

Table of Contents

Table of Contents	1
Библиотеки	2
IP-адреса	3
Useragent браузеров	6
Типы контента	8
Списки URL	10
Категории URL	14
Текстовые списки	15
Почтовые адреса	18
Номера телефонов	20
Команды	22
Профили оповещений	24
Категории срабатываний	25
Внешние сервисы обогащений	26
Приложения syslog	28
Syslog фильтры UserID агента	29

IP-адреса

Documentation: ☒

Product: SIEM

Version: 7.1.x

Раздел **IP-адреса** содержит списки диапазонов IP-адресов, которые могут использоваться в поисковых запросах.

Списки IP-адресов создаются на панели **Группы**. Они могут быть **локальными** и **обновляемыми**.

Локальные списки создаются и хранятся на самом устройстве.

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

IP-адреса в эти списки добавляются администратором вручную на панели **Адреса из выбранной группы**:

IP-адреса добавляются в виде: IP-адрес, IP-адрес/маска сети или диапазон IP-адресов, например: 192.168.1.5, 192.168.1.0/24 или 192.168.1.5-192.168.2.100.

Обновляемые списки получают информацию об IP-адресах с внешних серверов по указанному в свойствах списка URL обновления:

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

На вкладке **Настройка расписания автоматических обновлений** настраивается расписание обновления этого списка:

Администратор имеет возможность создавать свои обновляемые списки IP-адресов. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми IP-адресами.	Создать файл list.txt со списком адресов. Список адресов записывается в обычный текстовый файл, где адреса прописываются в столбик без знаков препинания. Например: <pre>x.x.x.x y.y.y.y z.z.z.z</pre>
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список IP-адресов и указать URL для обновления.	На каждом устройстве создать список IP-адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. Устройство будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Примечание URL списка задается в формате: <code>http://x.x.x.x/</code> или <code>ftp://x.x.x.x/</code>. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2 в поле "часы" будет означать "каждые два часа".

Useragent браузеров

Documentation: ☒

Product: SIEM

Version: 7.1.x

Списки Useragent браузеров создаются в веб-консоли администратора в разделе **Библиотеки → Useragent браузеров → Категории**. Они содержат информацию о типах браузеров у пользователей.

Списки могут быть **локальными** и **обновляемыми**.

Локальные списки создаются и хранятся на самом устройстве.

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

Данные в эти списки добавляются администратором вручную на панели **Шаблоны useragent**. Искерпывающий список строк Useragent представлен на этом ресурсе: <http://www.useragentstring.com/pages/useragentstring.php>.

Обновляемые списки получают информацию с внешних серверов по указанному в свойствах списка URL обновления:

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

На вкладке **Настройка расписания автоматических обновлений** настраивается расписание обновления этого списка:

Администратор имеет возможность создавать свои обновляемые списки Useragent и централизованно распространять их на все свои устройства. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми Useragent.	Создать файл list.txt со списком Useragent .
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список Useragent и указать URL для обновления.	На каждом устройстве создать список Useragent. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. Устройство будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2" в поле "часы" будет означать "каждые два часа".

Типы контента

Version: 7.1.x

Documentation: ☒

Product: SIEM

Раздел **Типы контента** содержит список типов контента, которые могут использоваться в поисковых запросах.

Списки Типов контента создаются на панели **Категории**. Они могут быть **локальными** и **обновляемыми**.

Локальные списки создаются и хранятся на самом устройстве.

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

Данные в формате MIME в эти списки добавляются администратором вручную на панели **Типы контента**. Различные типы контента и их описание доступны по ссылке <https://www.iana.org/assignments/media-types/media-types.xhtml>.

Обновляемые списки получают данные с внешних серверов по указанному в свойствах списка URL обновления:

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

На вкладке **Настройка расписания автоматических обновлений** настраивается расписание обновления этого списка:

Администратор имеет возможность создавать свои списки типов контента и централизованно распространять их на все свои управляемые устройства. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми типами контента.	Создать файл list.txt со списком типов контента.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список типа контента и указать URL для обновления.	На каждом устройстве создать список типа контента. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. Устройство будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Списки URL

Documentation: ☒

Product: SIEM

Version: 7.1.x

Раздел **Списки URL** содержит списки URL-адресов, которые могут использоваться в поисковых запросах.

Списки URL создаются на панели **Списки URL**. Они могут быть **локальными** и **обновляемыми**.

Локальные списки создаются и хранятся на самом устройстве.

Необходимо установить категорию создаваемого списка в поле **Чувствительность к регистру**:

- **Чувствительный к регистру** — список URL адресов, чувствительных к регистру букв в адресе.
- **Нечувствительный к регистру** — список URL адресов, нечувствительных к регистру букв в адресе. Использование списка этой категории исключает необходимость перебора вариантов написания одного и того же выражения с буквами в различных регистрах.
- **Домен** — список адресов доменов для использования в правилах DNS-фильтрации.

Категория списка задается при его создании. Изменить категорию после создания списка нельзя.

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

Данные в эти списки добавляются администратором вручную на панели **URL**:

В списках можно использовать специальные символы «^», «\$» и «*»:

«*» — любое количество любых символов

«^» — начало строки

«\$» — конец строки

Символы «?» и «#» не могут быть использованы.

Если URL-запись начинается с http://, «https://», «ftp://» или содержит один или более символов «/», то это считается URL и применяется только для HTTP(S) фильтрации, к DNS-фильтрации такая запись не применяется. В противном случае строка рассматривается как имя домена и применяется для DNS-фильтрации и HTTP(S)-фильтрации.

Для фильтрации точного адреса используйте символы «^» и «\$»:

`^http://domain.com/exacturl$`

Для фильтрации точного URL всех дочерних папок используйте символ «^»:

`^http://domain.com/exacturl/`

Для фильтрации домена со всеми возможными URL используйте запись такого вида:

`domain.com`

Пример интерпретации URL-записей:

Пример записи	Обработка DNS- запросов	Обработка HTTP-запросов
yahoo.com или *yahoo.com*	Фильтруется весь домен и домены более высоких (3,4 и т.д.) уровней, например: sport.yahoo.com mail.yahoo.com а также: qweryahoo.com	Фильтруется весь домен и все URL этого домена, а также домены более высоких (3,4 и т.д.) уровней, например: http://sport.yahoo.com http://mail.yahoo.com https://mail.yahoo.com http://sport.yahoo.com/123 http://qwertyyahoo.com/
^mail.yahoo.com\$	Отфильтрован только mail.yahoo.com	Отфильтрованы только: http://mail.yahoo.com https://mail.yahoo.com
^mail.yahoo.com/\$	Ничего не отфильтровано	Ничего не отфильтровано, так как последний символ слэш определяет URL, но не указаны «https» или «http»
^http://finance.yahoo.com/personal-finance/\$	Ничего не отфильтровано	Отфильтрован только: http://finance.yahoo.com/personal-finance/
^yahoo.com/12345/	Ничего не отфильтровано	Отфильтрованы: http://yahoo.com/12345/whatever/ https://yahoo.com/12345/whatever/

Обновляемые списки получают данные с внешних серверов по указанному в свойствах списка URL обновления:

Необходимо установить категорию создаваемого списка в поле **Чувствительность к регистру** (описание поля см. [ранее](#)).

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

На вкладке **Настройка расписания автоматических обновлений** настраивается расписание обновления этого списка:

Администратор имеет возможность создавать собственные списки и централизованно распространять их на все свои устройства. Для создания таких списков необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимым списком URL.	Создать текстовый файл list.txt со списком URL в следующем формате: www.site1.com/url1 www.site2.com/url2 ... www.siteend.com/urlN
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.

Наименование	Описание
Шаг 5. Создать список и указать URL для обновления.	На каждом устройстве создать список URL. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. Устройство будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Примечание URL списка задается в формате: http://x.x.x.x/ или ftp://x.x.x.x/. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2" в поле "часы" будет означать "каждые два часа".

Категории URL

Documentation: 

Product: SIEM

Version: 7.1.x

Раздел **Категории URL** содержит группы категорий, которые могут использоваться в поисковых запросах.

Группы категорий создаются на панели **Группы URL категорий**. Категории в группу категорий URL добавляются на панели **Категории**.

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

Текстовые списки

Documentation: ☒

Product: SIEM

Version: 7.3.x

Раздел **Текстовые списки** содержит произвольные текстовые списки, которые могут использоваться в поисковых запросах.

Списки создаются на панели **Текстовые списки**. Они могут быть **локальными** и **обновляемыми**.

Локальные списки создаются и хранятся на самом устройстве.

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

Данные в эти списки добавляются администратором вручную на панели **Строки**:

Обновляемые списки получают данные с внешних серверов по указанному в свойствах списка URL обновления:

Если список предполагается использовать в поисковых запросах, необходимо в свойствах создаваемого списка поставить соответствующий флажок.

На вкладке **Настройка расписания автоматических обновлений** настраивается расписание обновления этого списка:

Администратор имеет возможность создавать собственные списки и централизованно распространять их на все свои устройства. Для создания таких списков необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимым списком.	Создать текстовый файл list.txt со списком.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 4. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список и указать URL для обновления.	На каждом устройстве создать текстовый список. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. Устройство будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Примечание URL списка задается в формате: <code>http://x.x.x.x/</code> или <code>ftp://x.x.x.x/</code>. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Почтовые адреса

Documentation: ☒
Product: SIEM
Version: 7.1.x

Элемент библиотеки **Почтовые адреса** позволяет создать группы почтовых адресов, которые впоследствии можно использовать в правилах фильтрации почтового трафика и для использования в оповещениях.

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу почтовых адресов	В панели Группы почтовых адресов нажать на кнопку Добавить , дать название группе.
Шаг 2. Добавить почтовые адреса в группу	Выделить созданную группу, нажать на кнопку Добавить на панели Почтовые адреса и добавить необходимые почтовые адреса.

Администратор имеет возможность создавать обновляемые списки почтовых адресов и централизованно распространять их на устройства UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком почтовых адресов.	Создать файл list.txt со списком почтовых адресов.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.

Наименование	Описание
Шаг 5. Создать список почтовых адресов и указать URL для обновления.	На каждом UserGate создать список адресов. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*/2" в поле "часы" будет означать "каждые два часа".

Администратор может экспортировать и импортировать списки почтовых адресов используя соответствующие кнопки **Экспорт/Импорт**.

Номера телефонов

Documentation: ☒
Product: SIEM
Version: 7.1.x

Элемент библиотеки **Номера телефонов** позволяет создать группы номеров, которые впоследствии можно использовать в правилах оповещения SMPP.

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать группу телефонных номеров	В панели Группы телефонных номеров нажать на кнопку Добавить , дать название группе.
Шаг 2. Добавить номера телефонов в группу	Выделить созданную группу, нажать на кнопку Добавить на панели Группа телефонных номеров и добавить необходимые номера.

Администратор имеет возможность создавать обновляемые списки телефонных номеров и централизованно распространять их на устройства UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком номеров.	Создать файл list.txt со списком номеров.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.
Шаг 5. Создать список телефонных номеров и указать URL для обновления.	На каждом UserGate создать список номеров. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: - Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. - Ежедневно. - Еженедельно. - Ежемесячно. - Каждые ... часов. - Каждые ... минут. - Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2" в поле "часы" будет означать "каждые два часа".

Администратор может экспортировать и импортировать списки телефонных номеров используя соответствующие кнопки **Экспорт/Импорт**.

Команды

Product: SIEM
Version: 7.2.x
Documentation: ☒

Данный раздел позволяет создавать группы команд, предназначенных для отправки на коннекторы.

Для создания группы команд необходимо указать следующие параметры:

Наименование	Описание
Шаг 1. Создать список команд.	На панели Группы команд нажать на кнопку Добавить , задать название списка, описание и тип списка.
Шаг 2. Указать адрес обновления списка (не обязательно).	В случае создания обновляемого списка указать адрес сервера обновления. Более подробно об обновляемых списках смотрите далее в этой главе.
Шаг 3. Добавить команды в группу.	На панели Команды нажать на кнопку Добавить и указать название и текст команды. Для определения переменных необходимо использовать фигурные скобки ({}). Далее переменные будут использованы для подстановки актуальных значений.

При написании команд для отправки на устройства UserGate синтаксис аналогичен синтаксису команд интерфейса командной строки (CLI) NGFW. Подробнее о командах CLI читайте в разделе [Интерфейс командной строки](#) руководства администратора NGFW.

Пример команды с добавлением IP-адреса в качестве переменной в список заблокированных IP-адресов:

```
set libraries ip-list Blocked_addresses ips + [ {SRC_IP} ]
```

Полный список переменных, относящихся к срабатываниям, смотрите в разделе [Действия реагирования](#).

Пример создания правила аналитики с действием типа отправки команды на коннектор приведен в статье [Как настроить правило аналитики SIEM](#).

Администратор имеет возможность создавать обновляемые списки команд и централизованно распространять их на устройства UserGate. Для создания такого списка необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл с необходимыми списком команд.	Создать файл list.txt со списком команд.
Шаг 2. Создать архив, содержащий этот файл.	Поместить файл в архив zip с именем list.zip .
Шаг 3. Создать файл с версией списка.	Создать файл version.txt , внутри него указать номер версии списка, например, 3. Необходимо инкрементировать данное значение при каждом обновлении списка.
Шаг 4. Разместить файлы на веб-сервере.	Разместить у себя на сайте list.zip и version.txt , чтобы они были доступны для скачивания.

Наименование	Описание
Шаг 5. Создать список команд и указать URL для обновления.	На каждом UserGate создать список. При создании указать тип списка Обновляемый и адрес, откуда необходимо загружать обновления. UserGate будет проверять наличие новой версии на вашем сайте в соответствии с настроенным расписанием скачивания обновлений. Расписание можно настроить в свойствах списка; возможно указать следующие варианты: • Отключено. Проверка наличия обновлений для выбранного элемента производиться не будет. • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "**/2" в поле "часы" будет означать "каждые два часа".

Администратор может экспортировать и импортировать списки команды используя соответствующие кнопки **Экспорт/Импорт**. При импорте необходимо создать файл, содержащий список команд, заданных в следующем формате: ИМЯ_КОМАНДЫ:ТЕКСТ_КОМАНДЫ (для определения переменных используйте фигурные скобки).

Профили оповещений

Product: SIEM

Version: 7.1.x

Documentation: ☒

Профиль оповещения указывает транспорт, с помощью которого оповещения могут быть доставлены получателям. Поддерживается 2 типа транспорта:

- SMTP, доставка сообщений с помощью email
- SMPP, доставка сообщений с помощью SMS практически через любого оператора сотовой связи или через большое количество SMS-центров рассылки

Для создания профиля сообщений SMTP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMTP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес сервера SMTP, который будет использоваться для отсылки почтовых сообщений.
Порт	Порт TCP, используемый сервером SMTP. Обычно для протокола SMTP используется порт 25, для SMTP с использованием SSL - 465. Уточните данное значение у администратора почтового сервера.
Безопасность	Варианты безопасности отправки почты, возможны варианты: Нет, STARTTLS, SSL.
Аутентификация	Включает аутентификацию при подключении к SMTP-серверу.
Логин	Имя учетной записи для подключения к SMTP-серверу.
Пароль	Пароль учетной записи для подключения к SMTP-серверу.

Для создания профиля сообщений SMPP необходимо нажать на кнопку **Добавить** в разделе **Профили оповещений**, выбрать вариант **Добавить профиль оповещения SMPP** и заполнить необходимые поля:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Хост	IP-адрес сервера SMPP, который будет использоваться для отсылки SMS сообщений.
Порт	Порт TCP, используемый сервером SMPP. Обычно для протокола SMPP используется порт 2775, для SMPP с использованием SSL - 3550.
SSL	Использовать или нет шифрацию с помощью SSL.
Логин	Имя учетной записи для подключения к SMPP-серверу.
Пароль	Пароль учетной записи для подключения к SMPP-серверу.
Правила трансляции номеров	В некоторых случаях SMPP-провайдер ожидает номер телефона в определенном формате, например, в виде 89123456789. Для соответствия требованиям провайдера можно указать замену первых символов номеров с одних на другие. Например, заменить все номера, начинающиеся на +7, на 8.

Категории срабатываний

Documentation: 

Product: SIEM

Version: 7.1.x

Элемент библиотеки **Категории срабатываний** позволяет создать категории, по которым можно группировать определенные срабатывания правил аналитики, применяемые к событиям. Более подробно о правилах аналитики смотрите в разделе [Аналитика](#). По умолчанию создаются категории:

- Availability — правила аналитики, определяющие инциденты, приводящие к ухудшению доступности информационных систем.
- Performance — правила аналитики, определяющие инциденты, приводящие к ухудшению производительности информационных систем.
- Security — правила аналитики, определяющие инциденты, приводящие к ухудшению безопасности информационных систем.

Внешние сервисы обогащений

Documentation: ☒

Product: SIEM

Version: 7.1.x

В данном элементе библиотеки представлены ресурсы, с помощью которых происходит дополнительный сбор информации об угрозах. С данных источников приходят фиды — структурированные проанализированные данные об IP-адресах и доменах, с которых происходит распространение вредоносных файлов, их примеры и хэши; списки фишинговых сайтов, почтовые адреса отправителей фишинговых писем; адреса, с которых происходит сканирование сетей с целью обнаружения уязвимостей; IP-адреса, с которых проводятся атаки типа брутфорс; сигнатуры для обнаружения вредоносного программного обеспечения.

Чтобы использовать сервисы обогащения, необходимо их включить. Некоторые сервисы требуют прохождения регистрации с предоставлением ключа доступа.

Наименование	Описание
dnsgoogle	Интернет-сервис компании Google, представляющий собой общедоступные DNS-серверы. Подробнее: https://dns.google . Предназначен для типов улик: IP.
urlhaus	Проект abuse.ch. Целью проекта является сбор, отслеживание и обмен URL-адресами вредоносных программ. Подробнее: https://urlhaus.abuse.ch/ . Предназначен для типов улик: Домен, Хэш, Имя хоста, IP, URL.
dshield	Система корреляции журналов межсетевого экрана для совместной работы. Система получает журналы от добровольцев со всего мира и использует их для анализа тенденций атак. Подробнее: https://www.dshield.org/xml.html . Предназначен для типов улик: Домен, FQDN, IP.
cybercrime	Сервис предоставляет информацию об уровнях угрозы разных объектов. Подробнее: http://cybercrime-tracker.net . Предназначен для типов улик: Домен, FQDN, IP, URL, Другое.
cyberprotect	Сервис предоставляет информацию об уровнях угрозы разных объектов. Подробнее: https://console.threatscore.cyberprotect.cloud/ . Предназначен для типов улик: Домен, Хэш, IP, URL, Агент пользователя.
unshorten	Сервис предоставляет возможности предварительного просмотра целевого URL для любого короткого URL и проверки безопасности на вредоносные ссылки. Сервис не использует внешний ресурс; анализирует ответ на запрос по тестируемому URL. Предназначен для типов улик: URL.
ipwhois	Сервис позволяет получить информацию об IP-адресах. Подробнее: https://ipwhois.io/ . Предназначен для типов улик: IP.
ipinfo	Инструмент для определения владельца, Интернет-провайдера и местонахождения веб-сайта, домена или IP-адреса. Подробнее: https://ipinfo.io/ . Предназначен для типов улик: IP. Для использования сервиса необходимо ввести реквизиты.

Наименование	Описание
hashdd	Сервис предоставляет базу вредоносных хэшей файлов и различные проверки для получения полного представления об угрозе. Подробнее: https://hashdd.com/. Предназначен для типов улик: Хэш. Для использования сервиса необходимо ввести реквизиты.
urlscan	Сервис для получения информации о подозрительных, вредоносных и фишинговых URL. Подробнее: https://urlscan.io/. Предназначен для типов улик: Домен, FQDN, Хэш, IP, URL. Для использования сервиса необходимо ввести реквизиты.
emailrep	Система, которая собирает данные об адресах электронной почты, доменах и пользователях. Подробнее: https://emailrep.io/. Предназначен для типов улик: Почта. Для использования сервиса необходимо ввести реквизиты.
greynoise	Компания занимается анализом фоновых шума Интернета (пакеты данных, адресованные IP-адресам или портам, где нет сетевого устройства, настроенного для их приёма). Благодаря такой фильтрации снижается количество ложных срабатываний. Подробнее: https://www.greynoise.io/. Предназначен для типов улик: IP. Для использования сервиса необходимо ввести реквизиты.
abuseip	Проект, который занимается борьбой со злоумышленной деятельностью. Подробнее: https://www.abuseipdb.com/. Предназначен для типов улик: IP. Для использования сервиса необходимо ввести реквизиты.
hybridanalysis	Сервис проверки файлов на вредоносность. Подробнее: https://www.hybrid-analysis.com/. Предназначен для типов улик: Хэш. Для использования сервиса необходимо ввести реквизиты.

Documentation: 
Product: SIEM
Version: 7.1.x

Данный раздел содержит приложения, которые могут быть использованы в правилах syslog для сбора информации.

Чтобы добавить приложение необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать приложение.	Нажать кнопку Добавить и указать название и описание приложения.
Шаг 2. Указать приложение.	Указать название приложения, для которого будут применены правила syslog.

Syslog фильтры UserID агента

Version: 7.1.x, 7.2.x
Documentation: ☒
Product: SIEM

При использовании Syslog в качестве источников событий UserGate производит фильтрацию событий в соответствии с указанными Syslog фильтрами UserID агента. Фильтры Syslog представляют из себя стандартные Regexp выражения, которые пользователь может писать и сам. В стандартной поставке представлены два вида фильтров:

Наименование	Описание
SSH Authentication	Фильтр предназначенный для отслеживания событий входа/выхода пользователей по протоколу SSH в журналах syslog.
Unix PAM Authentication	Фильтр предназначенный для отслеживания событий входа/выхода пользователей посредством технологии Pluggable Authentication Modules (PAM) в журналах syslog.
Unix PUserGate WEC Agent	Фильтр, предназначенный для отслеживания событий, переданных через syslog из UserID агента для AD/WEC-серверов. (Доступно начиная с релиза ПО 7.2.0).

ПримечаниеИспользуя правила Regexp, возможно написание дополнительных правил. Таким образом фильтры Syslog представляют из себя универсальный инструмент, который можно использовать практически в любых случаях.

Найденные события отображаются во вкладке **Журналы и отчёты**, в разделе **Журналы → Агент UserID → Syslog**.

