

Table of Contents

Table of Contents	1
Журналы и отчеты	2
Журналы	3
Общие сведения	4
Журнал событий	5
Журнал веб-доступа	6
Журнал DNS	7
Журнал трафика	8
Журнал COB	9
Журнал АСУ ТП	10
Журнал инспектирования SSH	11
История поиска	12
Журналы конечных устройств	13
Журнал syslog	14
Журнал защиты почтового трафика	15
Журнал UserID	16
Журнал RADIUS	17
Экспорт журналов	18
Пользовательская нормализация логов	21
Поиск и фильтрация данных	31
Описание форматов журналов	32
Экспорт журналов в формате CEF	33
Экспорт журналов в формате JSON	59
Отчеты	75
Общие сведения	76
Шаблоны	77
Создание пользовательских шаблонов отчетов	78
Правила отчетов	79
Созданные отчеты	81
Отчеты инцидентов	82
Общие сведения	83
Шаблоны отчетов инцидентов	84
Правила отчетов инцидентов	85
Созданные отчеты инцидентов	86

Общие сведения

Product: SIEM

Version: 7.x

Documentation: 

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

- **Журнал событий** — содержит события, связанные с изменением настроек серверов, подключенных к UserGate SIEM, авторизацией пользователей, администраторов, обновлениями различных списков и т.п.
- **Журнал веб-доступа** — подробный журнал всех веб-запросов, обработанных UserGate SIEM.
- **Журнал DNS** — содержит события, связанные с DNS трафиком.
- **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** — содержит события, регистрируемые системой обнаружения и предотвращения вторжений.
- **Журнал АСУ ТП** — содержит события, регистрируемые правилами контроля АСУ ТП.
- **Журнал инспектирования SSH** — журнал срабатывания правил инспектирования SSH. Для регистрации данных событий необходимо включить журналирование.
- **История поиска** — содержит поисковые запросы пользователей в популярных поисковых системах.
- **Журнал событий конечных устройств** — отображает события, получаемые от контролируемых с помощью программного обеспечения UserGate Endpoint конечных устройств, а также события, полученные из контроллера домена AD по WMI.
- **Журнал правил конечных устройств** — события срабатывания правил межсетевого экрана конечных устройств, в настройках которых включено журналирование.
- **Приложения конечных устройств** — отображает приложения, которые когда-либо запускались на конечных устройствах.
- **Аппаратура конечных устройств** — содержит информацию об устройствах, подключённых к конечным устройствам.
- **Журнал syslog** — отображены записи сообщений о событиях удалённых Unix-систем, полученные по протоколу syslog.
- **Журнал защиты почтового трафика** — содержит события срабатывания правил защиты почтового трафика, в настройках которых включено журналирование.
- **Журнал UserID** — содержит описание событий отражающие результат работы UserID агента.
- **Журнал RADIUS** — содержит события, собранные агентом UserID из данных RADIUS accounting.
- **Журнал событий SIEM** — содержит события, связанные с изменением настроек сервера UserGate SIEM, авторизацией пользователей, администраторов, обновлениями различных списков и т.п.

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

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 UserGate SIEM.

Ротация записей журнала событий не производится.

Журнал событий

Documentation: 

Product: SIEM

Version: 7.x

Журнал событий отображает события, связанные с изменением параметров сервера UserGate SIEM, например, добавление, удаление или 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, компоненте, 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

Documentation: ☒

Product: SIEM

Version: 7.x

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.

Documentation: ☒
Product: SIEM
Version: 7.x

Журнал DNS отображает события, связанные с DNS трафиком. Для логирования событий DNS на UserGate NGFW должна быть включена DNS-фильтрация в настройках DNS-прокси и разрешено журналирование в правилах контентной фильтрации, в которые будет попадать DNS трафик.

Отображается следующая информация:

- Узел.
- Время.
- Пользователь.
- Правило.
- Причины.
- Имя домена.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC-адрес источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Сетевой протокол.
- Категория URL.
- Информация.

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 трафика

Product: SIEM

Documentation: ☒

Version: 7.x

Журнал трафика отображает события срабатывания правил межсетевого экрана или правил NAT, в настройках которых включено журналирование. 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.

Documentation: ☒
Product: SIEM
Version: 7.x

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

- Файлы Pcap.
- Узел UserGate 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.

Documentation: ☒
Product: SIEM
Version: 7.x

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

- Узел UserGate 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.

Documentation: ☒
Product: SIEM
Version: 7.x

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: 7.x
Documentation: 
Product: SIEM

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.

Журналы конечных устройств

Documentation: 

Product: SIEM

Version: 7.x

Журналы конечных устройств отображают информацию, получаемую от контролируемых с помощью программного обеспечения UserGate Client конечных устройств.

В UserGate SIEM имеются следующие журналы:

- **Журнал событий конечных устройств** — отображает события, получаемые от конечных устройств.
- **Журнал правил конечных устройств** — события срабатывания правил межсетевого экрана конечных устройств, в настройках которых включено журналирование.
- **Приложения конечных устройств** — отображает приложения, которые когда-либо запускались на конечных устройствах.
- **Аппаратура конечных устройств** — содержит информацию об устройствах, подключённых к конечным устройствам.

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

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 syslog

Documentation: ☒
Product: SIEM
Version: 7.x

Журнал syslog отображает события, собранные агентом UserID с серверов syslog. В журнале отображаются события входа пользователей в систему и завершение их сеанса работы. Отображена следующая информация:

Наименование	Описание
Узел	Узел UserGate, на котором зафиксировано событие.
Время	Время произошедшего события.
Запись журнала syslog	Ссылка на событие.
Правило	Правило под которое попало syslog-сообщение.
Критичность	Уровень события syslog.
Объект	Представление процесса, вызвавшего сообщение (kernel messages,user-level messages,security/authentication и тд)
Имя компьютера	Имя компьютера на котором произошло событие.
Приложение	Приложение вызвавшее событие.
Идентификатор процесса	PID процесса вызвавшего событие.
Данные	Описание события.

Журнал защиты почтового трафика

Documentation: ☒
Product: SIEM
Version: 7.x

Журнал защиты почтового трафика отображает события срабатывания правил защиты почтового трафика, в настройках которых включено журналирование. Отображается следующая информация:

- Узел UserGate, на котором произошло событие.
- Время срабатывания.
- Пользователь.
- Отправитель.
- Получатель
- Правило.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Приложение.
- Протокол прикладного уровня.
- Байт отправлено/получено.
- Пакетов отправлено/получено.

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.

Documentation: ☒
Product: SIEM
Version: 7.x

Журнал UserID содержит описание событий отражающие результат работы UserID агента. Отображена следующая информация:

Наименование	Описание
Узел	Узел UserGate, на котором зафиксировано событие
Время	Время произошедшего события
Действие	Действие, примененное к событию
Источник логов	Источник полученного события
Пользователь	Пользователь UG, который вызвал событие
IP-адрес	IP-адрес узла, на котором произошло событие
Информация	Описание события

Журнал RADIUS

Documentation: ☒
Product: SIEM
Version: 7.x

Журнал RADIUS отображает события, собранные агентом UserID из данных RADIUS accounting. В журнале отображаются события входа пользователей в систему и завершение их сеанса работы. Отображена следующая информация:

Наименование	Описание
Узел	Узел UserGate, на котором зафиксировано событие
Время	Время произошедшего события
Идентификатор правила	Идентификатор правила, срабатывание которого создало событие
Пользователь	Пользователь, который вызвал событие
Группы	Строка групп, в которых состоит пользователь
Статус соединения	Текущий статус соединения
IP источника	IP-адрес источника, откуда пришло сообщение
IP адрес NAS	IP-адрес NAS, авторизовавшего пользователя
IP-адрес пользователя	IP-адрес пользователя (framed ip address)

Экспорт журналов

Documentation: ☒
Product: SIEM
Version: 7.x

Функция экспортирования журналов UserGate SIEM позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки.
UserGate SIEM 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.
Параметры разового экспорта	Выбор диапазона экспорта журналов.
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: • 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. 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 систему SIEM для выбора необходимого формата выгрузки журналов. Подробное описание форматов журналов читайте в приложении Описание форматов журналов.
Тип сервера	SSH (SFTP), FTP, syslog.

Наименование	Описание
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 системой SIEM.
Критичность	Только для типа серверов syslog. Необязательное поле, проконсультируйтесь с документацией на используемую 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.
Объект	Только для типа серверов syslog. Необязательное поле, проконсультируйтесь с документацией на используемую 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.

Наименование	Описание
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".

Пользовательская нормализация логов

Documentation: ☒
Product: SIEM
Version: 7.x
Technology: SIEM

Правила нормализации логов позволяют приводить к единому виду данные, полученные UserGate SIEM с различных источников (сенсоров).

Логи, поступающие с различных сенсоров в UserGate SIEM, могут обрабатываться с помощью регулярных выражений, указанных в правилах пользовательской нормализации. В результате данные, найденные в логах, будут записаны в стандартные поля базы данных UserGate SIEM.

Порядок выполнения правил нормализации задается администратором в разделе **Журналы и отчеты → Журналы → Пользовательская нормализация логов**. Последующие правила могут перезаписать значения, нормализованные и записанные предыдущими. Менять расположение правила можно перетаскиванием правила с помощью мыши, или с помощью кнопок меню: **Вниз, Наверх, Выше, Ниже**.

Источники логов и их поля, которые можно дополнительно нормализовать:

Журнал событий конечных устройств	Syslog
Конечное устройство (sensorName)	Правило (ruleName)
Данные (data)	Имя компьютера (computerName)
Статус (status)	Приложение (applicationName)
Источник журнала событий (sourceName)	Идентификатор процесса (processId)
Категория инцидента (logCategoryString)	Данные (data)
Имя компьютера (computerName)	
Пользователь (userName)	
Строка вставки (insertionString)	
Файл журнала лога (logFile)	

Список полей базы данных UserGate SIEM, в которые можно сохранять найденные данные (т.е. использовать эти названия полей в регулярных выражениях в правилах нормализации):

Название	Тип
node	string
userId	guid
user	string
ruleId	guid
rule	string
ipSource	ip
ipDest	ip
portSource	integer16
portDest	integer16

Название	Тип
macSource	mac
macDest	mac
natIpSource	ip
natIpDest	ip
natPortSource	integer16
natPortDest	integer16
applicationName	string
bytesSent	integer64
bytesRecv	integer64
packetsSent	integer64
packetsRecv	integer64
mime	string
httpMethod	string
referer	url
url	url
statusCode	integer16
userAgent	string
sensor	string
sensorId	guid
processId	string
networkProtocol	ip protocol
status	string
error	integer
counterId	guid
logCategory	integer16
taskCategory	string
computerName	string
logEventCode	integer16
logEventId	integer16

Название	Тип
logEventType	integer16
logFile	string
severity	severity
module	string
component	string
event	string
syslogFacility	integer8
syslogSeverity	integer8
image	string
cmdLine	string
originalFileName	string
parentProcessId	integer64
parentImage	string
parentCommandLine	string
targetObject	string
targetFilename	string
scriptBlockText	string
queryName	string
queryResults	string
workstationName	string
logonId	string
imageLoaded	string
sourceImage	string
targetImage	string
customString1	string
...	string
customString15	string
customNumber1	string
...	string

Название	Тип
customNumber5	string
customIp1	ip
customIp2	ip
customDate1	date
customDate2	date

Типы полей:

Тип	Значение по умолчанию	Описание
string	""	Строка любой длины.
guid	00000000-0000-0000-0000-000000000000	Строка вида XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX, где X - шестнадцатичная цифра (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f, A, B, C, D, E, F).
ip	0.0.0.0	Строка вида X.X.X.X, где X = 0..255; или X:X:X:X:X:X, где X = 4-значное шестнадцатичное число.
integer	0	Любое целое неотрицательное число.
url	""	Строка URL, формат в RFC1738.
ip protocol	255	Число 0 .. 255 или строка из списка протоколов ниже.
severity	unknown	Строки: unknown, critical, error, info, warning.
integer8	0	Целое число в интервале [0, 255].
integer16	0	Целое число в интервале [0, 65535].
integer64	0	Целое число в интервале [0, 2^64-1].
date	1970-01-01T00:00:00	2024-03-06T10:30:00.

Список протоколов, допустимых для поля networkProtocol (буквы могут быть в любом регистре):

Название	Значение
IP	0
ICMP	1
IGMP	2
GGP	3
IP-ENCAP	4
ST	5
TCP	6
CBT	7
EGP	8

Название	Значение
IGP	9
BBN-RCC-MON	10
NVP-II	11
PUP	12
ARGUS	13
EMCON	14
XNET	15
CHAOS	16
UDP	17
MUX	18
DCN-MEAS	19
HMP	20
PRM	21
XNS-IDP	22
TRUNK-1	23
TRUNK-2	24
LEAF-1	25
LEAF-2	26
RDP	27
IRTP	28
ISO-TP4	29
NETBLT	30
MFE-NSP	31
MERIT-INP	32
DCCP	33
3PC	34
IDPR	35
XTP	36
DDP	37

Название	Значение
IDPR-CMTP	38
TP++	39
IL	40
IPV6	41
SDRP	42
IPV6-ROUTE	43
IPV6-FRAG	44
IDRP	45
RSVP	46
GRE	47
DSR	48
BNA	49
IPSEC-ESP	50
IPSEC-AH	51
I-NLSP	52
SWIPE	53
NARP	54
MOBILE	55
TLSP	56
SKIP	57
IPV6-ICMP	58
IPV6-NONXT	59
IPV6-OPTS	60
ANY HOST INTERNAL PROTOCOL	61
CFTP	62
ANY LOCAL NETWORK	63
SAT-EXPAK	64
KRYPTOLAN	65
RVD	66

Название	Значение
IPPC	67
ANY DISTRIBUTED FILE SYSTEM	68
SAT-MON	69
VISA	70
IPCU	71
CPNX	72
CPHB	73
WSN	74
PVP	75
BR-SAT-MON	76
SUN-ND	77
WB-MON	78
WB-EXPAK	79
ISO-IP	80
VMTP	81
SECURE-VMTP	82
VINES	83
IPTM	84
NSFNET-IGP	85
DGP	86
TCF	87
EIGRP	88
OSPFIGP	89
SPRITE-RPC	90
LARP	91
MTP	92
AX.25	93
IPIP	94
MICP	95

Название	Значение
SCC-SP	96
ETHERIP	97
ENCAP	98
ANY PRIVATE ENCRYPTION SCHEME	99
GMTP	100
IFMP	101
PNNI	102
PIM	103
ARIS	104
SCPS	105
QNX	106
A/N	107
IPCOMP	108
SNP	109
COMPAQ-PEER	110
IPX-IN-IP	111
VRRP	112
PGM	113
ANY 0-HOP PROTOCOL	114
L2TP	115
DDX	116
IATP	117
STP	118
SRP	119
UTI	120
SMP	121
SM	122
PTP	123
IS-IS OVER IPV4	124

Название	Значение
FIRE	125
CRTP	126
CRUDP	127
SSCOPMCE	128
IPLT	129
SPS	130
PIPE	131
SCTP	132
FC	133
RSVP-E2E-IGNORE	134
MOBILITY HEADER	135
UDPLITE	136
MPLS-IN-IP	137
MANET	138
HIP	139
SHIM6	140
WESP	141
ROHC	142
USE FOR EXPERIMENTATION AND TESTING	254
RESERVED	255

Для создания правила нормализации необходимо в разделе **Журналы и отчеты → Журналы → Пользовательская нормализация логов** нажать **Добавить** и в открывшемся окне заполнить следующие поля:

Наименование	Описание
Включено	Включение/выключение правила пользовательской нормализации логов.
Название	Название правила пользовательской нормализации логов.
Описание	Описание правила пользовательской нормализации логов.
Категория	Выбор категории (типа) логов, для которых применяется данное правило: - Журнал событий конечных устройств; - Syslog.
Столбец с данными	Выбор столбца, из которого будут извлекаться данные.
Регулярное выражение	Строка регулярного выражения с группами, названия которых совпадают со столбцами, куда будут записываться значения.

Пример создания правила, которое обрабатывает логи категории syslog, извлекает из них имя пользователя, ip, port и записывает их в соответствующие поля базы данных UserGate SIEM:

Свойства правила пользовательской нормализации логов

Включено:

☒

Название:

Syslog1

Описание:

Категория:

Syslog

Столбец с данными:

Данные

Регулярное выражение:

.+Accepted.+for\s(?<user>[A-Za-z0-9]+)\sfrom\s(?<ipSource>[0-9.]+)\sport\s(?<portSource>[0-9]+)

Сохранить

Отмена

Правила пользовательской нормализации могут быть экспортированы в бинарный файл, или импортированы в систему с помощью кнопок **Экспорт/Импорт** в меню инструментов раздела **Журналы и отчеты** → **Журналы** → **Пользовательская нормализация логов** (доступно в версии ПО 7.4.0 и выше):

В UserGate SIEM имеется встроенная библиотека правил нормализации логов, которая содержит созданные разработчиками UserGate референсные правила нормализации. Правила из библиотеки могут быть импортированы в раздел пользовательской нормализации логов и использованы для создания собственных правил. Подробнее о библиотеке правил — в разделе [Правила нормализации логов](#).

Поиск и фильтрация данных

Documentation: ☒

Product: SIEM

Version: 7.x

Количество записей, регистрируемых в журналах, как правило, очень велико, и UserGate SIEM 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. Подробнее — в приложении [«Синтаксис языка запросов»](#).

Documentation: ☒
Product: SIEM
Version: 7.x

Формат журнала событий

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	events
	Origin	Модуль, в котором произошло событие.	admin_console
	Severity	Важность события.	Может принимать значения: 1 — информационные. 4 — предупреждения. 7 — ошибки. 10 — критичные.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Тип события.	login_successful
	suser	Имя пользователя.	Admin
	src	IPv4-адрес источника.	192.168.117.254
	cat	Компонент, в котором произошло событие.	console_auth
	cs1Label	Поле используется для указания деталей события.	Attributes
	cs1	Детали события в формате JSON.	{"name":"MIME_BUILTIN_COMPOSITE","module":"nlist_import"}

Формат журнала веб-доступа

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	webaccess
	Name	Тип источника.	log

Тип поля	Название поля	Описание	Пример значения
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknwn, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта.	{"id":39,"name":"Social Networking","threat_level":3}
	proto	Используемый протокол 4-го уровня.	TCP.
	app	Протокол прикладного уровня и его версия.	HTTP/1.1
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP).	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Default Allow
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone

Тип поля	Название поля	Описание	Пример значения
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле указывает было ли содержимое расшифровано.	Decrypted
	cs6	Расшифровано или нет.	true, false
	flexString1Label	Поле указывает на тип контента.	Media type
	flexString1	Тип контента.	text/html
	flexString2Label	Поле указывает на категорию запрашиваемого URL-адреса.	URL Categories
	flexString2	Категория URL.	Computers & Technology
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение.	3
	cn2Label	Поле используется для указания количества переданных пакетов в направлении назначение — источник.	Packets received
	cn2	Количество переданных пакетов в направлении назначение — источник.	1
	cn3Label	Поле указывает исходный ответ сервера.	Response
	cn3	Код ответа HTTP.	302

Формат журнала веб-доступа **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	webaccess
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknowн, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica

Тип поля	Название поля	Описание	Пример значения
	act	Действие, принятое устройством в соответствии с настроенными политиками.	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта.	{"id":39,"name":"Social Networking","threat_level":3}
	proto	Используемый протокол 4-го уровня.	TCP.
	app	Протокол прикладного уровня и его версия.	HTTP/1.1
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP).	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Default Allow
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted
	flexString1Label	Поле указывает на категорию запрашиваемого URL-адреса.	URLCats
	flexString1	Категория URL.	Computers & Technology
	cn1Label	Поле указывает исходный ответ сервера.	Response
	cn1	Код ответа HTTP.	302

ПримечаниеОбщее правило для компактного формата — значения некоторых полей обрезаются по длине до 80 символов. Например, список url-категорий, url, имя пользователя, имя правила, имя зоны, и т.д.

Формат журнала DNS

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	dns
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
	act	Действие, принятое устройством в соответствии с настроенными политиками.	block
	reason	Причина, по которой было создано событие, например, url категория, на которых сработало правило.	{"url_cats":{"id":37,"name":"Search Engines & Portals","threat_level":1}}
	proto	Используемый протокол 4-го уровня.	UDP
	dhost	Имя хоста назначения, адрес которого определяется с помощью DNS сервера.	google.com
	app	Протокол прикладного уровня.	DNS
	suser	Имя пользователя.	user1 (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.0.11
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535. Для DNS обычно используется порт 53.
	cs1Label	Поле используется для указания сработавшего правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Rule1
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)

Тип поля	Название поля	Описание	Пример значения
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле используется для указания передаваемых данных.	Data
	cs6	Передаваемые данные.	{"question":{"domain":"google.com","type":"A","class":"IN"}, "answer": [{"domain":"google.com","type":"TXT","class":"IN","ttl":5,"data":"Blocked"}, {"domain":"google.com","type":"A","class":"IN","ttl":5,"data":"10.10.0.1"}]}
	flexString1Label	Поле указывает на категорию запрашиваемого URL-адреса.	URL Categories
	flexString1	Категория URL.	Search Engines & Portals

Формат журнала DNS CEF Compact :

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	dns
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
	act	Действие, принятое устройством в соответствии с настроенными политиками.	block
	reason	Причина, по которой было создано событие, например, url категория, на которых сработало правило.	{"url_cats":{"id":37,"name":"Search Engines & Portals","threat_level":1}}
	proto	Используемый протокол 4-го уровня.	UDP
	dhost	Имя хоста назначения, адрес которого определяется с помощью DNS сервера.	google.com
	app	Протокол прикладного уровня.	DNS

Тип поля	Название поля	Описание	Пример значения
	suser	Имя пользователя.	user1 (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.0.11
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535. Для DNS обычно используется порт 53.
	cs1Label	Поле используется для указания сработавшего правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Rule1
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted
	cs4Label	Поле используется для указания передаваемых данных.	Data
	cs4	Передаваемые данные.	{"question":[{"domain":"google.com","type":"A","class":"IN"}], "answer": [{"domain":"google.com","type":"TXT","class":"IN","ttl":5,"data":"Blocked"}, {"domain":"google.com","type":"A","class":"IN","ttl":5,"data":"10.10.0.1"}]}
	flexString1Label	Поле указывает на категорию запрашиваемого URL-адреса.	URLCats
	flexString1	Категория URL.	Search Engines & Portals

Формат журнала трафика

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие.	firewall
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.

Тип поля	Название поля	Описание	Пример значения
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Имя сработавшего приложения	my_app
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	00:50:56:80:28:08
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	dmac	MAC-адрес назначения.	00:50:56:80:7D:21
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT).	192.168.174.134 (0.0.0.0 — если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если настроены правила NAT).	192.226.127.130 (0.0.0.0 — если нет)
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)

Тип поля	Название поля	Описание	Пример значения
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение.	3
	cn2Label	Поле используется для указания количества пакетов, переданных в направлении назначение — источник.	Packets received
	cn2	Количество пакетов, переданных в направлении назначение — источник.	1

Формат журнала трафика **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие.	firewall
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unklown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Имя сработавшего приложения	my_app
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.

Тип поля	Название поля	Описание	Пример значения
	smac	MAC-адрес источника.	00:50:56:80:28:08
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	dmac	MAC-адрес назначения.	00:50:56:80:7D:21
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	sourceTranslatedAddress	Адрес источника после переназначения (если настроены правила NAT).	192.168.174.134 (0.0.0.0 — если нет)
	sourceTranslatedPort	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	destinationTranslatedAddress	Адрес назначения после переназначения (если настроены правила NAT).	192.226.127.130 (0.0.0.0 — если нет)
	destinationTranslatedPort	Порт назначения после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (0 — если нет)
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted

Формат журнала COB

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	idps
	Signature	Название сработавшей сигнатуры COB.	BlackSun Test
	Threat Level	Уровень угрозы сигнатуры.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unkown, если категория не определена.

Тип поля	Название поля	Описание	Пример значения
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Протокол прикладного уровня.	HTTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	msg	Уровень угрозы сигнатуры и её название.	[2] BlackSun
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	IDPS Rule Example
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)

Формат журнала COB CEF Compact:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate

Тип поля	Название поля	Описание	Пример значения
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	idps
	Signature	Название сработавшей сигнатуры COB.	BlackSun Test
	Threat Level	Уровень угрозы сигнатуры.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	app	Протокол прикладного уровня.	HTTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	msg	Уровень угрозы сигнатуры и её название.	[2] BlackSun
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	IDPS Rule Example

Формат журнала АСУ ТП

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	scada

Тип поля	Название поля	Описание	Пример значения
	Name	Тип источника.	log
	PDU Severity	Критичность АСУ ТП.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	app	Протокол прикладного уровня.	Modbus
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Scada Rule Example
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле указывает на информацию об устройстве.	PDU Details
	cs6	Информация об устройстве в формате JSON.	<pre>{ "protocol": "modbus", "pdu_severity": 0, "pdu_func": "3", "pdu_address": 0, "mb_value": 0, "mb_quantity": 0, "mb_payload": "AAIAAA==", "mb_message": "response", "mb_addr": 0 }</pre>

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	ssh
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unkown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	app	Протокол прикладного уровня.	SSH или SFTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	SSH inspection rule
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country

Тип поля	Название поля	Описание	Пример значения
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Указание на команду, передаваемую по SSH.	Command
	cs6	Команда, передаваемая по SSH, в формате JSON.	whoami

Формат журнала инспектирования SSH
 CEF Compact:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	ssh
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unklown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	app	Протокол прикладного уровня.	SSH или SFTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	smac	MAC-адрес источника.	FA:16:3E:65:1C:B4
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	SSH inspection rule
	cs2Label	Поле используется для индикации зоны источника.	SrcZone
	cs2	Название зоны источника.	Trusted

Тип поля	Название поля	Описание	Пример значения
	cs3Label	Поле используется для индикации зоны назначения.	DstZone
	cs3	Название зоны назначения.	Untrusted
	cs4Label	Указание на команду, передаваемую по SSH.	Command
	cs4	Команда, передаваемая по SSH, в формате JSON.	whoami

Формат журнала защиты почтового трафика

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	mailsecurity
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@einsonstal
	act	Действие, выполненное устройством в соответствии с настроенными политиками.	mark
	app	Протокол прикладного уровня.	SMTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4-адрес источника.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4-адрес назначения.	10.10.10.10
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	10
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	10
	cs1Label	Поле используется для указания названия правила.	Rule
	cs1	Название правила защиты почтового трафика.	Mail security rule
	cs2Label	Поле используется для указания зоны источника.	Source Zone

Тип поля	Название поля	Описание	Пример значения
	cs2	Зона источника.	Untrusted
	cs3Label	Поле используется для индикации страны источника трафика.	Source Country
	cs3	Страна источника трафика.	RU (отображается двухбуквенный код страны)
	cs4Label	Поле используется для указания зоны назначения трафика.	Destination Zone
	cs4	Название зоны назначения трафика.	Untrusted
	cs5Label	Поле используется для индикации страны назначения трафика.	Destination Country
	cs5	Страна назначения.	RU (отображается двухбуквенный код страны)
	cs6Label	Поле используется для указания почтового адреса получателя.	To
	cs6	Email получателя.	receiver@example.com
	flexString1Label	Поле используется для указания почтового адреса отправителя.	From
	flexString1	Email отправителя.	sender@example.com
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение.	3
	cn2Label	Поле используется для указания количества переданных пакетов в направлении назначение — источник.	Packets received
	cn2	Количество переданных пакетов в направлении назначение — источник.	1

Формат журнала защиты почтового трафика **CEF Compact**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	mailsecurity
	Name	Тип источника.	log
	Threat Level	Уровень угрозы приложения.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unkown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822

Тип поля	Название поля	Описание	Пример значения
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@einsonstal
	act	Действие, выполненное устройством в соответствии с настроенными политиками.	mark
	app	Протокол прикладного уровня.	SMTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	src	IPv4-адрес источника.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4-адрес назначения.	10.10.10.10
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	10
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	10
	cs1Label	Поле используется для указания названия правила.	Rule
	cs1	Название правила защиты почтового трафика.	Mail security rule
	cs2Label	Поле используется для указания зоны источника.	SrcZone
	cs2	Зона источника.	Untrusted
	cs4Label	Поле используется для указания зоны назначения трафика.	DstZone
	cs4	Название зоны назначения трафика.	Untrusted
	cs5Label	Поле используется для указания почтового адреса отправителя.	From
	cs5	Email отправителя.	sender@example.com
	cs6Label	Поле используется для указания почтового адреса получателя.	To
	cs6	Email получателя.	receiver@example.com

Формат журнала событий конечных устройств

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_log

Тип поля	Название поля	Описание	Пример значения
	Name	Тип источника.	log
	Severity	Важность события.	Может принимать значения: 1 — error; 2 — warning; 3 — info; 4 — audit success; 5 — audit failure.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	msg	Подробная информация о событии.	Состояние Windows Defender успешно изменено на SECURITY_PRODUCT_STATE_ON.
	suser	Имя пользователя.	Admin
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId
	cs1	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Поле используется для индикации имени конечного устройства или сенсора.	endpointName
	cs2	Имя конечного устройства или сенсора.	DESKTOP-0731Nfq
	cs3Label	Поле используется для указания на тип события.	logLevel
	cs3	Тип события.	Аудит успеха, Предупреждение, Сведения, Аудит отказа, Ошибка
	cs4Label	Поле используется для указания категории события.	logCategoryString
	cs4	Категория события.	Special Logon
	cs5Label	Поле используется для индикации типа журнала.	logFile
	cs5	Тип журнала, содержащего важную информацию о программных и аппаратных событиях.	Security (файл журнала безопасности), Application (файл журнала приложений), System (файл системного журнала), Windows PowerShell
	cs6Label	Поле используется для указания на источник журнала событий.	sourceName
	cs6	Источник журнала событий.	Microsoft-Windows-Security-Auditing
	cn1Label	Поле используется для индикации кода события журнала.	logEventCode
	cn1	Код события журнала.	1154
	cn2Label	Поле используется для указания на идентификатор события.	logEventId
	cn2	Идентификатор события.	10016

Тип поля	Название поля	Описание	Пример значения
	cn3Label	Поле используется для индикации типа события логa.	logEventType
	cn3	Тип события логa.	1 (error), 2 (warning), 3 (information), 4 (audit success), 5 (audit failure).
	flexString1Label	Поле используется для индикации строки вставки.	insertionString
	flexString1	Строка вставки - данные блока eventData события Windows.	Windows DefenderSECURITY_PRODUCT_STATE_ON

Формат журнала правил конечных устройств

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_log
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknwn, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP
	shost	Имя хоста.	www.google.com
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	filePath	Приложение, к которому было применено правило межсетевого экрана.	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId
	cs1	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Поле используется для указания на имя NetBIOS конечного устройства.	endpointName

Тип поля	Название поля	Описание	Пример значения
	cs2	Имя NetBIOS конечного устройства.	DESKTOP-0731NFQ
	cs3Label	Поле используется для указания правила, срабатывание которого создало запись в журнале.	Rule
	cs3	Название правила.	Test rule name
	flexString1Label	Поле указывает на тип контента.	Media type
	flexString1	Тип контента.	text/html
	flexString2Label	Поле указывает на категорию запрашиваемого URL-адреса.	Categories
	flexString2	Категория URL.	Computers & Technology

Формат журнала правил конечных устройств **CEF Format**:

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_log
	Name	Тип источника.	log
	Threat Level	Уровень угрозы категории URL.	Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	proto	Используемый протокол 4-го уровня.	TCP
	shost	Имя хоста.	www.google.com
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	filePath	Приложение, к которому было применено правило межсетевое экрана.	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Тип поля	Название поля	Описание	Пример значения
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId
	cs1	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Поле используется для указания на имя NetBIOS конечного устройства.	endpointName
	cs2	Имя NetBIOS конечного устройства.	DESKTOP-0731NFQ
	cs3Label	Поле используется для указания правила, срабатывание которого создало запись в журнале.	Rule
	cs3	Название правила.	Test rule name

Формат журнала приложений конечных устройств

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_applications
	Name	Тип источника.	log
	Threat Level	Значение по умолчанию.	0
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Действие (запуск или остановка приложения).	start, stop
	suser	Пользователь.	DESKTOP-0731NFQ\User
	filePath	Расположение файла.	C:\Windows\system32\cmd.exe
	spid	Идентификатор процесса.	3860
	fileHash	Хэш приложения.	B4979A9F970029889713D756C3F123643DDE73DA
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId
	cs1	Идентификатор конечного устройства.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Поле используется для указания на имя NetBIOS конечного устройства.	endpointName
	cs2	Имя NetBIOS конечного устройства.	DESKTOP-0731NFQ
	cs3Label	Поле используется для индикации командной строки.	cmdLine

Тип поля	Название поля	Описание	Пример значения
	cs3	Запрос командной строки.	C:\Windows\system32\sc.exe start w32time task_started
	cs4Label	Поле используется для указания идентификатора сессии.	sessionId
	cs4	Идентификатор сессии.	1656395717

Формат журнала аппаратуры конечных устройств

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	endpoint_hardware
	Name	Тип источника.	log
	Threat Level	Значение по умолчанию.	0
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Идентификатор устройства, сгенерировавшего это событие.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	act	Действие (подключение или извлечение устройства).	add_device, remove_device
	sourceServiceName	Драйвер Windows, обеспечивающий взаимодействие компьютера с оборудованием/устройством.	USBHUB3
	cs1Label	Поле используется для указания идентификатора конечного устройства.	endpointId
	cs1	Идентификатор конечного устройства.	35fb5820-74db-4eac-b05b-d01bc284c4e8
	cs2Label	Поле используется для указания на имя NetBIOS конечного устройства.	endpointName
	cs2	Имя NetBIOS конечного устройства.	DESKTOP-0731NFQ
	cs3Label	Поле используется для указания идентификатора подключаемого/извлекаемого устройства.	deviceId
	cs3	Идентификатор устройства.	USB\VID_0E0F&PID_0002\6&201153C1&0&8
	cs4Label	Поле используется для индикации имени устройства.	deviceName
	cs4	Название устройства.	Kingston DataTraveler 2.0 USB Device

Формат журнала syslog

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate

Тип поля	Название поля	Описание	Пример значения
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	syslog
	Name	Тип источника.	log
	Threat Level	Уровень угрозы.	Может принимать значения: • 0 — emergencies; • 1 — alerts; • 2 — critical; • 3 — errors; • 4 — warnings; • 5 — notifications; • 6 — informational; • 7 — debugging.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
	msg	Описание события.	[3603:3603:1128/175000.938565:ERROR:CONSOLE(6)] "console.assert", source: devtools://devtools/bundled/devtools-frontend/front_end/panels/console/console.js (6)
	cn1Label	Поле используется для указания типа источника событий syslog. Подробнее о значениях syslog facility смотрите в RFC 5424 .	Facility
	cn1	Тип источника событий syslog. Например, user-level messages.	1
	cs1Label	Поле используется для указания имени устройства, на котором произошло событие.	Hostname
	cs1	Имя компьютера, на котором произошло событие.	node1
	cs2Label	Поле используется для указания приложения, вызвавшего событие.	Tag
	cs2	Приложение, вызвавшее событие.	org.gnome.Shell.desktop
	cs3Label	Поле используется для указания идентификатора процесса события.	ProcessID
	cs3	PID процесса вызвавшего событие.	3036
	cs4Label	Поле используется для указания срабатывания правила.	Rule
	cs4	Название правила, срабатывание которого вызвало событие.	Example — Allow user-level messages

Формат журнала RADIUS

Тип поля	Название поля	Описание	Пример значения

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	radius
	Name	Тип источника.	log
	Threat Level	Уровень угрозы.	Может принимать значения: • 0 — emergencies; • 1 — alerts; • 2 — critical; • 3 — errors; • 4 — warnings; • 5 — notifications; • 6 — informational; • 7 — debugging.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
	act	Статус пользователя (acct_status_type).	start, stop, interim update, accounting-on, accounting-off
	suser	Имя пользователя.	Unknown, если ползователь неизвестен.
	src_ip	IP-адрес источника, откуда пришло сообщение.	192.168.57.4
	dst	IP-адрес NAS, авторизовавшего пользователя.	172.16.1.4
	dvc	IP-адрес пользователя (framed ip address).	192.168.57.29
	cs1Label	Поле используется для указания группы, в которой состоит пользователь.	user groups
	cs1	Строка групп в которых состоит пользователь.	test_group

Формат журнала UserID

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	userid
	Name	Тип источника.	log

Тип поля	Название поля	Описание	Пример значения
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1701085036026
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
	act	Действие, принятое устройством в соответствии с настроенными политиками.	login
	reason	Причина, по которой было создано событие.	{ "user_groups_sids":["S-1-5-21-3795870133-5220325-2125745684-513","S-1-5-21-3795870133-5220325-2125745684-512"], "user_sid":"S-1-5-21-3795870133-5220325-2125745684-1103", "login":"user1","domain":"DEV","event_id":4624}
	suser	Имя пользователя.	user1 (Unknown, если пользователь неизвестен)
	src	IPv4 источника трафика.	10.10.0.11
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	dev.local

Documentation: ☒
Product: SIEM
Version: 7.x

Описание журнала событий

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
ip_address	IPv4-адрес источника события.	192.168.174.134
attributes	Детали события в формате JSON.	{"rule":{"logrotate":12,"attributes":{"timezone":"Asia/Novosibirsk"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"}
event_type	Тип события.	logexport_rule_updated
event_severity	Важность события.	info (информационные), warning (предупреждения), error (ошибки), critical (критичные).
event_origin	Модуль, в котором произошло событие.	core
event_component	Компонент, в котором произошло событие.	console_auth
user	Имя пользователя.	{"guid":"37333739-3733-3734-3635-366400000000","name":"System","groups":[]}}

Описание журнала веб-доступа

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session	Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
reasons	Причина, по которой было создано событие, например, причина блокировки сайта.	"url_cats":[{"id":39,"name":"Social Networking","threat_level":3}]
proto	Используемый протокол 4-го уровня.	TCP
host	Имя хоста.	www.google.com
action	Действие, принятое устройством в соответствии с настроенными политиками.	block
bytes_sent	Количество байтов, переданных в направлении источник — назначение.	52
bytes_rcv	Количество пакетов, переданных в направлении назначение — источник.	100
packets_sent	Количество пакетов, переданных в направлении источник — назначение.	2

Название поля			Описание	Пример значения
packets_recv			Количество байтов, переданных в направлении назначение — источник.	5
request_method			Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET
url			Поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
media_type			Тип контента.	application/json
status_code			Код ответа HTTP.	302
http_referer			URL источника запроса (реферер HTTP).	https://www.google.com/
decrypted			Поле указывает было ли содержимое расшифровано.	true, false
useragent			Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
application	id		Идентификатор приложения.	20
	name		Название приложения.	Youtube
	threat_level		Уровень угрозы приложения.	0
	app_protocol		Протокол прикладного уровня и его версия.	HTTP/1.1"
url_categories	id		Идентификатор категории, к которой относится URL.	39
	threat_level		Уровень угрозы категории URL.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
	name		Название категории, к которой относится URL.	Social Networking
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника.	Trusted
	country		Страна источника трафика.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника	01:23:45:67:89:AB
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Страна назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения.	192.168.174.134

Название поля		Описание	Пример значения
	port	Порт назначения.	Может принимать значения от 0 до 65535.
	mac	MAC-адрес назначения.	01:23:45:67:89:AB
rule	guid	Уникальный идентификатор правила, срабатывание которого вызвало создание события.	f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
	name	Название правила.	Default allow
	type	Тип сработавшего правила.	
user	guid	Уникальный идентификатор пользователя.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name	Имя пользователя	user_name
	groups	guid	Уникальный идентификатор группы, в которой состоит пользователь.
		name	Название группы, в которой состоит пользователь.

Описание журнала DNS

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: уууу-мм-ддThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session		Идентификатор сессии.	00000000-0000-0000-0000-000000000000
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
reasons		Причина, по которой было создано событие, например, url категория, на которых сработало правило.	{"url_cats":[{"id":37,"name":"Search Engines & Portals","threat_level":1}]}
proto		Используемый протокол 4-го уровня.	UDP
host		Имя хоста.	google.com
data		Поле используется для указания передаваемых данных.	{"question":[{"domain":"google.com","type":"A","class":"IN"}], "answer":[{"domain":"google.com","type":"TXT","class":"IN","ttl":5,"data":"Blocked"}, {"domain":"google.com","type":"A","class":"IN","ttl":5,"data":"10.10.0.1"}]}
url_categories	id	Идентификатор сработавшей URL-категории.	37
	threat_level	Уровень угрозы сработавшей категории.	Может принимать значения: 1 — очень низкий. 2 — низкий. 3 — средний. 4 — высокий. 5 — очень высокий.
	name	Название сработавшей категории.	Search Engines & Portals
action		Действие, принятое устройством в соответствии с настроенными политиками.	block
application	id	Идентификатор приложения.	5

Название поля		Описание		Пример значения
		name	Название приложения.	
		threat_level	Уровень угрозы приложения.	0
		app_protocol	Протокол прикладного уровня.	DNS
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	01:23:45:67:89:AB
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535. Для DNS обычно используется порт 53.
	mac		MAC-адрес назначения	01:23:45:67:89:AB
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	Rule1
	Type		Тип сработавшего правила.	
user	guid		Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	user1
	groups	guid	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала трафика

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session	Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)

Название поля			Описание	Пример значения
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
proto			Используемый протокол 4-го уровня.	TCP или UDP
action			Действие, принятое устройством в соответствии с настроенными политиками.	accept
bytes_sent			Количество байтов, переданных в направлении источник — назначение.	100
bytes_recv			Количество байтов, переданных в направлении назначение — источник.	6
packets_recv			Количество пакетов, переданных в направлении назначение — источник.	1
packets_sent			Количество пакетов, переданных в направлении источник — назначение.	1
json_data			Дополнительные данные.	null
application	id		Идентификатор приложения.	195
	threat_level		Уровень угрозы приложения.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
	app_protocol		Протокол прикладного уровня.	HTTP
	name		Название приложения.	Youtube
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535.
nat	source	ip	Адрес источника после переназначения (если настроены правила NAT).	192.168.117.85 (если NAT не настроен, то: "nat":null)
		port	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (если NAT не настроен, то: "nat":null)

Название поля			Описание	Пример значения
	destination	ip	Адрес назначения после переназначения (если настроены правила NAT).	64.233.164.198 (если NAT не настроен, то: "nat":null)
		port	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (если NAT не настроен, то: "nat":null)
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	type		Тип правила.	firewall
	name		Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
user	guid		Уникальный идентификатор пользователя. Если пользователь типа Unkown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	Admin
	groups	guid	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала COB

Название поля			Описание	Пример значения
timestamp			Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session			Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
proto			Используемый протокол 4-го уровня.	TCP или UDP
action			Действие, принятое устройством в соответствии с настроенными политиками.	accept
bytes_sent			Количество байтов, переданных в направлении источник — назначение.	100
bytes_recv			Количество байтов, переданных в направлении назначение — источник.	6
packets_sent			Количество пакетов, переданных в направлении источник — назначение.	1
packets_recv			Количество пакетов, переданных в направлении назначение — источник.	1
json_data			Дополнительные данные.	null
application	id		Идентификатор приложения.	195
	threat_level		Уровень угрозы приложения.	Может принимать значения: 1 — очень низкий. 2 — низкий. 3 — средний. 4 — высокий. 5 — очень высокий.
	name		Название приложения.	Youtube

Название поля		Описание	Пример значения
	app_protocol	Протокол прикладного уровня.	HTTP
user	guid	Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name	Имя пользователя.	Admin
	groups	guid	Уникальный идентификатор группы, в которых состоит пользователь.
		name	Название группы, в которой состоит пользователь.
rule	guid	Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name	Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
	type	Тип сработавшего правила	idps
signatures	id	Идентификатор сработавшей сигнатуры.	999999
	threat_level	Уровень угрозы сработавшей сигнатуры.	Может принимать значения: 1 — очень низкий. 2 — низкий. 3 — средний. 4 — высокий. 5 — очень высокий.
	name	Название сработавшей сигнатуры.	BlackSun Test
source	zone	guid	Уникальный идентификатор зоны источника трафика.
		name	Название зоны источника трафика.
	country	Название страны источника.	RU (отображается двухбуквенный код страны)
	ip	IPv4-адрес источника трафика.	10.10.10.10
	port	Порт источника.	Может принимать значения от 0 до 65535.
	mac	MAC-адрес источника.	01:23:45:67:89:AB
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.
		name	Название зоны назначения трафика.
	country	Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip	IPv4-адрес назначения трафика.	104.19.197.151
	port	Порт назначения.	Может принимать значения от 0 до 65535.
	mac	MAC-адрес назначения.	01:23:45:67:89:AB

Описание журнала АСУ ТП

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z

Название поля			Описание	Пример значения
pdu_severity			Критичность АСУ ТП.	1
pdu_func			Код функции (говорит ведомому устройству, какие данные или выполнение какого действия требует от него ведущее устройство).	12
pdu_address			Адрес регистра, с которым необходимо провести операцию.	3154
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
details	pdu_varname		Имя переменной. Параметр, в основном, используется для обмена данными в режиме реального времени. Параметр относится к протоколу MMS.	VAR
	pdu_device		Адрес устройства, используемый в протоколах MMS и OPCUA.	DEV
	mb_write_quantity		Количество значений для записи (команда Read Write Register).	998
	mb_write_addr		Начальный адрес регистра для записи (команда Read Write Register).	776
	mb_value		Записываемое значение (для команд Write Single Coil, Write Single Register).	322
	mb_unit_id		Адрес устройства.	186
	mb_read_quantity		Количество значений для чтения (команда Read Write Register).	658
	mb_read_addr		Начальный адрес регистра для чтения (команда Read Write Register).	122
	mb_quantity		Количество значений для чтения.	875
	mb_payload		Значения регистров (для команд Read Coil, Read Holding Registers, Read Input Registers, Read/Write Multiple registers, Write Multiple Coil).	75be5ecdc24f9883
	mb_or_mask		Значение маски OR команды Mask Write Register.	1024
	mb_message		Сообщение Modbus.	exception
	mb_exception_code		Код ошибки. Актуален для типа сообщения error_response.	255
	mb_and_mask		Значение маски AND команды Mask Write Register.	121
	mb_addr		Адрес регистра.	3154
	iec104_msgtype		Тип запроса.	request, response, error_response
	iec104_ioa		Адрес объекта информации, который позволяет однозначно идентифицировать приёмной стороной тип события.	23
	iec104_cot		Причина передачи протокольного блока данных прикладного уровня (Application Protocol Data Unit, APDU).	6
	iec104_asdu		Адрес ASDU (COA — Common Object Address). Параметр относится к протоколу IEC-104.	123
app_protocol			Протокол прикладного уровня.	Modbus
action			Действие, принятое устройством в соответствии с настроенными политиками.	pass
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted

Название поля			Описание	Пример значения
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535.
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	SCADA Sample Rule

Описание журнала инспектирования SSH

Название поля			Описание	Пример значения
timestamp			Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
command			Команда, передаваемая по SSH.	whoami
action			Действие, принятое устройством в соответствии с настроенными политиками.	block
application		id	Идентификатор приложения.	195
		name	Название приложения.	
		threat_level	Уровень угрозы приложения.	Может принимать значения от 2 до 10 (установленный уровень угрозы приложения, умноженный на 2).
		app_protocol	Протокол прикладного уровня.	SSH или SFTP
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	FA:16:3E:65:1C:B4

Название поля			Описание	Пример значения
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес назначения.	01:23:45:67:89:AB
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	SSH Rule Example
	type		Тип сработавшего правила.	ssh
user	guid		Уникальный идентификатор пользователя. Если пользователь типа Unkown, то идентификатор: 00000000-0000-0000-0000-000000000000.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	Admin
	groups	guid	Уникальный идентификатор группы, в которых состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала защиты почтового трафика

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
action		Действие, принятое устройством в соответствии с настроенными политиками.	mark
bytes_sent		Количество байтов, переданных в направлении источник — назначение.	0
bytes_rcv		Количество байтов, переданных в направлении назначение — источник.	0
packets_sent		Количество пакетов, переданных в направлении источник — назначение.	0
packets_rcv		Количество пакетов, переданных в направлении назначение — источник.	0
decrypted		Поле указывает было ли содержимое расшифровано.	true, false
from		Почтовый адрес отправителя.	sender@example.com
to		Почтовый адрес получателя.	receiver@example.com
application	id	Идентификатор приложения.	9

Название поля		Описание		Пример значения
		name	Название приложения.	
		threat_level	Уровень угрозы приложения.	Может принимать значения от 2 до 10 (установленный уровень угрозы приложения, умноженный на 2).
		app_protocol	Сетевой протокол прикладного уровня.	SMTP
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
	mac		MAC-адрес источника.	01:23:45:67:89:AB
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	10.10.10.10
	port		Порт назначения.	Может принимать значения от 0 до 65535.
	port		MAC-адрес назначения.	01:23:45:67:89:AB
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	Mail security rule
	type		Тип сработавшего правила.	Mail security rule
user	guid		Уникальный идентификатор пользователя.	a7a3cd49-8232-4f1a-962a-3659af89e96f
	name		Имя пользователя.	user_name
	groups	guid	Уникальный идентификатор группы, в которой состоит пользователь.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

Описание журнала событий конечных устройств

Название поля	Описание	Пример значения
user_name	Имя пользователя.	DESKTOP-0731NFQ\Username
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
status	Результат выполнения WMI или SNMP запроса.	OK, Error
source_name	Источник журнала событий.	Microsoft-Windows-Security-Auditing

Название поля	Описание	Пример значения
endpoint_name	Название конечного устройства или сенсора.	DESKTOP-0731NFQ
endpoint_id	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
node	Идентификатор конечного устройства или узла, на котором запущен сенсор.	35fb5820-74db-4eac-b05b-d01bc284c4e8
log_level	Тип события.	Аудит успеха, Предупреждение, Сведения, Аудит отказа, Ошибка
log_file	Тип журнала, содержащего важную информацию о программных и аппаратных событиях.	Security (файл журнала безопасности), Application (файл журнала приложений), System (файл системного журнала), Windows PowerShell
log_event_type	Тип события лога.	1 (error), 2 (warning), 3 (information), 4 (audit success), 5 (audit failure).
log_event_id	Идентификатор события.	4672
log_event_code	Код события журнала.	14056
log_category_string	Категория события.	Special Logon
insertion_string	Строка вставки - данные блока eventData события Windows.	Windows DefenderSECURITY_PRODUCT_STATE_ON
error	Ошибка WMI или SNMP, возникшая в результате выполнения запроса.	0
data	Подробная информация о событии.	Тип запуска службы "Установщик модулей Windows" был изменен с "Автоматически" на "Вручную".
counter_id	Идентификатор счётчика, добавленного в WMI или SNMP сенсор.	35fb5820-74db-4eac-b05b-d01bc284c4e8
computer_name	Имя компьютера.	DESKTOP-0731NFQ

Описание журнала правил конечных устройств

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
session		Идентификатор сессии.	00000006-0000-0000-f04d-14bdad0f01bb
proto		Используемый протокол 4-го уровня.	TCP
host		Имя хоста.	www.google.com
action		Действие, принятое устройством в соответствии с настроенными политиками.	drop, accept, nat
endpoint_name		Имя конечного устройства.	DESKTOP-0731NFQ
endpoint_id		Идентификатор конечного устройства.	35fb5820-74db-4eac-b05b-d01bc284c4e8
media_type		Тип контента.	application/json
app_name		Приложение, к которому было применено правило межсетевого экрана.	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
source	ip	IPv4-адрес источника.	10.10.10.10
	port	Порт источника.	Может принимать значения от 0 до 65535.

Название поля		Описание	Пример значения
destination	ip	IPv4-адрес назначения.	104.19.197.151
	port	Порт назначения	Может принимать значения от 0 до 65535.
rule	guid	Уникальный идентификатор правила, срабатывание которого создало событие.	f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
	name	Название правила, срабатывание которого вызвало событие.	Default allow
	type	Тип сработавшего правила.	
url_categories	id	Идентификатор категории, к которой относится URL.	39
	threat_level	Уровень угрозы категории URL.	Может принимать значения: • 1 — очень низкий. • 2 — низкий. • 3 — средний. • 4 — высокий. • 5 — очень высокий.
	name	Название категории, к которой относится URL.	Social Networking

Описание журнала приложений конечных устройств

Название поля		Описание	Пример значения
user_name		Имя пользователя, под учётной записью которого выполнен вход на конечном устройстве.	DESKTOP-0731NFQ\User
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
endpoint_name		Название конечного устройства или сенсора.	DESKTOP-0731NFQ
endpoint_id		Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
process_id		Идентификатор процесса.	3916
hash		Хэш приложения.	B4CE5C3495FEA0A4FDBAC8ABDCD199F7E4CA8C1F
app_name		Приложение, которое было запущено/остановлено.	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
action		Действие (запуск или остановка приложения).	start, stop
version		Версия приложения.	6.2.19041.746
subject		Субъект подписи.	Microsoft Corporation
issuer		Издатель сертификата для приложения.	Microsoft Windows Production PCA 2011
cmd_line		Запрос командной строки.	C:\Windows\system32\svchost.exe -k wsappx -p -s AppXSvc
session_id		Идентификатор сессии.	1656038456

Описание журнала аппаратуры конечных устройств

Название поля		Описание	Пример значения

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
endpoint_name	Название конечного устройства или сенсора.	DESKTOP-0731NFQ
endpoint_id	Идентификатор конечного устройства или сенсора.	35fb5820-74db-4eac-b05b-d01bc284c4e8
action	Действие (подключение/извлечение устройства).	add_device, remove_device
device_name	Название устройства, которое было подключено/извлечено.	Generic USB Hub
device_id	Идентификатор устройства.	USB\VID_0E0F&PID_0002\6&201153C1&0&7
service	Драйвер Windows, обеспечивающий взаимодействие компьютера с оборудованием/устройством.	USBHUB3

Описание журнала syslog

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda
syslog_facility		Тип источника события syslog. Например, user-level messages. Подробнее о значениях syslog facility смотрите в RFC 5424 .	1
syslog_severity		Уровень важности события syslog. Например, warning. Подробнее о значениях syslog severity смотрите в RFC 5424 .	4
computer_name		Имя устройства, на котором произошло событие.	node1
app_name		Приложение, вызвавшее событие.	org.gnome.Shell.desktop
process_id		PID процесса, вызвавшего событие.	3036
data		Описание события.	[3603:3603:1130/125201.838651:ERROR:CONSOLE(6)] "console.assert()", source: devtools://devtools/bundled/devtools-frontend/front_end/panels/console/console.js (6)
rule	guid	Уникальный идентификатор правила, срабатывание которого создало событие.	16535060-5a1a-4e92-8331-239406ec34da
	name	Название правила, срабатывание которого вызвало событие.	Example — Allow user-level messages
	type	Тип сработавшего правила.	

Описание журнала RADIUS

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda

Название поля		Описание	Пример значения	
event_type		Статус пользователя (acct_status_type).	start, stop, interim update, accounting-on, accounting-off	
action		Действие, принятое устройством в соответствии с настроенными политиками.	login	
src_ip		IP-адрес источника, откуда пришло сообщение.	192.168.57.4	
nas_ip		IP-адрес NAS, авторизовавшего пользователя.	172.16.1.4	
framed_ip		IP-адрес пользователя.	192.168.57.29	
rule	guid	Уникальный идентификатор правила, срабатывание которого создало событие.	16535060-5a1a-4e92-8331-239406ec34da	
user	guid	Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b0000044f	
	name		Имя пользователя.	user_name
	groups	guid	Уникальный идентификатор группы, в которой состоит пользователь.	aa218609-8716-9252-df20-88c43a0d0bf6
		name	Название группы, в которой состоит пользователь.	test_group

Описание журнала UserID

Название поля		Описание	Пример значения	
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z	
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ntoorereaeda	
reasons		Причина, по которой было создано событие.	{\"user_groups_sids\":[\"S-1-5-21-3795870133-5220325-2125745684-513\", \"S-1-5-21-3795870133-5220325-2125745684-512\", \"S-1-5-21-3795870133-5220325-2125745684-572\"], \"user_sid\": \"S-1-5-21-3795870133-5220325-2125745684-1103\", \"login\": \"user1\", \"domain\": \"DEV\", \"event_id\": 4624}	
action		Действие, принятое устройством в соответствии с настроенными политиками.	login	
src_ip		IPv4 источника события.	10.10.0.11	
rule	guid	Уникальный идентификатор правила, срабатывание которого создало событие.	16535060-5a1a-4e92-8331-239406ec34da	
	name	Название правила, срабатывание которого вызвало событие.	dev.local	
	type	Тип сработавшего правила.	syslog	
user	guid	Уникальный идентификатор пользователя. Если пользователь типа Unknown, то идентификатор: 00000000-0000-0000-0000-000000000000.	745591c3-9d21-092d-8db4-5b9b0000044f	
	name	Имя пользователя.	user1	
	groups	guid	Уникальный идентификатор группы, в которых состоит пользователь.	aa218609-8716-9252-df20-88c43a0d0bf6
		name	Название группы, в которой состоит пользователь.	CN=Domain Users,CN=Users,DC=dev,DC=local

Общие сведения

Documentation: ☒
Product: SIEM
Version: 7.x

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: SIEM

Version: 7.x

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

Список возможных шаблонов отчетов, сгруппированных по категориям:

- **Пользовательский** — группа шаблонов по обобщенной статистике срабатывания правил отчетов.
- **Captive-портал** — группа шаблонов по событиям, авторизации пользователей с помощью Captive-портала.
- **Приложения конечных устройств** — группа шаблонов со списками приложений, которые когда-либо запускались на конечных устройствах.
- **Журнал правил конечных устройств** — группа шаблонов по событиям срабатывания правил межсетевого экрана конечных устройств.
- **Журнал событий конечных устройств** — группа шаблонов по событиям, полученным от контролируемых с помощью программного обеспечения UserGate Endpoint конечных устройств
- **События** — группа шаблонов по событиям, регистрируемым в журнале событий.
- **СОВ** — группа шаблонов по событиям, регистрируемым в журнале СОВ.
- **Защита почтового трафика** — группа шаблонов по событиям, регистрируемым в журнале защиты почтового трафика.
- **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.
- **UserID** — группа шаблонов для создания отчетов по работе UserID агента.
- **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).

Создание пользовательских шаблонов отчетов

Documentation: ☒

Product: SIEM

Version: 7.x

Если в системных шаблонах отсутствуют параметры, необходимые для отчета, вы можете создать собственный шаблон и использовать его в правилах генерации этого отчета.

Чтобы создать шаблон:

1. В разделе **Журналы и отчеты** → **Отчеты** → **Пользовательские шаблоны** нажмите **Добавить**.

2. В окне настройки шаблона выполните следующее:

- Укажите название и при необходимости описание шаблона.
- Укажите источник, данные которого требуется использовать для создания отчета. Вы можете выбрать [один из журналов](#) или [список срабатываний правил аналитики](#).
- При необходимости введите [выражение на языке запросов](#), по которому будут отфильтрованы данные при создании отчета.
- При необходимости укажите параметр, по которому будут отсортированы записи отчета, а также направление сортировки (по возрастанию или по убыванию значений параметра).

Выбор параметра для сортировки недоступен, если указан параметр для группировки записей. В этом случае сортировка выполняется по количеству записей в каждой группе в порядке убывания.

- При необходимости укажите параметр, по которому будут сгруппированы записи отчета.

Выбор параметра для группировки недоступен, если указан параметр для сортировки записей.

- В блоке **Столбцы** → **Доступно** двойным щелчком мыши выберите параметры, значения которых необходимо отображать в отчете.

Примечание Чтобы запись отчета, содержащая массив в качестве значения параметра, была преобразована в несколько записей (по одной для каждого элемента массива), установите флажок «Разъединять записи».

3. Нажмите **Сохранить**.

Созданный шаблон отобразится в таблице **Пользовательские шаблоны**. Для использования шаблона необходимо добавить его [в правило генерации отчетов](#).

Правила отчетов

Documentation: ☒
Product: SIEM
Version: 7.x

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.
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.

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.

ПримечаниеДля 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: SIEM

Version: 7.x

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: SIEM
Version: 7.x

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 .

Шаблоны отчетов инцидентов

Documentation: 

Product: SIEM

Version: 7.x

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).

Правила отчетов инцидентов

Documentation: ☒
Product: SIEM
Version: 7.x

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: SIEM

Version: 7.x

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**.

