/app/SplunkEnterpriseSecuritySuite/incident\_review?form.selected\_urgency=critical

1. Нажать **Save.**
2. Когда вы закончите добавлять позиции в меню, нажать **Save**, чтобы сохранить изменения.
3. Нажать **OK** для обновления страницы и отображения ваших изменений.

Если вы добавляете ссылку со множеством параметров, вы должны модифицировать заданные параметры путем кодирования &, разделяя параметры как &amP;. Например, впишите ссылку на фильтрованное представление Incident Review, которая показывает новые и свободные заметные события как

/app/SplunkEnterpriseSecuritySuite/incident\_review?form.status\_form=l&amp;form.owner\_fо

Вы также можете создать URL вручную, используя параметры в нижеуказанной таблице. Используйте символ звездочки для отображения всех результатов для определенного параметра. Требуются не все параметры.

|  |  |  |  |
| --- | --- | --- | --- |
| **Параметр** | **Описание** | **Возможные значения** | **Пример** |
| form.selected\_urgency | Показ заметных событий в порядке  срочности, заданным данным параметром. | Critical(критично),  high (в большой степени),  medium (средне),  low (незначительно),  informational (для информации) | form.selected\_urgency=critical |
| form.status\_form | Показ заметных событий по статусу, заданному данным параметром. Целое число соответствует каждому значению статуса. | 0 для незадействованных,1 для новых,  2 для действующих, 3 для незаконченных,  4 для решенных,  5 для законченных | form.status\_form=0 |
| form.owner\_form | Показ заметных событий, принадлежащих пользователю, заданному данным параметром. | Имена пользователей | form.owner\_form=admin |
| form.source | Показ заметных событий, созданных поиском корреляций, заданным данным параметром. HTML кодировка указывается в имени поиска корреляций и использует имя, которое появляется в заметном событии, а не имя, которое появляется в Content Management (Управлении контентом). | Endpoint - Host With Multiple Infections – Rule | form.source=Endpoint%20-%20Host%20With%20Multiple%20Infections%20-%20Rule |
| form.rule\_name | Показ заметных событий, созданных  поиском корреляций, заданным данным параметром. HTML кодировка устанавливается в имени поиска корреляций. Используйте имя, которое возникает в Управлении Контентом. | Host With Multiple Infections | form.rule\_name=Host%20With%20Multiple%20Infections |

|  |  |  |  |
| --- | --- | --- | --- |
| form.tag | Показывает заметные события с тегом, заданным данным параметром. | malware (вредоносное ПО),  any custom tag value (значение любого пользовательского тега) | form.tag=malware |
| form.srch | Показывает заметные события, соответствующие SPL, заданному данным параметром. HTML кодировка специальных символов, таких как = для пар "ключ - значение". | dest=127.0.0.1 | form.srch=dest%3D127.0.0.1 |
| form.security\_domain\_form | Показывает заметные события в домене безопасности, заданном данным параметром. | Access (доступ), endpoint (конечная точка), network (сеть), threat (угроза), identity (идентификация) | form.security\_domain\_form=endpoint |
| earliest= и latest= | Показывает заметные события во временном диапазоне, заданном данными  параметрами. Устанавливает относительный временной диапазон. HTML кодировка специальных символов, таких как @. | -24h@h, now | earliest=-24h%40h&latest=now |
| form.new\_urgency\_count\_form | Показывает несрочные заметные события, заданные данным параметром. | Critical , high, medium, low, informational. | form.new\_urgency\_count\_form=informational |
| form.selected\_urgency | Показывает срочные заметные события, заданные данным параметром. Используйте многократные объекты данного параметра, чтобы выбрать многочисленные настройки срочности. | Critical , high, medium, low, informational | form.selected\_urgency=critical&form.selected\_urgency=high |
| event\_id | Показывает заметное событие, которое соответствует заданному event\_id. | 3C84A9D8-87F6-4066-8659-C7DD680F98E6@@notable@@80e0f89da83cad6665dd1de7447cedb4 | event\_id=3C84A9D8-87F6-4066-8659-C7DD680F98E6@@notable@@80e0f89da83cad6665dd1de7447cedb4 |
| form.association\_type  form.association\_id | Употребленные совместно, показывают заметные события, связанные с short ID или поиском. | short\_id, investigation  EYIYNW, 5a4be2b8cdc9736b2352c7c3 | form.association\_type=short\_id&form.association\_id=EYIYNW |

**Восстановление навигации по умолчанию**

Восстановить навигацию меню Splunk Enterprise Security по умолчанию:

1. В меню Enterprise Security выбрать **Configure > General > Navigation**.
2. В верхнем правом углу нажать **Restore Default Configuration**.
3. Нажать **OK** для подтверждения.
4. Прокрутить вниз страницы и нажать **Save**.

**Конфигурация расширенной фильтрации в Splunk Enterprise Security**

Некоторые панели в Splunk Enterprise Security включают опцию расширенной фильтрации, при помощи которой можно фильтровать позиции вне представлений панели, упрощая поиск тех событий, которые требуют рассмотрения.

• Если вы определили, что событие является угрозой, используйте редактор расширенной фильтрации, чтобы добавить позицию в ваш черный список известных угроз.

• Если вы определили, что событие не является угрозой, вы можете добавить его в белый список, чтобы убрать из представления панели.

Кнопка расширенной фильтрации появляется только в случае, если у пользователя есть разрешение. Для конфигурации данного разрешения см. раздел «Конфигурация пользователей и ролей» в *Руководстве по Установке и Конфигурации*.

**События Белого Списка**

После того, как вы определили, что событие не является угрозой, вы можете внести его в белый список, чтобы скрыть его из представления панели. После того, как вы внесете событие в белый список, сводная статистика продолжит подсчитывать внесенные в него позиции, при этом данные позиции не будут отражены на панели.

***Внесение события в белый список***

Используйте расширенный фильтр, чтобы внести события в белый список, либо отфильтровать на панели.

Например, внести в белый список события трафика на панели Traffic Size Analysis:

1. Использовать прямоугольники для пометки выбранного режима, чтобы выбрать позиции для фильтрования.
2. Нажать **Per-panel Filter** в верхнем правом углу, чтобы показать опции для событий, которые могут быть отфильтрованы на данной панели.
3. Выбрать переключатель, чтобы отфильтровать события на данной панели.
4. Например, на панели **Traffic Size Analysis** вы можете, как фильтровать события, чтобы они больше не появились, так и выделить их, чтобы они были отмечены как важные.
5. Нажать **Save**,когда вы закончили.

В данном примере после того, как позиция была добавлена в белый список, она больше не считается угрозой и больше не появляется на панели **Traffic Size Analysis**.

***Исключение позиции из белого списка***

* 1. Нажать **Per-panel Filter,** затем **View/edit lookup file** для просмотра списка элементов, которые недавно были отфильтрованы.
  2. Нажать правой кнопкой мыши по ячейке таблицы для просмотра контекстного меню.
  3. Выбрать **Remove row**, чтобы убрать строку, содержащую позицию, внесенную в белый список.
  4. Нажать **Save.**

**События Черного Списка**

Событие также может быть внесено в черный список. Внесение позиции в черный список означает, что вы идентифицировали событие как вредоносное, или подумали поддержать связь с командой или контрольным сервером, которые являются вредоносными. Каждый раз, когда событие или строка показываются в данных, вы захотите исследовать систему, пользователя, связанного с системой или сетевую деятельность, чтобы понять природу и возможное распространение угрозы.

Внесение события или строки в черный список идентично внесению в белый список. События могут быть внесены в черный список только после того, как они были отфильтрованы на панели.

Чтобы внести в черный список событие трафика, например, панель **Traffic Size Analysis**, выполните следующие действия:

1. Нажать **Per-panel Filter,** затем **View/edit lookup file** для просмотра списка элементов, которые недавно были отфильтрованы.
2. Разместить элемент, который вы хотите добавить в черный список. Под столбцом **filter** дважды нажмите слово«whitelist» для редактирования ячейки. Удалите «whitelist» и впишите «blacklist».
3. Нажмите **Save.**

**Редактирование списка расширенных фильтров**

Для просмотра текущего списка расширенных фильтров на панели выберите **Configure > Content Management**. Таблицы просмотра с описанием, указывающим, что они относятся к расширенным фильтрам, показывают текущие расширенные фильтры для панели в имени поиска. События, добавленные в белый список для панели, перечислены в данных таблицах просмотра.

Например, таблица просмотра **Threat Activity Filter** показывает фильтры для панели **Threat Activity**.

Редактировать таблицу просмотра расширенного фильтра.

1. Открыть список фильтров для соответствующей панели. Название фильтра, например, ppf\_threat\_activity, показано в верхнем левом углу.
2. Чтобы отредактировать фильтр, выбрать ячейку и начать вводить текст.
3. Чтобы вставить или убрать строку или столбец в разделе фильтр, нажать правой кнопкой мыши по полю для редактирования. Удаление строки, добавляет данную позицию назад на панель представления и убирает ее из белого списка.
4. Чтобы «blacklist» (внести позицию в черный список), использовать редактор для добавления в таблицу и выбрать "blacklist" в столбце "filter".
5. Нажать **Save**, чтобы сохранить изменения.

***Выполнение аудита расширенных фильтров***

Изменения, совершенные для расширенных фильтров, зарегистрированы в журналах регистрации расширенных фильтров. Редактор просмотров и модуль расширенных фильтров изменяют расширенные фильтры. Используйте панель Per-Panel Filter Audit,чтобы выполнить проверку расширенных фильтров.

**Создание Веб-сообщения Splunk в Splunk Enterprise Security**

Создайте сообщение в Splunk Web, основанное на результатах поиска, используя оповещение Create Splunk messages. Только администраторы могут создавать сообщения, используя данное оповещение.

Сообщение, которое вы создаете с помощью данного оповещения должно уже существовать в messages.conf. Смотрите раздел «Настройка Веб-сообщений Splunk» в *Руководстве Администратора* Splunk Enterprise для дополнительной информации о создании сообщений.

1. Вы можете создать Веб-сообщения Splunk из поиска или из поиска корреляций:

|  |  |
| --- | --- |
| **Опция** | **Шаги** |
| **Создать новое оповещение** | На странице **Search** в приложении **Search and Reporting** выбрать **Save As** > **Alert.** Вписать и выбрать детали оповещения и задать нужную конфигурацию, запуск или приостановка. |
| **Создать или редактировать поиск корреляций** | В меню ES выбрать **Configure > Content Management.** Выбрать **Create New Content > Correlation Search.** Вписать и выбрать нужную конфигурацию поиска корреляций. |
| **Редактировать поиск корреляций** | В меню ES выбрать **Configure > Content Management.** Выбрать поиск корреляций. |

1. Нажать **Add Actions** и выбрать **Create Splunk messages.**
2. Выбрать **Name.** Имя соответствует строке в messages.conf существующего сообщения.

Например, DISK\_MON:INSUFFICIENT\_DISK\_SPACE\_ERROR.

1. (Опционально) Ввести **Message ID**, которое идентифицирует сообщение.

Например, insufficient\_diskspace.

1. (Опционально) Если сообщение использует поле подстановки, введите **Fields** для использования. Поля, используемые для подстановки аргумента, должны быть возвращены в результаты поиска для включения в сообщение. Впишите поля в порядке, в котором они должны быть подставлены в сообщении.

Например, для сообщения Host %s has free disk space %d, below the minimum 5GB., введите поля src,FreeMBytes.

1. (Опционально) Выбрать **Yes** для **Keep Only Latest** иоставить только последнее сообщение, выполненное поиском.

Например, если хост имел низкий объем дискового пространства в течение трех дней, вместо того, чтобы каждый день в течение трех дней получать сообщения, выберите **Yes** для данной настройки, чтобы видеть только одно сообщение.

1. Нажать **Save.**

**Выявление ошибки скрипта в Splunk Enterprise Security**

Выявите ошибки скрипта из модульного ввода в Splunk Enterprise Security. Если вы видите сообщение об ошибке завершения скрипта, или о скрипте, который находится в неизвестном состоянии, исследуйте скрипт и строку, которая произвела ошибку. Поиск Audit - script Errors замещает скрипт проверки конфигурации и

создает сообщения Splunk, чтобы предупредить о ненулевых кодах выхода, которые возникли из скриптов в вашем развертывании Splunk.

|  |  |  |
| --- | --- | --- |
| **Возможная основная причина** | **Проверка** | **Смягчение последствий** |
| Скрипт не завершился успешно. | Проверить файлы журнала регистрации для скрипта. Выполнить скрипт вручную, чтобы посмотреть, успешно ли он протекает, и проверить код завершения, который получается в результате. | Исследовать причины, почему скрипт завершился с ненулевым кодом выхода. |
| Скрипт завершился успешно с ненулевым кодом выхода. | Выполнить скрипт вручную, чтобы посмотреть, успешно ли он протекает, и проверить код завершения, который получается в результате. | |  | | --- | | Включить скрипт в режим уменьшения воздействия для поиска, чтобы он не показывал сообщения для данного скрипта. | |
| Скрипт находится в неизвестном состоянии. Известна конечная точка выполнения скрипта, но нет статуса завершения или начальной точки. | Проверить настройки модульной системы ввода, чтобы убедиться в их верности. | Исправить настройки модульной системы ввода. |

**Предупреждение сообщения об особых скриптах**

В случае необходимости, вы можете предупредить сообщения об особых скриптах, путем изменения сочетания порядка в макросе 'script\_error\_msg\_ignore'.

Если вы локально определили регулярные выражения блокировки скрипта в строке

[conf iguration\_check: //conf check\_script\_errors], вы можете копировать его в макрос. Например, строка блокировки включает следующие регулярные выражения:

suppress = ((streamfwd|splunk-(wmi\.path|MonitorNoHandle\.exe|winevtlog\.exe|netmon\.exe|perfmon\.exe|regmon\.exe|winprintmon\.exe|admon\.exe)).\*exited with code 1)

Макрос копирует данную блокировку следующим определением:

match(script, "(streamfwd|splunk-(wmi\.path|MonitorNoHandle\.exe|winevtlog\.exe|netmon\.exe|perfmon\.exe|regmon\.exe|winprintmon\.exe|admon\.exe|powershell\.exe))") AND exit\_status=1

Чтобы уменьшить частоту сообщений об особых скриптах, а не предупредить

их появление, приостановите оповещения. Установите приостановку оповещений для поиска Audit - Script Errors, основанном на необходимых значениях, как например, поле script.

* + Для Splunk Enterprise, см. раздел « Приостановление оповещений» в *Руководстве по Оповещениям.*
  + Для Splunk Cloud, см. «Приостановление оповещений» в *Руководстве по Оповещениям.*

**Сообщения о выявлении неполадок в индексах по умолчанию, поиск которых задает администратор**

Сообщения о выявлении неполадок системы Splunk в индексах по умолчанию, поиск которых задает администратор на платформе Splunk.

**Поиски, по умолчанию осуществляемые администратором, включают сводные индексы.**

Когда пользователь-администратор ищет сводные индексы по умолчанию, можно наблюдать замедленное быстродействие. Вы можете прекратить показ сообщений о данной настройке путем ограничения индексов, которые осуществляет администратор или путем отмены поиска.

***Ограничение индексов, поиск которых осуществляет администратор***

Предупредите поиск сводных индексов администратором. Вы можете идентифицировать имена сводных индексов, поскольку имена индексов заканчиваются как in .summary, например, endpoint\_summary.

1. Выбрать **Settings > Access controls.**
2. Нажать **Roles.**
3. Нажать **admin.**
4. В разделе **Indexes** нажать любой сводный индекс, чтобы убрать его из выбранных индексов.
5. Нажать **Save.**

***Прекращение поиска для предупреждения сообщений***

Если вы не хотите ограничивать индексы, поиск которых осуществляет администратор, но вы хотите остановить показ сообщений, прекратите поиск.

1. Выбрать **Settings > Searches, reports, and alerts.**
2. Разместить поиск **Audit - Default Admin Search Indexes**.
3. Выбрать **Edit** > **Disable.**
4. Нажать **Disable.**

**Сообщения неисправности о необязательном праве доступа на считывание или запись анализа коллекций хранилища KV Store**

Сообщения неисправности Splunk Web о ролях, которые обладают необязательным правом доступа на считывание или запись анализа коллекций хранилища KV Store.

В Splunk Web можно встретить следующие сообщения неисправности:

Health Check: Review roles for unnecessary read or write access to the investigation\_attachment collection and remove access if possible

Health Check: Review roles for unnecessary read or write access to the investigation\_event collection and remove access if possible

Health Check: Review roles for unnecessary read or write access to the investigation\_canvas\_entries collection and remove access if possible

Health Check: Review roles for unnecessary read or write access to the files collection and remove access if possible

Health Check: Review roles for unnecessary read or write access to the investigation collection and remove access if possible

Health Check: Review roles for unnecessary read or write access to the investigative\_canvas collection and remove access if possible

Эти сообщения выдает сохраненный поиск Audit – Investigation Collection ACLs.

Поиск направлен на обнаружение не администраторских прав доступа к анализу коллекций KV Store.

**Удаление необязательного права доступа на считывание или запись из коллекций**

Если вы видите эти сообщения, удалите соответствующие коллекции [collections/<stanza\_name>] из директории $SPLUNK\_HOME/etc/apps/SplunkEnterpriseSecuritySuite/metadata/local.meta.

Рекомендуется предоставлять доступ к данным коллекциям только ролям с администраторскими правами. После внесения изменений, обновите кеш файла из Splunk Web:

http://<yoursplunkserver>8000/en-us/debug/refresh?.

В поисковом блоке кластерной среды внесите изменения в файл local.meta для каждого члена кластера, далее обновите кеш файла из Web Splunk для каждого поискового блока: http://<yoursplunkserver>:8000/en-us/debug/refresh?.

**Поиски администратором по умолчанию включают все внешние индексы**

Когда администратор осуществляет поиск всех внешних индексов по умолчанию, вы можете наблюдать замедленное быстродействие. Вы можете прекратить показ сообщений о данной настройке путем ограничения индексов, которые осуществляет администратор или путем отмены поиска.

***Ограничение индексов, поиск которых осуществляет администратор***

Предупредите администратора от поиска всех внешних индексов.

1. Выбрать **Settings > Access controls.**
2. Нажать **Roles.**
3. Нажать **admin.**
4. В разделе **Indexes** нажать **All non-internal indexes**, чтобы убрать их из выбранных индексов.
5. Нажать **Save.**

***Прекращение поиска для предупреждения сообщений***

Если вы не хотите ограничивать индексы, поиск которых осуществляет администратор, но желаете остановить показ сообщений, прекратите поиск.

1. Выбрать **Settings > Searches, reports, and alerts.**
2. Разместить поиск **Audit - Default Admin Search All Non-Internal**.
3. Выбрать **Edit > Disable.**
4. Нажать **Disable.**

**Выявление неполадок отказа загрузки системы распознавания в Splunk Enterprise Security**

Если вы получили сообщение о том, что не удалось загрузить список угроз, существует несколько возможных основных причин.

|  |  |  |
| --- | --- | --- |
| **Возможные ключевые причины** | **Проверка** | **Смягчение последствий** |
| Угроза или источник распознавания больше не доступен по IP адресу или URL. | Попробовать посетить URL или выполните curl вручную. | Отключить источник распознавания, если его больше нельзя загрузить. |

|  |  |  |
| --- | --- | --- |
| Настройки брандмауэра или прокси предупреждают распознавания от доступа. | Проверить, видите ли вы URL, или выполните curl источника поиска информации вручную на другом устройстве. | Изменить настройки брандмауэра или прокси, чтобы разрешить доступ к источнику распознавания. |

**Панели устранения неполадок в Splunk Enterprise Security**

Каждая панель в Enterprise Security отражает данные из разных моделей данных. Без соответствующих данных, панели будут пустыми. Если вы ожидаете появление данных, или возникающие данные старше, чем вы рассчитывали, следуйте данным шагам устранения неполадок.

1. Выполнить поиск модели данных. Нажать **Open in Search** в нижнем левом углу панели представления, чтобы осуществить прямой поиск модели данных. Панель **New Search** также показывает поисковые команды и объекты, используемые для заполнения определенного представления.
2. Если поиск не приносит результатов, установить, доступны ли в модели данных любые данные, необходимые для панели.

1. См. раздел «Матрица требований к панелям мониторинга» в данном руководстве, чтобы определить модель данных массива, используемых панелью.

2. Использовать модель данных и массив модели данных для поиска событий в модели данных.

|  |  |  |
| --- | --- | --- |
| **Действие** | **Поиск** | **Ожидаемый результат** |
| Удостовериться, что данные приведены в соответствии с Общей Информационной Моделью. | | datamodel **data\_model\_name root\_object\_name** search | table Jime, sourcetype, **root\_object\_name**.\*  Например,  I datamodel Network\_Traffic All\_Traffic search ! dedup sourcetype I table \_time, sourcetype, All\_Traffic.\* | Возвращает перечень типов источников, объектов модели данных и полей, заполненных данным типом источника. |

1. Если данные недоступны, подтвердить ускорение модели данных.

1. В Enterprise Security перейти к **Audit > Data Model Audit**.

2. Просмотреть панель **Acceleration Details** на предмет информации о статусе ускорения модели данных, завершена ли она на 100%. См.

раздел «Конфигурация моделей данных для Splunk Enterprise Security» в *Руководстве по Установке и Обновлению*.

1. Если статус ускорения модели данных является ожидаемым, подтвердить, что доступны дополнительно необходимые источники данных. Например, панель **User Activity** использует дополнительные источники данных.

|  |  |  |
| --- | --- | --- |
| **Название**  **Панели** | **Тип данных** | **Источник данных** |
| User Activity (Активность пользователя) | Просмотры | |  | | --- | |  |   Файлы просмотров **Cloud Domains, Corporate Email Domains** и **Corporate Web Domains**. |
| Идентификаторы | Поля идентификаторов: bunit, email,  watchlist, work\_city, work\_country,  work\_iat, и work\_iong. Для дополнительной информации, см. раздел «Поля просмотра идентификаторов» в данном руководстве. |
| Поиски корреляций | \* Высокая Почтовая Активность С Некорпоративными Доменами  \* Наблюдаемое Событие Списка Просмотров  \* Веб-загрузки, Осуществляемые Пользователями На Некорпоративные Сайты. |
| Access  Anomalies  (Дефекты доступа) | Поиски корреляций | \* Невозможные События Перемещений, Замеченные Для Пользователей. |

**Матрица требований к панелям мониторинга для Splunk Enterprise Security**

Панели мониторинга Enterprise Security полагаются на события, которые подчиняются Общей Информационной Модели (CIM), и заполняются из ускорений моделей данных, если иное не отмечено.

**Модель соотношения панели мониторинга и данных**

***А - Е***

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Название Панели Мониторинга** | | **Заголовок Панели** | | | | | **Модель Данных** | | | | | | **Набор Данных**  **Модели данных** |
| Access Anomalies (Дефекты доступа) | | Geographically Improbable Accesses (Географически невозможные доступы) | | | | | Полагается на сводный индекс the gia\_summary,  который заполняется поиском **Access - Geographically Improbable Access - Summary Gen**. Данный поиск отражает модель Authentication | | | | | | Authentication.app, .src, .user |
| Concurrent Application Accesses (Одновременные Доступы ) | | | | | Authentication | | | | | | Authentication.app, .src, .user |
| Access Center (Центр доступа) | | Access Over Time By Action (Сверхурочный доступ через действие) | | | | | Authentication | | | | | | Authentication.action |
| Access Over Time By App (Сверхурочный доступ через приложение) | | | | | Authentication.app |
| Top Access By Source  (Главный доступ к ресурсам) | | | | | Authentication.src |
| Top Access By Unique User (Главный доступ уникального пользователя) | | | | | Authentication.user,.src |
| Access Search (Поиск доступа) | | | | | | | Authentication.action, .app, src, .dest, .user, src\_user |
| Access Tracker (Система отслеживания доступа) | First Time Access (Первый доступ) – Длительность 7 дней | | | | | | Отсутствует. Вызывает просмотр access\_tracker | | | | | | |
| Inactive Account Usage (Пользование неактивным аккаунтом) - Длительность 90 дней | | | | | |
| Completely Inactive Accounts (Полностью неактивные аккаунты) - Длительность 90 дней | | | | | |
| Account Usage For Expired Identities (Пользование аккаунтом для истекших идентификаторов) – Длительность 7 дней | | | | | | Authentication | | | | | Authentication.dest | |
| Account Management (Управление аккаунтом) | Account Management Over Time (Сверхурочное управление аккаунтом ) | | | | | | Account Changes | | | | | All\_Changes.Account\_Management, .action | |
| Account Lockouts  (Блокировка аккаунта) | | | | | | All\_Changes.Account\_Management, .result | |
| Account Management By Source User (Управление аккаунтом пользователя ресурсов) | | | | | | All\_Changes.Account\_Management, .src\_user | |
| Top Account Management Events (События управления главным аккаунтом) | | | | | | All\_Changes.Account\_Management, .action | |
| Asset Center  (Центр ресурсов) | Assets By Priority (Ресурсы по приоритету) | | | | | | [Assets And Identities](http://docs.splunk.com/Documentation/ES/5.1.0/Install/Datamodels#Assets_And_Identities) | | | | | All\_Assets.priority, .bunit, .category, .owner | |
| Assets By Business Unit (Ресурсы по бизнес-единицам) | | | | | |
| Assets By Category (Ресурсы по категориям) | | | | | |
| Asset Information (Информация о ресурсах) | | | | | |
| Asset Investigator (Исследователь ресурсов) | Asset Investigator (Исследователь ресурсов) | | | | | | Основывается на выборе событийных линий | | | | | | |
| **Название Панели Мониторинга** | | | | | **Заголовок Панели** | **Модель Данных** | | | **Набор данных**  **Модели Данных** | | | | |
| Data Protection (Защита данных) | | | | | Data Integrity Control By Index (Контроль целостности данных по индексу) | Incident Management | | | | | | | |
| Sensitive Data (Чувствительные данные) | Отсутствует. Вызывает поиск REST в индексах, проверяя выполнение контроля целостности данных. | | | | | | | |
| Default Account Activity (Активность аккаунта по умолчанию) | | | | | Default Account Usage Over Time By App (Сверхурочное пользование аккаунтом по умолчанию через приложение) | Authentication | | | | Authentication.Default\_Authentication, .action, .app | | | |
| Default Accounts In Use (Аккаунты по умолчанию в пользовании) | Authentication.user\_category, .dest, .user | | | |
| Default Local Accounts (Локальные Аккаунты по Умолчанию) | Нет. Вызывает просмотр useraccounts\_tracker | | | | | | | |
| DNS Activity (Активность DNS) | | | | | Top Reply Codes By Unique Sources (Главные коды ответа по уникальным ресурсам) | Network Resolution DNS | | | DNS.message\_type, DNS.reply\_code | | | | |
| Top DNS Query Sources (Главные источники запросов DNS) | DNS.message\_type, DNS.src | | | | |
| Top DNS Queries (Главные запросы DNS) | DNS.message\_type, DNS.query | | | | |
| Queries Per Domain (Запросы домена) | DNS.message\_type, DNS.query | | | | |
| Recent DNS Queries (Недавние запросы DNS) | DNS.message\_type | | | | |
| DNS Search (Поиск DNS) | | | | | | DNS.message\_type, DNS.reply\_code, DNS.dest, DNS.src ,DNS.query\_type, DNS.query, DNS.answer | | | | |
| **Название Панели Мониторинга** | | | **Заголовок Панели** | | | | | **Модель Данных** | | | **Массив Модели Данных** | | | |
| Email Activity (Почтовая активность) | | | Top Email Sources (Главные источники электронных сообщений) | | | | | [Email](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Email) | | | All\_Email.src | | | |
| Large Emails (Большие электронные сообщения) | | | | | All\_Email.size, src, .src\_user, .dest | | | |
| Rarely Seen Senders (Редко встречающиеся отправители) | | | | | All\_Email.protocol, .src, .src\_user, .recipient | | | |
| Rarely Seen Receivers (Редко встречающиеся получатели) | | | | | All\_Email.protocol, .src, .recipient | | | |
| Email Search (Почтовый поиск) | | | | | | | | All\_Email.protocol, .recipient, .src, .src\_user, .dest | | | |
| Endpoint Changes (Изменения конечной точки) | | | | Endpoint Changes By Action (Изменения конечной точки через действие) | | | | [Change Analysis](http://docs.splunk.com/Documentation/CIM/4.11.0/User/ChangeAnalysis) | | | All\_Changes.Endpoint\_Changes, .action | | | |
| Endpoint Changes By Type (Изменения конечной точки по типу) | | | | All\_Changes.Endpoint\_Changes, .object\_category | | | |
| Endpoint Changes By System (Изменения конечной точки системой) | | | | All\_Changes.Endpoint\_Changes, .object\_category, .dest | | | |

### *F - M*

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Название Панели Мониторинга** | | | | **Заголовок Панели** | | **Модель данных** | | **Набор Данных**  **Модели Данных** | | | | |
| Forwarder Audit (Проверка экспедитора) | | | | Event Count Over Time By Host (Сверхурочное количество событий с хоста) | | Отсутствует. Вызывает макрос host\_eventcount и поиск. | | | | | | |
| Hosts By Last Report Time (Хосты по времени последнего отчета) | |
| Splunkd Process Utilization (Использование процесса Splunkd) | | [Application State](http://docs.splunk.com/Documentation/CIM/4.11.0/User/ApplicationState) | | | | | All\_Application\_State.Processes.cpu\_load\_percent, .mem\_used, .process, All\_Application\_State.dest | |
| Splunk Service Start Mode (Режим запуска сервиса Splunk) | | All\_Application\_State.Services.start\_mode, .status, .service | |
| HTTP Category Analysis (Анализ категорий HTTP) | | | | Category Distribution (Распределение по категориям) | | [Web](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Web) | | | | | Web.src, .category | |
| Category Details (Детали категорий) | | Web.src, .dest, .category, | |
| HTTP User Agent Analysis (Анализ агента пользователя HTTP) | | | | User Agent Distribution (Распределение по агенту пользователя) | | [Web](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Web) | | | | | Web.http\_user\_agent\_length, .http\_user\_agent | |
| User Agent Details (Детали агента пользователя) | | Web.http\_user\_agent\_length, .src, .dest, .http\_user\_agent | |
| **Название Панели Мониторинга** | | | | | **Заголовок Панели** | **Модель Данных** | | | | | **Набор Данных**  **Модели Данных** |
| Identity Center (Центр идентификации) | | | | | Identities By Priority (Идетификация по приоритету) | [Assets and Identities](http://docs.splunk.com/Documentation/ES/5.1.0/Install/Datamodels#Assets_And_Identities) | | | | | All\_Identities.priority, .bunit, .category |
| Identities By Business Unit (Идентификация по бизнес-единицам) |
| Identities By Category (Идентификация по категориями) |
| Identity Information (Идентификационная информация) |
| Identity Investigator (Исследователь идентификации) | | | | | Identity Investigator (Исследователь идентификации) | Основан на выборе событийных линий. | | | | | |
| Incident Review Audit  (Аудит Анализа Инцидентов) | | | | | Review Activity By Reviewer (Активность анализатора) | Отсутствует. Вызывает поиск по коллекции es\_notable\_events KV Store. | | | | | |
| Top Reviewers (Главные анализаторы) |
| Notable Event By Status (Заметные события по статусу) – Длительность 48 часов. |
| Notable Events By Owner - Last 24 hours (Заметные события владельца) – Длительность 24 часа. |
| Recent Review Activity (Недавняя активность Анализа) |
| Indexing Audit (Проверка индексирования) | | | | | Events Per Day Over Time (Сверхурочные события в день) | Отсутствует. Вызывает поиск по коллекции licensing\_epd KV Store. | | | | | | | |
| Events Per Day  (События в день) |
| Events Per Index (Last Day) (События по Индексу) (Последнего дня) |
| Intrusion Center (Центр атак) | | | | | Attacks Over Time By Severity (Сверхурочные атаки по тяжести) | [Intrusion Detection](http://docs.splunk.com/Documentation/CIM/4.11.0/User/IntrusionDetection) | | | IDS\_Attacks.severity | | | | |
| Top Attacks (Главные атаки) | IDS\_Attacks.dest, .src, .signature | | | | |
| Scanning Activity (Many Attacks) (Сканирование атак)(Много атак) | IDS\_Attacks.signature | | | | |
| New Attacks (Новые атаки) | IDS\_Attacks.ids\_type | | | | |
| Intrusion Search (Поиск атак) | | | | | | IDS\_Attacks.severity, .category, .signature, .src, .dest | | | | |
| Investigations (Расследования) | | Investigations (Расследования) | | | | Отсутствует. Вызывает поиск по коллекции investigation KV Store. | | | | | | | |
| Investigation timelines (Временная шкала Расследования) | | | | Отсутствует. Вызывает поиск по коллекции investigation\_event KV Store collection. | | | | | | | |
| Investigation note attachments (Приложения к записи расследования) | | | | Отсутствует. Вызывает поиск по коллекции investigation\_attachment KV Store. | | | | | | | |
| Action history (История действий) | | | | Отсутствует. Вызывает один из пяти типов поиска. См. «Управление расследованиями в [Splunk Enterprise Security](http://docs.splunk.com/Documentation/ES/5.1.0/Admin/Manageinvestigations)». | | | | | | | |
| Investigation workbench artifacts (Артефакты рабочего места исследований) | | | | Нет. Вызывает поиск по коллекции investigation\_leads KV Store. | | | | | | | |
| Investigation workbench (Рабочее место расследований) | | Authentication Data (Аутентификационные данные) | | | | [Authentication](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Authentication) | | | Authentication.app, .action, .src, .src\_user, .dest, .user | | | | |
| Certificate Activity (Активность сертификатов) | | | | [Certificates](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Certificates) | | | Certificates.SSL, .src, .src\_port, .dest, .dest\_port, .ssl\_is\_valid, .ssl\_validity\_window, .ssl\_hash, .ssl\_serial, .ssl\_subject, .ssl\_start\_time, .ssl\_end\_time | | | | |
| Computer Inventory ( Компьютерная учетная запись) | | | | [Inventory](http://docs.splunk.com/Documentation/CIM/4.11.0/User/ComputeInventory) | | | Compute\_Inventory.All\_Inventory, .os, .vendor\_product, .user, .dest | | | | |
| DNS Data (Данные DNS) | | | | [Network Resolution DNS](http://docs.splunk.com/Documentation/CIM/4.11.0/User/NetworkResolutionDNS) | | | Network\_Resolution.DNS, DNS.dest, .query, .query\_count, .message\_type, .answer, .reply\_code | | | | |
| Email Data  (Почтовые данные) | | | | [Email](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Email) | | | Email.All\_Email, .src, .dest, .src\_user, .action, .recipient, .recipient\_count, .subject | | | | |
| Filesystem Changes (Изменения системы файлов) | | | | [Change Analysis](http://docs.splunk.com/Documentation/CIM/4.11.0/User/ChangeAnalysis) | | | Change\_Analysis.All\_Changes, .user, .dest, .action, .status, All\_Changes.Endpoint\_Changes.Filesystem\_Changes, .file\_name, .file\_hash, .file\_path, .file\_size, .file\_create\_time, .file\_modify\_time, .file\_access\_time | | | | |
| IDS Alerts (IDS оповещения) | | | | [Intrusion Detection](http://docs.splunk.com/Documentation/CIM/4.11.0/User/IntrusionDetection) | | | Intrusion\_Detection.IDS\_Attacks, .user, .src, .dest, .severity, .category, .signature, .ids\_type, .vendor\_product, .dvc | | | | |
| Latest OS Updates (Последние обновления OS) | | | | [Updates](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Updates) | | | Updates.status, .user, .dest, .signature\_id, .signature, .vendor\_product | | | | |
| Network Session Data (Данные сетевых сеансов) | | | | [Network Sessions](http://docs.splunk.com/Documentation/CIM/4.11.0/User/NetworkSessions) | | | Network\_Sessions.All\_Sessions, .src\_ip, .dest\_ip, .dest\_nt\_host, .tag, .action, .vendor\_product | | | | |
| Network Traffic Data (Данные сетевого трафика) | | | | [Network Traffic](http://docs.splunk.com/Documentation/CIM/4.11.0/User/NetworkTraffic) | | | Network\_Traffic.All\_Traffic, .packets, .src\_ip, .dest\_ip, .user, .transport, .action, .src, .src\_port, .dest, .dest\_port | | | | |
| Notable Events  (Заметные события) | | | | [Incident Management](http://dev.splunk.com/view/enterprise-security/SP-CAAAFBM#incidentmanagement) | | | Incident\_Management.Notable\_Events, .user, .src, .dest, .rule\_name, .severity, .urgency, .security\_domain, .status\_label, .owner, .savedsearch\_description | | | | |
| Port Activity  (Активность порта) | | | | [Application State](http://docs.splunk.com/Documentation/CIM/4.11.0/User/ApplicationState) | | | Application\_State.Ports, .dest, .user, dest\_port, .transport, .process\_name, .process | | | | |
| Process Activity  (Активность процессов) | | | | [Application State](http://docs.splunk.com/Documentation/CIM/4.11.0/User/ApplicationState) | | | Application\_State.All\_Application\_State, .dest, .user, .process\_name, .process | | | | |
| Registry Activity  (Активность регистраций) | | | | [Change Analysis](http://docs.splunk.com/Documentation/CIM/4.11.0/User/ChangeAnalysis) | | | Change\_Analysis\_All\_Changes, .user, .dest, .action, .status, .object, object\_path, .object\_attrs, .object\_id, .Endpoint\_Changes.Registry\_Changes | | | | |
| Risk Scores  (Оценка рисков) | | | | [Risk Analysis](http://dev.splunk.com/view/enterprise-security/SP-CAAAFBM#risk) | | | Risk.All\_Risk, .risk\_score, .risk\_object\_type, .risk\_object | | | |  |
| Service Activity  (Активность сервиса) | | | | [Application State](http://docs.splunk.com/Documentation/CIM/4.11.0/User/ApplicationState) | | | Application\_State.Services, .dest, .user, .service, .service\_id, .status, .start\_mode, .process\_name, .process | | | |  |
| System Vulnerabilities  (Уязвимость системы) | | | | [Vulnerabilities](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Vulnerabilities) | | | Vulnerabilities.Vulnerabilities, .user, .dest, .severity, .signature, .category, .vendor\_product | | | |  |
| User Account Changes (Изменения пользовательского аккаунта) | | | | [Change Analysis](http://docs.splunk.com/Documentation/CIM/4.11.0/User/ChangeAnalysis) | | | Change\_Analysis.All\_Changes, .user, .dest, .action, .status, .object, .object\_path, .object\_attrs, .object\_id, .Account\_Management | | | |  |
| Web Activity (Веб-активность) | | | | [Web](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Web) | | | Web.Web, .src, .dest, .user, .action, .http\_method, .url, .http\_referrer, .http\_user\_agent, .http\_content\_type, .status | | | |  |
| **Название Панели Мониторинга** | | | **Заголовок Панели** | | | **Модель Данных** | | | | **Набор Данных**  **Модели Данных** | | |
| Malware Center (Центр вредоносного ПО) | | | Malware Activity Over Time By Action (Сверхурочная активность вредоносного ПО через действие) | | | [Malware](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Malware) | | | | Malware\_Attacks.action | | |
| Malware Activity Over Time By Signature (Сверхурочная активность вредоносного ПО по подписи) | | | Malware\_Attacks.signature | | |
| Top Infections (Главные заражения) | | | Malware\_Attacks.signature, .dest | | |
| New Malware (Новое вредоносное ПО) - Длительность 30 дней. | | | Отсутствует. Вызывает просмотр malware\_tracker. | | | | | | |
| Malware Operations (Операции вредоносного ПО) | | | Clients By Product Version (Версия клиента по продукту) | | | Отсутствует. Вызывает просмотр malware\_operations\_tracker . | | | | | | |
| Clients By Signature Version (Версия клиента по подписи) | | |
| Oldest Infections (Прежние заражения) | | |
| Repeat Infections (Повторные заражения) | | | [Malware](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Malware) | Malware\_Attacks.action, .signature, .dest | | | | | |
| Malware Search (Поиск вредоносного ПО) | | | | | | Malware\_Attacks.action, .file\_name, .user, .signature, .dest | | | | | |
| Modular Action Center (Центр модульных действий) | Action Invocations Over Time By Name (Сверхурочный вызов действия по имени) | | | | | [Splunk Audit Logs](http://docs.splunk.com/Documentation/CIM/4.11.0/User/SplunkAuditLogs) | Modular\_Actions.Modular\_Action\_Invocations, .action\_name | | | | | |
| Top Actions By Name(Главные действия по имени) | | | | | Modular\_Actions.Modular\_Action\_Invocations, .action\_mode, .user, .duration, .search\_name, .rid, .sid | | | | | |
| Top Actions By Search (Главные действия по поиску) | | | | | Modular\_Actions.Modular\_Action\_Invocations, .action\_name, .action\_mode, .user, .search\_name, .rid, .sid | | | | | |

### *N – S*

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Название Панели Мониторинга** | **Заголовок Панели** | | | | **Модель Данных** | | | | **Набор Данных**  **Модели Данных** | |
| Network Changes (Изменения сети) | Network Changes By Action (Изменения сети по действию) | | | | [Change Analysis](http://docs.splunk.com/Documentation/CIM/4.11.0/User/ChangeAnalysis) | | | | All\_Changes.Network\_Changes, .action | |
| Network Changes By Device (Изменения сети по устройству) | | | | All\_Changes.Network\_Changes, .dvc | |
| New Domain Analysis (Проверка нового домена) | New Domain Activity (Активность нового домена) | | | | [Web](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Web) | | | | Web.dest | |
| New Domain Activity By Age (Активность нового домена по возрасту) | | | |
| New Domain Activity By TLD (Активность нового домена по TLD) | | | |
| Registration Details (Детали регистрации) | | | | Отсутствует. | | | | | |
| **Название Панели Мониторинга** | **Заголовок Панели** | | | | **Модель Данных** | | | | **Набор Данных**  **Модели Данных** | |
| Port & Protocol Tracker (Система слежения «порт и протокол») | Port/Protocol Profiler (Профиль порт/протокол) | | | | [Network Traffic](http://docs.splunk.com/Documentation/CIM/4.11.0/User/NetworkTraffic) | | | | All\_Traffic.transport, .dest\_port | |
| Prohibited Or Insecure Traffic Over Time - Last 24 Hours (Сверхурочный запрещенный или небезопасный трафик) – Длительность 24 часа. | | | | All\_Traffic.src\_category, .dest\_category, .src, .dest, .transport, .dest\_port | |
| Prohibited Traffic Details - Last 24 Hours (Детали запрещенного трафика) – Длительность 24 часа. | | | | All\_Traffic.src\_category, .dest\_category, .src, .dest, .transport, .dest\_port | |
| New Port Activity - Last 7 Days (Активность нового порта) – Длительность 7 дней. | | | | Отсутствует. Вызывает просмотр the application protocols . | | | | | |
| Protocol Center (Центр протоколов) | Connections By Protocol (Соединения по протоколу) | | | | [Network Traffic](http://docs.splunk.com/Documentation/CIM/4.11.0/User/NetworkTraffic) | | | | | All\_Traffic.app |
| Usage By Protocol (Пользование по протоколу) | | | | All\_Traffic.app, .bytes |
| Top Connection Sources (Источники главных соединений) | | | | All\_Traffic.src |
| Usage For Well Known Ports (Пользование известными портами) | | | | All\_Traffic.bytes, .dest\_port |
| Long Lived Connections (Длительные соединения) | | | | All\_Traffic.src, .src\_port, .duration, .dest, .dest\_port, .transport |
| Risk Analysis (Анализ рисков) | Risk Modifiers Over Time (Сверхурочные модификаторы рисков) | | | | [Risk Analysis](http://dev.splunk.com/view/enterprise-security/SP-CAAAFBM#risk) | | | | | All\_Risk.risk\_score |
| Risk Score By Object (Оценка рисков по объекту) | | | | All\_Risk.risk\_score |
| Most Active Sources (Наиболее активные источники) | | | | All\_Risk.risk\_score, .risk\_object |
| Recent Risk Modifiers (Недавние модификаторы рисков) | | | | All\_Risk.\* |
| **Название Панели Мониторинга** | **Заголовок Панели** | | **Модель Данных** | | | **Набор Данных**  **Модели Данных** | | | | |
| Security Posture (Состояние безопасности) | Notable Events By Urgency (Заметные события по срочности) | | | | | | Отсутствуют. Вызывает поиск по коллекции es\_notable\_events KVStore. | | | |
| Notable Events Over Time (Сверхурочные заметные события) | | | | | |
| Top Notable Events (Главные заметные события) | | | | | |
| Top Notable Event Sources (Источники главных заметных событий) | | | | | |
| Session Center (Центр сеансов) | Sessions Over Time (Сверхурочные сеансы) | | | [Network Sessions](http://docs.splunk.com/Documentation/CIM/4.11.0/User/NetworkSessions) | | | | All\_Sessions.Session\_\* | | |
| Session Details (Детали сеансов) | | | All\_Sessions.\* | | |
| SSL Activity (SSL активность) | SSL Activity By Common Name (SSL активность по имени) | | | [Certificates](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Certificates) | | | | All\_Certificates.SSL.ssl\_subject\_common\_name | | |
| SSL Cloud Sessions (SSL Cloud сеансы) | | | All\_Certificates.SSL.ssl\_subject\_common\_name, .src, | | |
| Recent SSL Sessions (Недавние SSL сеансы) | | |  | | |
| SSL Search (поиск SSL) | | | | All\_Certificates.src, .dest, .ssl\_subject\_common\_name, .ssl\_subject\_email, .ssl\_issuer\_common\_name, .ssl\_issuer\_organization, .ssl\_start\_time, .ssl\_end\_time, .ssl\_validity\_window, .ssl\_is\_valid | | |
| Suppression Audit (Проверка замедлений) | | Suppressed Events Over Time (Сверхурочные замедленные события) - Длительность 24 часа. | | Отсутствуют | | | | Вызывает макрос для поиска заметных событий. | | |
| Suppression History Over Time (Сверхурочная история замедлений) – Длительность 30 дней. | | Вызывает макрос и поиск по Summary Gen information. | | |
| Suppression Management Activity (Активность управления замедлениями) | | Вызывает поиск по типу события. | | |
| Expired Suppressions (Истекшие замедления) | | Вызывает поиск по типу события. | | |
| System Center (Системный центр) | | Operating Systems (Операционные системы) | | Отсутствует. Вызывает просмотр system\_version\_tracker . | | | | | | |
| Top-Average CPU Load By System (Загрузка CPU выше среднего по системе) | | [Performance](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Performance) | | All\_Performance.CPU.cpu\_load\_percent, All\_Performance.dest | | | | |
| Services By System Count (Сервисы по счету системы) | | [Application State](http://docs.splunk.com/Documentation/CIM/4.11.0/User/ApplicationState) | | All\_Application\_State.Services | | | | |
| Ports By System Count (Порты по счету системы) | | All\_Application\_State.Ports | | | | |

### *T - Z*

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Название Панели Мониторинга** | **Заголовок Панели** | | | | | **Модель Данных** | | **Набор Данных**  **Модели Данных** | | | |
| Threat Activity (Активность угроз) | Threat Activity Over Time (Сверхурочная активность угроз) | | | | | [Intrusion Detection](http://docs.splunk.com/Documentation/CIM/4.11.0/User/IntrusionDetection), [Network Traffic](http://docs.splunk.com/Documentation/CIM/4.11.0/User/NetworkTraffic), and [Web](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Web). Для дополнительной информации см. раздел «Источники данных активности угроз». | | | | | |
| Most Active Threat Collections (Наиболее активные группы угроз) | | | | |
| Most Active Threat Sources (Наиболее активные источники угроз) | | | | |
| Threat Activity Details (Детали активности угроз) | | | | |
| Threat Artifacts (Артефакты угроз) | Threat Overview (Обзор угроз) | | | | | Отсутствует. Вызывает коллекции поиска информации об угрозах KV Store. Для просмотра списка коллекций поиска информации об угрозах, см. «Поддерживаемые типы [распознавания угроз в Splunk Enterprise Security](http://docs.splunk.com/Documentation/ES/5.1.0/Admin/Supportedthreatinteltypes)» | | | | | |
| Endpoint Artifacts (Артефакты конечной точки) | | | | |
| Network Artifacts (Артефакты сети) | | | | |
| Email Artifacts (Почтовые артефакты) | | | | |
| Certificate Artifacts (Артефакты сертификатов) | | | | |
| Threat Intelligence Audit (Проверка распознавания угроз) | Threat Intelligence Downloads (Загрузки распознавания угроз) | | | | | Отсутствует. Вызывает поиск конечной точки REST. | | | | | |
| Threat Intelligence Audit Events (События проверки распознавания угроз) | | | | | Отсутствует. Вызывает поиск по типу событий. | | | | | |
| Time Center (Центр управления временем) | Time Synchronization Failures (Ошибки синхронизации времени) | | | | | [Performance](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Performance) | | | All\_Performance.OS.Timesync, All\_Performance.dest, .dest\_should\_timesync, OS.Timesync.action | | |
| Systems Not Time Synching (Системы, не синхронизированные по времени) | | | | |
| Indexing Time Delay (Задержка индексации времени) | | | | | Отсутствует. Вызывает результаты поиска Summary Gen. | | | | | |
| Time Service Start Mode Anomalies (Дефекты запуска сервиса времени) | | | | | [Application State](http://docs.splunk.com/Documentation/CIM/4.11.0/User/ApplicationState) | | | All\_Application\_State.Services.start\_mode, .Services.status, .dest\_should\_timesync, .tag, .dest | | |
| Traffic Center (Центр управления трафиком) | Traffic Over Time By Action (Сверхурочный трафик по действию) | | | | | [Network Traffic](http://docs.splunk.com/Documentation/CIM/4.11.0/User/NetworkTraffic) | | | All\_Traffic.action | | |
| Traffic Over Time By Protocol (Сверхурочный трафик по протоколу) | | | | | All\_Traffic.transport | | |
| Scanning Activity (Активность сканирования) (Много систем) | | | | | All\_Traffic.dest, .src | | |
| Top Sources (Главные источники) | | | | | All\_Traffic.src | | |
| Traffic Search (Поиск трафика) | | | | | | All\_Traffic.action, .src\_port, .src, .dest, .transport, .dest\_port | | |
| Traffic Size Analysis (Анализ объема трафика) | | | | Traffic Size Anomalies Over Time (Сверхурочные аномалии объема трафика) | | [Network Traffic](http://docs.splunk.com/Documentation/CIM/4.11.0/User/NetworkTraffic) | | | All\_Traffic.transport, .src | | |
| Traffic Size Details (Детали объема трафика) | | All\_Traffic.bytes, .dest, .src | | |
| **Название Панели Мониторинга** | | **Заголовок Панели** | | | | **Модель Данных** | | | | **Набор Данных**  **Модели Данных** | |
| Update Center (Центр обновлений) | | Top Systems Needing Updates (Необходимые обновления главных систем) | | | | [Updates](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Updates) | | | | Updates.status, .dest, .signature\_id, .vendor\_product | |
| Top Updates Needed (Необходимые главные обновления) | | | | Updates.status, .dest, .signature\_id, .vendor\_product | |
| Systems Not Updating (Необновляемые системы) – Более чем 30 дней. | | | | Updates.dest\_should\_update, .dest, .signature\_id, .vendor\_product, .status | |
| Update Service Start Mode Anomalies (Аномалии запуска сервиса обновлений) | | | | [Application State](http://docs.splunk.com/Documentation/CIM/4.11.0/User/ApplicationState) | | | | All\_Application\_State.Services.start\_mode, .Services.status, .Services.service, .tag | |
| Update Search (Поиск обновлений) | | | | | | [Updates](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Updates) | | | | Updates.dest\_should\_update, .status, .dest, .signature\_id, .vendor\_product | |
| URL Length Analysis (Анализ длины URL) | | | URL Length Anomalies Over Time (Сверхурочные аномалии длины URL) | | | [Web](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Web) | | | | Web.http\_method, .url | |
| URL Length Details (Детали длины URL) | | | Web.url\_length, .src, .dest, .url | |
| User Activity (Активность пользователя) | | | Users By Risk Scores (Пользователи по оценке рисков) | | | [Risk Analysis](http://docs.splunk.com/Documentation/ES/5.1.0/Install/Datamodels#Risk_Analysis) | | | | All\_Risk.risk\_object | |
| Non-corporate Web Uploads (Некорпоративные Веб-загрузки) | | | [Web](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Web) | | | | Web.bytes, .user, .http\_method, .url | |
| Non-corporate Email Activity (Некорпоративная почтовая активность) | | | [Email](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Email) | | | | All\_Email.size, .recipient, .src\_user, | |
| Watchlisted Site Activity (Активность сайта списков просмотра) | | | [Web](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Web) | | | | Web.src, .url | |
| Remote Access (Удаленный доступ) | | | [Authentication](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Authentication) | | | | Authentication.src, .user | |
| Ticket Activity (Активность тикетов) | | | [Ticket Management](http://docs.splunk.com/Documentation/CIM/4.11.0/User/TicketManagement) | | | | All\_Ticket\_Management.description, .priority, . severity, .src\_user | |
| **Название Панели Мониторинга** | | | | | **Заголовок Панели** | | **Модель Данных** | | | | **Набор Данных**  **Модели Данных** |
| View Audit  (Проверка представлений) | | | | | View Activity Over Time (Сверхурочная активность представлений) | | [Splunk Audit Logs](http://docs.splunk.com/Documentation/CIM/4.11.0/User/SplunkAuditLogs) | | | | View\_Activity.app, .view |
| Expected View Activity (Ожидаемая активность представлений) | | View\_Activity.app, .view, .user |
| Vulnerability Center (Центр уязвимости) | | | | | Top Vulnerabilities (Главные уязвимости) | | [Vulnerabilities](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Vulnerabilities) | | | | Vulnerabilities.signature, .dest |
| Most Vulnerable Hosts (Наиболее уязвимые хосты) | | Vulnerabilities.signature, .severity, .dest |
| Vulnerabilities By Severity (Уязвимость по степени тяжести) | | Vulnerabilities.signature, .severity, .dest |
| New Vulnerabilities (Новая уязвимость) | | Вызывает просмотр vuln\_signature\_reference. | | | | |
| Vulnerability Operations  (Операции уязвимости) | | | | | Scan Activity Over Time (Сверхурочная активность сканирования) | | [Vulnerabilities](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Vulnerabilities) | | | | Vulnerabilities.dest |
| Vulnerabilities By Age (Уязвимость по возрасту) | | vulnerability\_tracker lookup. | | | | |
| Delinquent Scanning (Сканирование нарушителей) | | [Vulnerabilities](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Vulnerabilities) | | | | Vulnerabilities.dest |
| Vulnerability Search (Поиск уязвимости) | | | | | | | Vulnerabilities.category, .signature, .dest, .severity, .cve, |
| Web Center (Веб-центр) | | | | | Events Over Time By Method (Сверхурочные события по методу) | | [Web](http://docs.splunk.com/Documentation/CIM/4.11.0/User/Web) | | | | Web.http\_method |
| Events Over Time By Status (Сверхурочные события по статусу) | | Web.status |
| Top Sources (Главные источники) | | Web.dest, .src |
| Top Destinations (Главные адреса назначения) | | Web.dest, .src |
| Web Search (Веб-поиск) | | | | | | | Web.http\_method, .status, .src, .dest, .url |

**Панели мониторинга для дополнений**

Данные панели мониторинга включены в Splunk Enterprise Security. Используйте навигационный редактор, чтобы добавить или реорганизовать панели мониторинга на панели меню. Для получения дополнительной информации об использовании навигационного редактора, смотрите раздел «Персональная настройка панели меню в Splunk Enterprise Security».

Для просмотра целого списка панелей мониторинга в Enterprise Security, выберите **Search > Dashboards**. Для просмотра списка панелей мониторинга в Enterprise Security на предмет наличия добавлений, используйте панель мониторинга Content Profile (Профиль Контента). См. раздел «Профиль Контента».

|  |  |  |
| --- | --- | --- |
| **Название Панели Мониторинга** | **Домен Безопасности** | **Часть Дополнения** |
| Access Anomalies  (Дефекты Доступа) | Access | DA-ESS-AccessProtection |
| Access Center (Центр Доступа) | Access | DA-ESS-AccessProtection |
| Access Search (Поиск Доступа) | Access | DA-ESS-AccessProtection |
| Access Tracker  (Система отслеживания доступа) | Access | DA-ESS-AccessProtection |
| Account Management  (Управление аккаунтом) | Access | DA-ESS-AccessProtection |
| Asset Center (Центр ресурсов) | Asset | SA-IdentityManagement |
| Asset Investigator  (Исследователь Ресурсов) | Asset | SA-IdentityManagement |
| Content Profile (Профиль Контента) | Audit | SplunkEnterpriseSecuritySuite |
| Data Model Audit  (Проверка модели Данных) | Audit | Splunk\_SA\_CIM |
| Default Account Activity  (Активность аккаунта по умолчанию) | Access | DA-ESS-AccessProtection |
| DNS Activity (Активность DNS) | Network | DA-ESS-NetworkProtection |
| DNS Search (Поиск DNS) | Access | DA-ESS-NetworkProtection |
| Email Activity (Почтовая активность) | Access | DA-ESS-NetworkProtection |
| Email Search (Почтовый поиск) | Access | DA-ESS-NetworkProtection |
| Endpoint Changes  (Изменения конечной точки) | Endpoint | DA-ESS-EndpointProtection |
| Forwarder Audit  (Проверка экспедитора) | Audit | SA-AuditAndDataProtection |
| HTTP Category Analysis  (Анализ категории HTTP) | Network | DA-ESS-NetworkProtection |
| HTTP User Agent Analysis  (Анализ агента пользователя HTTP) | Network | DA-ESS-NetworkProtection |
| Identity Center  (Центр идентификации) | Identity | SA-IdentityManagement |
| Identity\_investigator  (Исследователь идентификации) | Identity | SA-IdentityManagement |
| Incident Review (Оценка инцидентов) | Threat | SA-ThreatIntelligence |
| Incident Review Audit  (Проверка оценки инцидентов) | Threat | SA-ThreatIntelligence |
| Indexing Audit  (Проверка индексирования) | Audit | SA-AuditAndDataProtection |
| Intrusion Center (Центр атак) | Network | DA-ESS-NetworkProtection |
| Intrusion Search  (Поиск атак) | Network | DA-ESS-NetworkProtection |
| Malware Center  (Центр вредоносного ПО) | Endpoint | DA-ESS-EndpointProtection |
| Malware Operations  (Операции вредоносного ПО) | Endpoint | DA-ESS-EndpointProtection |
| Malware Search  (Поиск вредоносного ПО) | Endpoint | DA-ESS-EndpointProtection |
| Network Changes (Изменения сети) | Network | DA-ESS-NetworkProtection |
| New Domain Analysis  (Анализ новых доменов) | Network | DA-ESS-NetworkProtection |
| Per-Panel Filter Audit  (Проверка расширенного фильтра) | Audit | SA-Utils |
| Port & Protocol Tracker  (Система отслеживания «Порт и Протокол») | Network | DA-ESS-NetworkProtection |
| Predictive Analytics  (Аналитика прогнозов) |  | Splunk\_SA\_CIM |
| Protocol Center (Центр протоколов) | Network | DA-ESS-NetworkProtection |
| REST Audit  (Проверка REST) | Audit | SA-Utils |
| Risk Analysis (Анализ рисков) | Threat | SA-ThreatIntelligence |
| Search Audit  (Контроль поиска) | Audit | SA-AuditAndDataProtection |
| Security Posture  (Состояние безопасности) |  | SplunkEnterpriseSecuritySuite |
| Session Center (Центр сеансов) | Identity | SA-IdentityManagement |
| SSL Activity (Активность SSL) | Network | DA-ESS-NetworkProtection |
| SSL Search (Поиск SSL) | Network | DA-ESS-NetworkProtection |
| Suppression Audit  (Проверка замедлений) | Threat | SA-ThreatIntelligence |
| System Center (Системный центр) | Endpoint | DA-ESS-EndpointProtection |
| Threat Activity (Активность угроз) | Threat | DA-ESS-ThreatIntelligence |
| Threat Artifacts (Артефакты угроз) | Threat | DA-ESS-ThreatIntelligence |
| Threat Intelligence Audit  (Проверка распознавания угроз) | Audit | DA-ESS-ThreatIntelligence |
| Time Center  (Центр управления временем) | Endpoint | DA-ESS-EndpointProtection |
| Traffic Center  (Центр управления трафиком) | Network | DA-ESS-NetworkProtection |
| Traffic Search (Поиск трафика) | Network | DA-ESS-NetworkProtection |
| Traffic Size Analysis (Анализ объема трафика) | Network | DA-ESS-NetworkProtection |
| Update Center (Центр обновлений) | Endpoint | DA-ESS-EndpointProtection |
| Update Search (Поиск обновлений) | Endpoint | DA-ESS-EndpointProtection |
| URL Length Analysis  (Анализ длины URL) | Network | DA-ESS-NetworkProtection |
| User Activity  (Активность пользователя) | Identity | DA-ESS-IdentityManagement |
| View Audit  (Проверка представления) | Audit | SplunkEnterpriseSecuritySuite |
| Vulnerability Center  (Центр уязвимости) | Network | DA-ESS-NetworkProtection |
| Vulnerability Operations  (Операции уязвимости) | Network | DA-ESS-NetworkProtection |
| Vulnerability Search  (Поиск уязвимости) | Network | DA-ESS-NetworkProtection |
| Web Center  (Веб-центр) | Network | DA-ESS-NetworkProtection |
| Web Search (Веб-поиск) | Network | DA-ESS-NetworkProtection |

**Экстремальный поиск**

**Как Splunk Enterprise Security использует экстремальный поиск**

Экстремальный поиск расширяет язык поиска платформы Splunk с помощью набора команд. Список команд экстремального поиска см. в разделе «Экстремальные команды поиска».

В Splunk Enterprise Security реализована данная функция, и вы можете использовать команды экстремального поиска:

* Создание динамических пороговых значений на основе данных о событиях.
* Обеспечение понимания контекста путем замены счетчиков событий естественным языком.

Например, на информационной панели Security Security Malware Center в окне «Key Security Indicator» отображается общее количество систем с вредоносными заражениями за последние 48 часов.



Splunk ES определяет отображаемую скорость изменения путем сравнения текущего количества заражений с количеством зараженных систем за день до этого. Автоматическое определение нормального дневного диапазона для зараженных систем в вашей среде отсутствует. Порог полностью настраивается для пользователя. Вредоносные заражения увеличились на три, но значение не имеет никакого контекста, чтобы указать, является ли этот параметр заметным увеличением.

Тот же самый индикатор, использующий экстремальный поиск, отображает соответствующую информацию, но включает в себя расширенную информацию, недоступную для системы при отключении функции «Total Infections».



Используя экстремальный поиск, Splunk ES вычисляет количество заражений и уровень нового заражения с использованием динамически обновляемой модели. В ключевом индикаторе безопасности используется контекстный и понятный язык. В этом случае вы знаете, что общий показатель заражения вредоносными программами не выше, чем в любой другой день, и скорость изменения данного показателя не вызывает состояние обеспокоенности.

**Использование контекста и концепции в экстремальном поиске**

Основные идеи **контекста** и **концепта** являются решающими для понимания экстремального поиска. Эти понятия составляют основу модели данных, используемой для динамических пороговых значений, с помощью команды экстремального поиска.

1. **Контекст**: контекст определяет связь с полем или данными в числовых выражениях. Данные, подлежащие моделированию, должны быть представлены численными значениями в результате поиска. Примеры контекстов включают общую пропускную способность сети за последние 24 часа или латентность сети за последние 24 часа.

2. **Концепт**: термин, который применяется к данным, представляющий их качественное, а не количественное описание. Примеры включают термины «экстремальный», «высокий», «средний», «низкий» и «минимальный».

Объединив контекст и концепт, экстремальный поиск добавляет данным значение и оценку.

• Общая пропускная способность сети за последние 24 часа может быть экстремальной, высокой, средней, низкой или минимальной.

• Латентность сети за последние 24 часа может быть экстремальной, высокой, средней, низкой или минимальной.

Термины концепта описывают сетевую активность в обоих примерах, но имеют разные значения, основанные на контексте, к которому они применяются. Если ваша среда сообщает, что общая пропускная способность сети минимальна, это предупреждение. Если среда сообщает, что время ожидания сети минимальное, сеть работает нормально.

***Модели данных и экстремальный поиск***

После выбора контекста и концепта для представления ваших данных Splunk ES создает модель данных. Используя команды экстремального поиска, модель данных отображает контекст и статистику событий в разрезе концепта. Команды экстремального поиска обращаются к этой комбинированной модели как к контексту.

Сохраненные поисковые запросы обновляют контексты, такие как контекст динамического порога. Сохраненный поиск ищет данные о событиях для составления статистики обновления контекста.

Список сохраненных запросов поиска, которые обновляют контексты, см. в разделе «Контейнеры, контексты и ​​сохраненные результаты поиска» в данном документе.

**Конфигурация экстремального поиска для Enterprise Security**

Использование команд экстремального поиска в Enterprise Security не требует дополнительной настройки. Стандартная установка ES обеспечивает все контексты, используемые экстремальными командами поиска, и позволяет сохранять поисковые запросы, которые их поддерживают.

• Список контекстов и сохраненных результатов поисков, реализованных в Enterprise Security, см. в разделе «Контейнеры, контексты и ​​сохраненные результаты поиска» в данном документе.

• Список ключевых индикаторов безопасности, использующих экстремальный поиск, см. в разделе «Экстремальный поиск ключевых индикаторов безопасности» в данном документе.

• Список корреляционных поисковых запросов, использующих экстремальный поиск, см. в разделе «Корреляционные поисковые запросы, которые используют экстремальный поиск» в данном документе. По умолчанию все корреляционные поисковые запросы отключены.

***Корреляционные поисковые запросы, использующие экстремальный поиск***

Все корреляционные поисковые запросы в Enterprise Security по умолчанию отключены. См. «Включить корреляционные поисковые запросы» в данном руководстве.

Функция «Guided Search Creation» недоступна для корреляционных поисковых запросов, в которых используются команды экстремального поиска. Следующие корреляционные поисковые запросы используют экстремальный поиск.

|  |  |
| --- | --- |
| **Наименование поиска** | **Контекст** |
| Brute Force Access Behavior Detected | failures\_by\_src\_count\_1 h |
| Brute Force Access Behavior Detected Over One Day | failures\_by\_src\_count\_1 d |
| Abnormally High Number of Endpoint Changes By User | change\_count\_by\_user\_by\_change\_type\_1d |
| Host Sending Excessive Email | recipients\_by\_src\_1 h |
| Substantial Increase in Events | count\_by\_signature\_1 h |
| Substantial Increase in Port Activity | count\_by\_dest\_port\_1 d |
| Unusual Volume of Network Activity | count\_30m |

|  |  |
| --- | --- |
| Abnormally High Number of HTTP Method Events By Src | count\_by\_http\_method\_by\_src\_1d |

***Экстремальные ключевые индикаторы безопасности поиска***

Вы можете легко определить ключевые индикаторы, которые используют экстремальный поиск, поскольку они используют семантический язык вместо численных значений. По умолчанию ключевые индикаторы безопасности на каждой панели включены.

|  |  |
| --- | --- |
| **Наименование поиска** | **Контекст** |
| Access - Total Access Attempts | authentication: count\_1d, percentile |
| Malware - Total Infection Count | malware: count\_1d, percentile |
| Risk - Median Risk Score | median\_object\_risk\_by\_object\_type\_1d,  percentile |
| Risk - Median Risk Score By System | median\_object\_risk\_by\_object\_type\_1d,  percentile |
| Risk - Median Risk Score By User | median\_object\_risk\_by\_object\_type\_1d,  percentile |
| Risk - Median Risk Score By Other | median\_object\_risk\_by\_object\_type\_1d,  percentile |
| Risk - Aggregated Risk | total\_risk\_by\_object\_type\_1 d, percentile |
| Risk - Aggregated System Risk | total\_risk\_by\_object\_type\_1 d, percentile |
| Risk - Aggregated User Risk | total\_risk\_by\_object\_type\_1 d, percentile |
| Risk - Aggregated Other Risk | total\_risk\_by\_object\_type\_1 d, percentile |

***Контейнеры, контексты и сохраненные поисковые запросы***

Enterprise Security хранит контексты в объектах, называемых контейнерами. Контейнер является одновременно объектом в файловой системе и логической конфигурацией, используемой для классификации контекстов. В Enterprise Security контейнеры представляют собой файлы с расширением .context. Контейнер может содержать несколько контекстов. Вы можете просмотреть сохраненные поисковые запросы, которые генерируют контексты в витрине «Content Management» в Enterprise Security. Дополнительные сведения см. в разделе «Создание и управление сохраненными поисковыми запросами в Splunk Enterprise Security».

**Примечание**. Enterprise Security позволяет по умолчанию сохранять динамические контексты.

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование контейнера** | **Наименование контекста** | **Расположение приложения** | **Наименование динамического поиска контекста** |
| authentication | failures\_by\_src\_count\_1h | SA-AccessProtection | Access - Authentication Failures By Source - Context Gen |
| failures\_by\_src\_count\_1d | Access - Authentication Failures By Source Per Day - Context Gen |
| count\_1d | Access - Authentication Volume Per Day - Context Gen |
| change\_analysis | change\_count\_by\_user\_by\_change\_type\_1d | SA-EndpointProtection | Change - Total Change Count By User By Change Type Per Day - Context Gen |
| email | destinations\_by\_src\_1h | SA-EndpointProtection | Endpoint - Emails By Destination Count - Context Gen |
| recipients\_by\_src\_1h | Endpoint - Emails By Source - Context Gen |
| malware | count\_1d | SA-NetworkProtection | Endpoint - Malware Daily Count - Context Gen |
| ids\_attacks | count\_by\_signature\_1h | SA-NetworkProtection | Network - Event Count By Signature Per Hour - Context Gen |
| network\_traffic | count\_by\_dest\_port\_1d | SA-NetworkProtection | Network - Port Activity By Destination Port - Context Gen |
| src\_count\_30m | Network - Traffic Source Count Per 30m - Context Gen |
| count\_30m | Network - Traffic Volume Per 30m - Context Gen |
| web | count\_by\_http\_method\_by\_src\_1d | SA-NetworkProtection | Web - Web Event Count By Src By HTTP Method Per 1d - Context Gen |
| risk | median\_object\_risk\_by\_object\_type\_1d | SA-ThreatIntelligence | Risk - Median Object Risk Per Day - Context Gen |
| total\_risk\_by\_object\_type\_1d | Risk - Total Risk By Risk Object Type Per Day - Context Gen |
| default | percentile | SA-Utils | ESS - Percentile - Context Gen |
| default | height | Splunk\_SA\_ExtremeSearch | None. |
| trendchange | None. |
| compatibility | None. |

**Пример экстремального поиска в Splunk Enterprise Security**

Вы можете преобразовать существующие корреляционные поисковые запросы, чтобы использовать команды экстремального поиска. Вам не нужно вносить какие-либо изменения в конфигурацию или изменения в использование запросов, преобразованных для использования команд экстремального поиска. Список команд экстремального поиска см. в разделе «Команды экстремального поиска».

В этом примере показано, как преобразовать существующий корреляционный поисковый запрос «Brute Force Access Behavior Detected», используя команды экстремального поиска.

Этот пример предназначен только для иллюстрации. Корреляционный поисковый запрос «Brute Force Access Behavior», включенный в Splunk Enterprise Security, уже был преобразован для использования команд экстремального поиска.

**Поиск «Brute Force Access Behavior»**

Корреляционный поисковый запрос «Brute Force Access Behavior» проверяет чрезмерное количество неудачных попыток входа в систему, за которыми следует успешный вход в систему. Базовый поиск находит соответствующие события, подсчитывает события по типу «сбой» и отслеживает завершающее «успешное» событие для каждой проверки подлинности хоста за последний час. Если идентифицированные события соответствуют порогу, поиск посылает уведомление (предупреждение) для создания существенного события или другие типы предупреждений.

«Brute Force Access Behavior» - корреляционный поиск без экстремальных команд поиска:

| ‘datamodel (“Authentication”, “Authentication”) | stats

Values (Authentication.tag) as

tag, count (eval (‘Authentication.action’==”fallure”)) as

failure, count (eval (‘Authentication.action’==”success”)) as success by

Authentication.src | ‘drop\_dm\_object\_name (“Authentication”)’ | search

failure>6 success>0 | ‘settags”("access”) ‘

Без экстремальных команд поиска поиск определяет статический порог для событий «успех» с захватом | search failure>6. Администратор Enterprise Security должен выбрать пороговое значение или принять значение по умолчанию. Если администратор устанавливает слишком низкий порог, поиск создает множество существенных событий. Если администратор устанавливает слишком высокий порог, поиск может пропустить существенные события, создавая потенциально слепую зону для угрозы безопасности.

Поиск, который реализует экстремальный поиск, удаляет статическое значение и использует в этом примере данные аутентификации, полученные от Splunk Enterprise, чтобы определить существенный уровень сбоев аутентификации в вашей среде.

**1. Изучить данные**

Чтобы использовать экстремальный поиск, вы должны создать надежную модель данных для команд. Чтобы создать модель данных, вы должны понять, что представляют собой данные и на какой вопрос вы пытаетесь ответить.

Для приведенного выше примера (корреляционный поиск «Brute Force Access Behavior») вы знаете, что количество ошибок аутентификации не будет ниже нуля и может значительно превышать данный уровень. Шкала значений представляет собой проверенные значения аутентификации.

**2. Выбрать контекст**

Вы можете выбрать один из трех типов контекстов, каждый из которых требует трех точек данных.

• Среднее значение: требуется среднее значение, стандартное отклонение и счетчик событий.

• Медианное значение: требуется медианное значение, стандартное отклонение и счетчик событий.

• Домен: требуется минимум, максимум и счетчик событий.

В этом примере счетчик событий аутентификации не включает отрицательное значение и является прогрессивным, поэтому домен лучше всего подходит для данных аутентификации.

**3. Выбрать концепт**

Концепт представляет собой качественное описание данных. Splunk Enterprise Security включает в себя заранее определенные концепты интерпретации изменений, направления и амплитуды в качестве качественных показателей. Используемые концепты дифференцируются при помощи терминов.

• Изменение использует термины: «минимально, слегка, умеренно, сильно, экстремально».

• Направление использует термины: «уменьшение, неизменно, увеличение»

• Амплитуда использует термины: «минимальный, низкий, средний, высокий, экстремальный»

В этом случае концепт амплитуды наилучшим образом отражает поведение ошибок аутентификации.

**4. Создать контекст**

Как описано в разделе «Как Splunk Enterprise Security использует экстремальный поиск» в данном руководстве, контекст имеет как имя, так и контейнер, находящийся в приложении. Поиск «Brute Force Access Behavior» выполняется по отношению к событиям аутентификации, поэтому контейнер контекста называется «аутентификация». Контейнер «аутентификация» находится в приложении «SA-AccessProtection» вместе с поисковыми запросами аутентификации и другими объектами.

ES включает в себя предварительно инициализированный контекст аутентификации. Этот контекст не будет представлять вашу среду, если только сохраненный поиск не обновит ее с помощью событий. Splunk Enterprise Security содержит этот контекст, поэтому обновления будут иметь больший вес, чем значения, используемые при создании контекста. Домен для этого контекста аутентификации определяется с помощью min = 0, max = 10 и count = 0.

Для поиска «Brute Force Access Behavior» название контекста выбрано таким образом, чтобы облегчить быструю идентификацию: failures\_by\_src\_count\_1h.

Создайте исходный контекст с использованием данных примера.

| xsCreateDDContext. app=”SA-AccessProtection”

name=fallures\_by\_src\_count\_1h container=authentication scope=app terms=’xs\_default\_magnitude\_concepts’ min=0 max=10 count=0 type=domain

Данный контекст является определяемым пользователем контекстом, потому что вы указываете данные в поиске, чтобы убедиться, что контекст работает. В конечном поиске контекст определяется данными, поскольку он зависит от данных из результатов поиска более раннего поиска.

Отобразите контекст, после создания:

| xsdisplaycontext failures\_by\_src\_count\_1h in authentication



Перед реализацией экстремального поиска статический порог для сбоев аутентификации составлял шесть. На основе контекста failures\_by\_src\_count\_1h число шесть будет смоделировано в конце термина «среда». Модель будет изменяться после того, как обновленный поиск «Brute Force Access Behavior» проверит

данные аутентификации и сохраненный поиск, который обновляется через

failures\_by\_src\_count\_1h runs.

Перечислите термины, используемые в контексте:

I xslistconcepts failures\_by\_src\_count\_1h in authentication

**5. Применить контекст в поиске**

Вы можете использовать команду поиска xsWhere для оценки значения данных в контексте. Этот корреляционный поиск использует xsWhere, чтобы сравнить количество ошибок аутентификации с контекстом failures\_by\_src\_count\_1h, чтобы определить, имеет ли счетчик значение выше «medium».

В этом примере понятие среды представляет собой диапазон значений, которые изменяются после того, как контекст обновляется данными. Сохраненный поиск обновляет контекст. Если количество событий, идентифицированных сохраненными результатами поиска, больше, чем среднее (medium), корреляционный поиск с использованием экстремального поиска вышлет уведомление (предупреждение) и создаст существенное событие.

«Brute Force Access Behavior Detected» с возможностями экстремального поиска

| ‘datamodel (“Authentication”, “Authentication”) | stats

values (Authentication.tag) as

tag, count (eval (‘Authentication.action’==”failure”)) as

failure, count (eval (‘Authentication.action’==”success”)) as success by

Authentication.src | ’drop\_dm\_object\_name (“Authentication”) | search

success>0 | xswhere failure from failures\_by\_src\_count\_1h in

authentication is above medium | ‘settags (“access”)’

**6. Обновить контекст**

Порог поиска может быть динамическим, поскольку он использует сохраненный поиск для обновления контекста. Сохраненные поисковые запросы включаются в ES, они генерируют контекстную информацию для экстремального поиска с помощью «Context Gen», чтобы обеспечить легкую идентификацию.

Контекст домена, используемый корреляционным поиском по принципу «Brute Force Access Behavior», требует значений для минимума, максимума и счетчика. Эти значения взяты из модели данных аутентификации. Функция «Access - Authentication Failures By Source - Context Gen» сохранила поиск, который генерирует контекст failures\_by\_src\_count\_1h для корреляционного поиска запросов «Brute Force Access Behavior».

Для контекста failures\_by\_src\_count\_1h: результаты поиска контекста, генерирующего изменение максимального значения на кратное медиане, предотвращают выбросы от искажения основного контекста и потенциального введения оплошностей.

Функция сохраненного поиска «Access - Authentication Failures By Source - Context Gen»

| tstats ‘summariesonly’ count as failures from

datamodel=Authentication where Authentication.action=”failure” by

Authentication.src,\_time span=1h | stats median (failures) as median,

min (failures) as min, count as count | eval max = median\*2 |

xsUpdateDDContext app=”SA-AccessProtection”

name=failures\_by\_src\_count\_1h container=authentication scope=app

Этот поиск обновляет контекст failures\_by\_src\_count\_1h с помощью xsUpdateDDContext. В этом случае данные из поиска добавляются в контекст, создавая исторический тренд, который информирует контекст. Это отличается от контекстного поиска на шаге 4, который использовал xsupdateUDContext, поскольку первая часть поиска предоставляет данные, используемые контекстом, а не предоставляемые пользователем.

Как корреляционный поиск, так и сохраненный поиск «Access - Authentication Failures By Source - Context Gen» планируется запустить по умолчанию.

**7. Используйте хеджи для изменения результатов**

Хеджи – это семантические термины, которые изменяют диапазон, представленный концептом. Используйте хедж, чтобы ограничить, сжать или изменить форму кривой, которую использует термин концепта для моделирования данных. Хеджи «above» и «below» полезны для предупреждения о поиске, поскольку они переопределяют диапазон значений, которые будут соответствовать критериям поиска.

Корреляционный поиск «Brute Force Access Behavior Detected» применяет хедж, поэтому уведомление (предупреждение) появляется только тогда, когда количество отказов «выше среднего» (above medium).

Примеры концепции с различными типами хеджей:

|  |  |
| --- | --- |
| **Пример хеджирования** | **Изображение** |
| | xsDisplayConcept medium from failures\_by\_src\_count\_1h in authentication |  |
| | xsDisplayConcept very medium from failures\_by\_src\_count\_1h in authentication |  |

|  |  |
| --- | --- |
| I xsDisplayConcept above medium from failures\_by\_src\_count\_1h in authentication |  |
| | xsDisplayConcept below medium from failures\_by\_src\_count\_1h in authentication |  |
| | xsDisplayConcept around medium from failures\_by\_src\_count\_1h in authentication |  |

Файл справочника synonyms.csv в приложении Splunk\_SA\_ExtremeSearch содержит хеджи экстремального поиска.

**Выводы**

Корреляционный поиск «Brute Force Access Behavior Detected» с использованием экстремального поиска включен в состав Splunk Enterprise Security. Поиск генерации контекста выполняется и обновляет контекст с повторяющимся интервалом. Корреляционный поиск ссылается на контекст, а концепт в контексте устанавливает пороговое значение. Концепт хеджируется на уровне «above medium» (выше медианного), таким образом, что корреляционный поиск будет создавать только существенное событие, когда количество неудачных аутентификаций, за которыми следует успешная аутентификация, является «high» (высокий) или «extreme» (экстремальный).

Вкратце этот процесс можно объяснить следующим образом: экстремальный поиск преобразовал «корреляционный поиск «Brute Force Access Behavior Detected» из «найти все попытки аутентификации, при которых количество неудачных проверок X сопровождалось успешной аутентификацией» в «найти все попытки аутентификации, когда за высоким или экстремальным количеством неудачных попыток аутентификации следует успешная аутентификация».

**Команды экстремального поиска**

|  |  |
| --- | --- |
| **Команда поиска** | **Описание** |
| xsWhere | Используется для соответствия концепта в определенном контексте и определения совместимости. |
| xsFindBestConcept | Используется при оценке счетчика поиска и сопоставлении счетчика с контекстом. Ближайшее совпадение возвращает термин, используемый концептом. Ключевые индикаторы безопасности используют эту команду. |
| xsUpdateDDContext | Используется для обновления контекста, определяемого данными. Плановый отчет, который вызывает «xsUpdateDDContext», создает контекст, представляющий историческую витрину.  | xsUpdateDDContext in  app=<app> name=<context> container=<container> scope=app |

|  |  |
| --- | --- |
| xsListContexts | Используется для составления списка всех контекстов в контейнере  | xsListContexts in <container> |
| xsListConcepts | Используется для составления списка всех концептов в контектсе  | xsListConcepts from <context> in <container> |
| xsDisplayContext | Используется для отображения диапазона значений в контексте, включая термины, используемые в концепте:  | xsDisplayContext <context> IN <container> |
| xsDisplayConcept | Используется для отображения диапазона значений в концепте:  | xsDisplayConcept <concept> from <context> in <container> | xsDisplayConcept <hedge> <concept> from <context> in <container> |