

Table of Contents

Table of Contents	1
Журналы и отчеты	2
Журналы	3
Описание	4
Журнал событий	5
Журнал веб-доступа	6
Журнал трафика	7
Журнал инспектирования SSH	8
История поиска	9
Экспорт журналов	10
Журнал СОВ	13
Журнал АСУ ТП	14
Поиск и фильтрация данных	15
Отчеты	17
Общие сведения	18
Шаблоны	19
Пользовательские шаблоны	20
Правила отчетов	21
Созданные отчеты	23
Отчеты инцидентов	24
Общие сведения	25
Правила отчетов инцидентов	26
Созданные отчеты инцидентов	27
Шаблоны отчетов инцидентов	28

Описание

Version: 7.0.1

Product: LogAn

Documentation: ☒

LogAn журналирует все события, которые происходят во время его работы и работы подключенных к нему серверов, и записывает их в следующие журналы:

- **Журнал событий** — события, связанные с изменением настроек сервера LogAn, авторизацией пользователей, администраторов, обновлениями различных списков и т.п.
- **Журнал веб-доступа** — подробный журнал всех веб-запросов, обработанных LogAn.
- **Журнал трафика** — подробный журнал срабатываний правил межсетевого экрана, NAT, DNAT, Port forwarding, Policy-based routing. Для регистрации данных событий необходимо включить журналирование в необходимых правилах межсетевого экрана, NAT, DNAT, Port forwarding, Policy-based routing.
- **Журнал СОВ** — события, регистрируемые системой обнаружения и предотвращения вторжений.
- **Журнал АСУ ТП** — события, регистрируемые правилами контроля АСУ ТП.
- **Журнал инспектирования SSH** — журнал срабатывания правил инспектирования SSH. Для регистрации данных событий необходимо включить журналирование.
- **История поиска** — поисковые запросы пользователей в популярных поисковых системах.
- **Журнал событий конечных устройств** — отображает события, получаемые от контролируемых с помощью программного обеспечения UserGate Endpoint конечных устройств.
- **Журнал правил конечных устройств** — события срабатывания правил межсетевого экрана конечных устройств, в настройках которых включено логирование.
- **Приложения конечных устройств** — отображает приложения, которые когда-либо запускались на конечных устройствах.
- **Аппаратура конечных устройств** — содержит информацию об устройствах, подключённых к конечным устройствам.
- **Системный журнал (Syslog)** — отображены записи сообщений о событиях удалённых Unix-систем, полученные по протоколу Syslog.

Управление журналами автоматизировано: журналы циклически перезаписываются, обеспечивая необходимое для работы свободное дисковое пространство.

Примечание Записи журнала событий никогда не ротируются.

Ротация записей журналов (всех, кроме журнала событий) происходит автоматически по критерию свободного пространства на данном разделе. Записи о ротации базы данных будут отображены в журнале событий LogAn.

Журнал событий

Version: 6.1.9, 7.0.1, 7.1.0

Product: LogAn, SIEM

Documentation: 

Журнал событий отображает события, связанные с изменением настроек сервера LogAn, например, добавление/удаление/изменение данных учетной записи, правила или любого другого элемента. Здесь же отображаются все события входа в веб-консоль, авторизации пользователей через Captive-портал и другие.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как диапазон дат, компоненту, важности, типу события.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Журнал веб-доступа

Version: 6.1.9, 7.0.1, 7.1.0

Product: LogAn, SIEM

Documentation: 

Журнал веб-доступа отображает все запросы пользователей в Интернет по протоколам HTTP и HTTPS. Отображается следующая информация:

- узел UserGate, на котором произошло событие;
- время события;
- пользователь;
- действия;
- правило;
- причины (при блокировке сайта);
- URL назначения;
- зона источника;
- IP-адрес источника;
- порт источника;
- IP назначения;
- порт назначения;
- категории;
- протокол (HTTP);
- метод (HTTP);
- код ответа (HTTP);
- MIME (если присутствует);
- Байт передано/получено;
- пакетов отправлено;
- реферер (при наличии);
- операционная система;
- Useragent Браузера.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например, таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Журнал трафика

Version: 6.1.9, 7.0.1, 7.1.0

Product: LogAn, SIEM

Documentation: 

Журнал трафика отображает события срабатывания правил межсетевого экрана или правил NAT, в настройках которых включено логирование пакетов. Отображается следующая информация:

- узел UserGate, на котором произошло событие;
- время события;
- пользователь;
- действие;
- правило;
- приложение;
- протокол;
- зона источника;
- адрес источника;
- порт источника;
- IP-назначения;
- порт назначения;
- NAT IP-источника (если это правило NAT);
- NAT порт источника (если это правило NAT);
- NAT IP назначения (если это правило NAT);
- NAT порт назначения (если это правило NAT);
- Байт отправлено/получено;
- пакетов.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например, таким, как учетная запись пользователя, правило, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Журнал инспектирования SSH

Documentation: ☒

Version: 6.1.9, 7.0.1, 7.1.0

Product: LogAn, SIEM

Журнал инспектирования SSH отображает сработавшие правила инспектирования SSH. Отображается следующая информация:

- узел UserGate, на котором произошло событие;
- время;
- пользователь;
- действие;
- правило;
- команда;
- зона источника;
- IP-адрес источника;
- порт источника;
- MAC-адрес источника;
- зона назначения;
- IP-адрес назначения;
- порт назначения.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить отмеченными только те столбцы, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например, таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

История поиска

Version: 6.1.9, 7.0.1, 7.1.0

Product: LogAn, SIEM

Documentation: 

В разделе **История поиска** отображаются все поисковые запросы пользователей, для которых настроено журналирование в политиках веб-безопасности. Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например, таким, как пользователи, диапазон дат, поисковые системы и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Экспорт журналов

Version: 7.0.1, 7.1.0
Product: LogAn, SIEM
Documentation: ☒

Функция экспортирования журналов LogAn позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security Information and Event Management).

UserGate LogAn поддерживает выгрузку следующих журналов:

- Журнал DNS.
- Журнал событий.
- Журнал веб-доступа.
- Журнал COB.
- Журнал АСУ ТП.
- Журнал инспектирования SSH.
- Журнал трафика.
- Журнал событий конечных устройств.
- Журнал правил конечных устройств.
- Приложения конечных устройств.
- Аппаратура конечных устройств.

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP проводится по указанному в конфигурации расписанию или разово (кнопка **Послать разово**). Отправка на серверы Syslog происходит сразу же при добавлении записи в журнал.

Для отправки журналов необходимо создать конфигурации экспорта журналов в разделе **Экспорт журналов**.

При создании конфигурации требуется указать следующие параметры:

Наименование	Описание
Название правила	Название правила экспорта журналов.
Описание	Опциональное поле для описания правила.

Наименование	Описание
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: • Журнал DNS. • Журнал событий. • Журнал веб-доступа. • Журнал COB. • Журнал ACU ТП. • Журнал инспектирования SSH. • Журнал трафика. • Журнал событий конечных устройств. • Журнал правил конечных устройств. • Приложения конечных устройств. • Аппаратура конечных устройств. Для каждого из журналов возможно указать синтаксис выгрузки: • CEF — Common Event Format (ArcSight). • JSON — JSON format. • @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON. Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов. Подробное описание форматов журналов читайте в Приложение 2. Описание форматов журналов.
Тип сервера	SSH (SFTP), FTP, Syslog.
Адрес сервера	IP-адрес или доменное имя сервера.
Транспорт	Только для типа серверов Syslog — TCP или UDP.
Порт	Порт сервера, на который следует отправлять данные.
Протокол	Только для типа серверов Syslog — RFC5424 или BSD Syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM.
Критичность	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • Тревога: состояние, требующее незамедлительного вмешательства. • Критическая: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • Ошибки: в системе возникли ошибки. • Предупреждения: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • Уведомительная: события, которые относятся к необычному поведению системы, но не являются ошибками. • Информативная: информационные сообщения.

Наименование	Описание
Объект	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • Сообщения пользовательские. • Системный сервис. • Безопасность/авторизация. • Аудит. • Тревога. • Local 0. • Local 1. • Local 2. • Local 3. • Local 4. • Local 5. • Local 6. • Local 7.
Имя хоста	Только для типа серверов Syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер Syslog, в формате Fully Qualified Domain Name (FQDN).
App-Name	Только для типа серверов Syslog. Уникальное имя приложения, которое отправляет данные на сервер Syslog.
Логин	Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Пароль	Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Повторите пароль	Подтверждение пароля учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog.
Расписание	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты: • 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".

Журнал COB

Version: 7.0.1

Product: NGFW, LogAn

Documentation: 

Журнал системы обнаружения вторжений отображает сработавшие сигнатуры COB, для которых установлено действие журналировать или блокировать. Отображается следующая информация:

- Файлы Pcap.
- Узел NGFW, на котором произошло событие.
- Время.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Сигнатуры.
- Приложение.
- Сетевой протокол.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- MAC назначения.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Журнал АСУ ТП

Documentation: ☒

Version: 6.1.9, 7.0.1

Product: NGFW, LogAn

Журнал АСУ ТП отображает срабатывания правил автоматизированной системы управления технологическим процессом, для которых включена функция журналирования. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.
- Время.
- Действие.
- Правило.
- Зона источника.
- IP-адрес источника.
- IP-адрес назначения.
- Порт назначения.
- Протокол АСУ ТП.
- Команда АСУ ТП.
- Адрес регистра.

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого следует кликнуть указателем мыши на любой из столбцов, и в появившемся контекстном меню оставить галочки только для тех столбцов, которые необходимо отображать.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например таким, как протокол, диапазон дат, действие и т.д.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Поиск и фильтрация данных

Version: 7.0.1, 7.1.0
Product: LogAn, SIEM
Documentation: ☒

Количество записей, регистрируемых в журналах, как правило, очень велико, и LogAn предоставляет удобные способы поиска и фильтрации необходимой информации. Администратор может использовать простой и расширенный поиск по содержимому журналов.

При использовании простого поиска администратор использует графический интерфейс, чтобы задать фильтрацию по значениям требуемых полей журналов, отфильтровывая таким образом ненужную информацию. Например, администратор может задать интересующий его диапазон времени, список пользователей, категорий и т.п. Задание критериев поиска интуитивно понятно и не требует специальных знаний.

Построение более сложных фильтров возможно в режиме расширенного поиска с использованием специального языка запросов. В режиме расширенного поиска можно строить запросы с использованием полей журналов, которые недоступны в базовом режиме. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Значения полей могут быть введены с использованием одинарных или двойных кавычек, или без них, если значения не содержат пробелов. Для группировки нескольких условий можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

Наименование	Описание
AND или and	Логическое И, требует выполнения всех условий, заданных в запросе.
OR или or	Логическое ИЛИ, достаточно выполнения одного из условий запроса.

Операторы определяют условия фильтра и могут быть следующими:

Наименование	Описание
=	Равно. Требует полного совпадения значения поля указанному значению, например, <i>ip=172.16.31.1</i> будут отображены все записи журнала, в котором поле IP будет точно соответствовать значению 172.16.31.1.
!=	Не равно. Значение указанного поля не должно совпадать с указанным значением, например, <i>ip!=172.16.31</i> будут отображены все записи журнала, в котором поле IP не будет равно значению 172.16.31.1.
<=	Меньше либо равно. Значение поля должно быть меньше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, <i>date <= '2019-03-28T20:59:59' AND statusCode=303</i> .
>=	Больше либо равно. Значение поля должно быть больше либо равны указанному в запросе значению. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, <i>date >= "2019-03-13T21:00:00" AND statusCode=200</i> .
<	Меньше. Значение поля должно быть меньше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, <i>date < '2019-03-28T20:59:59' AND statusCode=404</i> .
>	Больше. Значение поля должно быть больше указанного в запросе значения. Может быть применимо только для полей, поддерживающих сравнения, например, поля даты, portSource, portDest, statusCode и т.п., например, <i>(statusCode>200 AND statusCode <300) OR (statusCode=404)</i> .
IN	Позволяет указать несколько значений поля в запросе. Список значений необходимо указывать в круглых скобках, например, например, <i>category IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')</i> .
NOT IN	Позволяет указать несколько значений поля в запросе; будут отображены записи, не содержащие указанные значения. Список значений необходимо указывать в круглых скобках, например, <i>category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud','reputation high risk','unknown category')</i> .

Наименование	Описание
~	Содержит. Позволяет указать подстроку, которая должна находиться в указанном поле, например, <i>browser ~ "Mozilla/5.0"</i> Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
!~	Не содержит. Позволяет указать подстроку, которая не должна присутствовать в указанном поле, например, <i>browser !~ "Mozilla/5.0"</i> Данный оператор может быть применен только к полям, в которых хранятся строковые данные.
MATCH	При использовании оператора MATCH подстрока, которая должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, <pre>details MATCH \"module\":\"threats\"</pre> Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.
NOT MATCH	При использовании оператора NOT MATCH подстрока, которая не должна присутствовать в указанном поле, задаётся в формате JSON и с использованием одинарных кавычек, например, <pre>details NOT MATCH \"module\":\"threats\"</pre> Синтаксис запросов с использованием данного оператора соответствует стандарту RE2. Подробнее о синтаксисе Google/RE2: https://github.com/google/re2/wiki/Syntax.

При составлении расширенного запроса LogAn показывает возможные варианты названия полей, применимых к ним операторов и возможных значений, облегчая оператору системы формирование сложных запросов. При переключении режима поиска с основного на расширенный LogAn автоматически формирует строку с поисковым запросом, которая соответствует фильтру, указанному в основном режиме поиска.

Общие сведения

Documentation: ☒
Product: LogAn, SIEM
Version: 6.1.9, 7.0.1, 7.1.0

С помощью отчетов администратор может предоставить различные срезы данных о событиях безопасности, конфигурирования или действиях пользователей. Отчеты могут создаваться по созданным ранее правилам и шаблонам в автоматическом режиме и отправляться адресатам по электронной почте.

Раздел **Отчеты** состоит из четырех подразделов — **Шаблоны**, **Пользовательские шаблоны**, **Правила отчетов** и **Созданные отчеты**. Чтобы создать отчет необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило создания отчета	Создать правило создания отчета, в котором указать необходимые параметры создания отчета.
Шаг 2. Запустить отчет	Запустить отчет в ручном режиме или дождаться времени, когда он запустится в автоматическом режиме по указанному в правиле расписанию.
Шаг 3. Получить отчет	Получить отчет по почте, если в правиле была настроена отправка отчета по почте, или скачать полученный отчет в разделе Созданные отчеты .

ПримечаниеПроцесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов.

Шаблоны

Documentation: ☒

Product: LogAn

Version: 6.1.9, 7.0.1

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов предоставляются компанией разработчиком UserGate.

Список возможных шаблонов отчетов, сгруппированных по категориям:

- **Captive-портал** — группа шаблонов по событиям, авторизации пользователей с помощью Captive-портала.
- **События** — группа шаблонов по событиям, регистрируемым в журнале событий.
- **COB** — группа шаблонов по событиям, регистрируемым в журнале COB.
- **Сетевая активность** — группа шаблонов по событиям, регистрируемым в журнале трафика.
- **Веб-портал** — группа шаблонов авторизации через SSL VPN.
- **Трафик** — группа шаблонов по событиям, регистрируемым в журнале трафика и относящимся к объему потребленного трафика пользователями, приложениями и т.п.
- **VPN** — группа шаблонов по событиям, относящимся к VPN.
- **Веб-активность** — группа шаблонов по событиям, регистрируемым в журнале веб-доступа.

Каждый шаблон содержит название, описание отчета и тип отображения отчета (таблица, гистограмма, пирог).

Пользовательские шаблоны

Documentation: ☒
Product: LogAn
Version: 7.0.1

В отличие от обычных шаблонов, предоставляемых производителем решения, пользовательские шаблоны позволяют создать отчет по тем критериям, которые необходимо пользователю. Администратор может выбрать необходимые поля для отображения, задать условия и возможные группировки. Созданные пользовательские отчеты могут быть использованы в правилах построения отчетов наряду с обычными предопределенными отчетами. Для создания пользовательского шаблона необходимо в разделе **Отчеты → Пользовательские отчеты** нажать на кнопку **Добавить** и заполнить следующие параметры:

Наименование	Описание
Название	Название пользовательского шаблона.
Описание	Опциональное поле для описания пользовательского шаблона.
Категория	Выбор источника данных для данного шаблона. Доступны значения: • Журнал событий. • Журнал трафика. • Журнал веб-доступа. • Журнал COB. • Журнал инспектирования SSH. • Срабатывания. • Журнал событий конечных устройств. • Журнал правил конечных устройств. • Приложения конечных устройств.
Запрос фильтра	SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении отчета по данному шаблону. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. В качестве полей данных можно использовать столбцы, перечисленные ниже в поле Столбцы . Ключевые слова и операторы, а также примеры их использования можно посмотреть в разделе документации Поиск и фильтрация данных .
Сортировать по	Укажите поле данных, по которому будут отсортированы данные в отчете. Сортировку можно указать по возрастанию и по убыванию.
Группировать по	Укажите поле данных, по которому будут сгруппированы данные в отчете.
Столбцы	Список столбцов, доступных для конкретного источника данных.
Выбранные	Список столбцов, выбранных для отображения в отчете.

Правила отчетов

Documentation: ☒
Product: LogAn, SIEM
Version: 6.1.9, 7.0.1, 7.1.0

Правило отчета задает параметры создаваемого отчета, а также расписание запуска отчетов и способы доставки отчета пользователям. При создании правила отчета администратор указывает следующие параметры:

Наименование	Описание
Включено	Включение/отключения отчета.
Название	Название правила.
Описание	Опциональное поле для описания правила.
Язык отчета	Выбор языка, который будет использован в отчете.
Диапазон	Диапазон времени, за который необходимо подготовить отчет.
Формат отчета	Формат отчета (PDF, HTML, XML, CSV), в котором будет создаваться данный отчет. Важно! Создание отчета в формате PDF создает высокую нагрузку на процессор и память. Чем объемнее отчет, тем более высокая нагрузка. Не используйте формат отчета PDF для пользовательских шаблонов. Для шаблонов Подробный список всех посещенных URL и Подробный список всех посещенных сайтов автоматически используется формат CSV, независимо от выбранного формата.
Количество записей	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству топ записей, например, топ 20 пользователей с ошибочной авторизацией в веб-консоль.
Количество в группировке (если применимо)	Задание ограничения числа записей, которые будут выводиться в отчетах, в которых присутствует ограничение по количеству сгруппированных записей, например, топ 10 пользователей по категориям — для каждой категории будет указано не более 10 пользователей. Данное ограничение применимо только для тех шаблонов отчетов, которые содержат группирование.
Пользователи	Задает пользователей или группы пользователей, для которых будет создаваться отчет. Если оставить поле пустым, то отчет будет создаваться для всех пользователей.
Шаблоны	Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон.

Наименование	Описание
Расписание	Выбор расписания для создания отчетов. Возможны варианты: - 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: 0-31) (месяц: 0-12) (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".
Доставка	Возможность задать опциональную отправку созданного отчета получателям по протоколу SMTP. Необходимо задать: - Профиль SMTP, который будет использован для отправки отчетов. Подробно о настройке профилей SMTP смотрите в главе Профили оповещений. - От — имя отправителя письма. - Тема письма — тема письма (subject). - Тело письма — содержимое письма. - Получатели — список получателей письма. Получатели должны быть добавлены в списки библиотеки Почтовые адреса.

Примечание Процесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов. Особенно важно учитывать загрузку ресурсов при запуске отчетов за большой диапазон времени.

Примечание Для того, чтобы запустить правило отчета не обязательно включать его и указывать время запуска правила. В ручном режиме можно запустить любой, в том числе отключенный отчет, для этого в списке правил необходимо выбрать требуемое правило и нажать на кнопку Запустить сейчас. Готовый отчет после создания будет доступен в разделе Созданные отчеты.

Созданные отчеты

Documentation: ☒

Product: LogAn, SIEM

Version: 6.1.9, 7.0.1, 7.1.0

В разделе **Созданные отчеты** хранятся все полученные отчеты. Отчеты создаются в формате pdf или csv. Для каждого отчета указывается название отчета, которое совпадает с названием правила отчета, которое было использовано для создания данного отчета, время создания отчета и размер отчета.

Для скачивания отчета необходимо использовать кнопку **Скачать**, для удаления — **Удалить**.

Время хранения готовых отчетов (ротация) настраивается по нажатию на кнопку **Настроить**. Значение по умолчанию — 60 дней.

Общие сведения

Documentation: ☒
Product: LogAn, SIEM
Version: 7.0.1, 7.1.0

В данном разделе администратор может формировать отчёты об инцидентах информационной безопасности. Отчеты могут создаваться в соответствии с созданными правилами и шаблонам; отчёт доступен для скачивания или передачи на коннектор.

Раздел состоит из трех подразделов - **Шаблоны отчетов инцидентов**, **Правила отчетов инцидентов** и **Созданные отчеты инцидентов**. Чтобы создать отчет, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило создания отчета.	Создать правило создания отчета, в котором указать необходимые параметры создания отчета.
Шаг 2. Запустить отчет.	Выбрать инцидент и сгенерировать отчет.
Шаг 3. Получить отчет.	Записи о создании отчетов доступны в разделе Созданные отчеты инцидентов .

Правила отчетов инцидентов

Documentation: ☒
Product: LogAn, SIEM
Version: 7.0.1, 7.1.0

Правило отчета задает параметры создаваемого отчета, а также способы доставки отчета пользователям. При создании правила отчета администратор указывает следующие параметры:

Наименование	Описание
Название	Название правила.
Описание	Опциональное поле для описания правила.
Язык отчёта	Выбор языка, который будет использован в отчете.
Часовой пояс	Часовой пояс, который будет использоваться при формировании отчёта.
Формат отчёта	Формат (PDF, HTML), в котором будет создаваться данный отчет.
Коннектор	Коннектор, на который необходимо отправить отчёт (необязательно).
Шаблоны	Список шаблонов, которые будут использоваться для построения отчета. Обязательно необходимо добавить хотя бы один шаблон.

ПримечаниеПроцесс создания отчета может продолжаться достаточно длительное время и может потреблять большое количество вычислительных ресурсов. Особенно важно учитывать загрузку ресурсов при запуске отчетов за большой диапазон времени.

После создания правила пользователь может запустить создание отчёта по выбранному инциденту. После формирования отчёт доступен для скачивания локально или передачи на выбранный коннектор.

Созданные отчеты инцидентов

Documentation: 

Product: LogAn, SIEM

Version: 7.0.1, 7.1.0

В разделе **Созданные отчеты инцидентов** хранятся все сформированные отчеты. Отчеты создаются в формате pdf или html. Для каждого отчета указывается название отчета, которое совпадает с названием правила отчета, использованного для создания данного отчета, время создания отчета и файл отчета с указанием его размера. Все отчеты доступны для скачивания и удаления.

Время хранения готовых отчетов (ротация) настраивается по нажатию на кнопку **Настроить**.

Шаблоны отчетов инцидентов

Documentation: 

Product: LogAn, SIEM

Version: 7.0.1, 7.1.0

Шаблон определяет внешний вид и поля, которые будут использоваться в отчете. Шаблоны отчетов инцидентов делятся на 2 категории:

- **Форма ключ-заключение** — шаблоны, позволяющие настроить поля, которые необходимо отобразить в отчёте. Шаблоны данного типа пользователь может создавать самостоятельно.
- **Инциденты** — группа шаблонов для создания отчётов по инцидентам. Шаблоны предоставляются компанией UserGate.

Каждый шаблон содержит название, описание отчета и тип отображения отчета (таблица, гистограмма, пирог).

