

## Table of Contents

|                                 |    |
|---------------------------------|----|
| Table of Contents               | 1  |
| Журналы                         | 2  |
| Общие сведения                  | 3  |
| Журнал событий                  | 4  |
| Журнал веб-доступа              | 5  |
| Журнал DNS                      | 6  |
| Журнал трафика                  | 7  |
| Журнал COB                      | 8  |
| Журнал инспектирования SSH      | 9  |
| История поиска                  | 10 |
| Журнал защиты почтового трафика | 11 |
| UserID-агент                    | 12 |
| Экспорт журналов                | 15 |
| Поиск и фильтрация данных       | 18 |
| Описание форматов журналов      | 20 |



Documentation: 

Product: NGFW

Version: 7.x

UserGate NGFW регистрирует события, возникающие в процессе его функционирования, и сохраняет их в следующих журналах:

- **Журнал событий** — содержит события, связанные с изменением параметров UserGate NGFW, авторизацией пользователей, обновлениями различных списков и т. п.
- **Журнал веб-доступа** — подробный журнал всех веб-запросов, обработанных UserGate NGFW.
- **Журнал DNS** — содержит события, связанные с DNS-трафиком.
- **Журнал трафика** — подробный журнал срабатывания правил межсетевого экрана, NAT, DNAT, правил подмены портов и правил маршрутизации на основе политик (PBR). Для регистрации этих событий необходимо включить функцию журналирования в соответствующих правилах.
- **Журнал СОВ** — содержит события, регистрируемые системой обнаружения и предотвращения вторжений.
- **Журнал инспектирования SSH** — журнал срабатывания правил инспектирования SSH. Для регистрации этих событий необходимо включить функцию журналирования.
- **История поиска** — содержит сведения о поисковых запросах пользователей в популярных поисковых системах.
- **Журнал защиты почтового трафика** — содержит события срабатывания правил защиты почтового трафика, в параметрах которых включена функция журналирования.
- **Агент UserID** — содержит описание событий, отражающих результат работы UserID-агента.

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 отображаются в журнале событий. В случае, если узел интегрирован с UserGate Log Analyzer, записи будут отображаться в журнале событий UserGate Log Analyzer. Ротация записей журнала событий никогда не производится.

**Примечание** В релизе 7.5.0 и выше при изменении имени узла в настройках кластера конфигурации его новое имя будет отображаться как в веб-консоли, так и во всех журналах и отчетах.

Documentation: 

Product: NGFW

Version: 7.x

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

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.

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

## Журнал веб-доступа

---

Version: 7.x

Product: NGFW

Documentation: ☒

Журнал веб-доступа отображает все запросы пользователей в интернет по протоколам HTTP и HTTPS. Выводятся события срабатывания правил фильтрации контента, инспектирования SSL, Веб-безопасности, Captive-портала в настройках которых включено журналирование. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.
- Время события.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Причины (при блокировке сайта).
- URL назначения.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- Категории сайтов.
- Приложение.
- Протокол прикладного уровня.
- HTTP метод.
- Код ответа HTTP.
- Тип контента (если присутствует).
- Информация.
- Байт отправлено/получено.
- Пакетов отправлено/получено.
- Реферер (при наличии).
- Операционная система.
- User-agent браузер.

**Примечание** В столбцах трафика (Байт отправлено/получено, Пакетов отправлено/получено) указывается трафик после срабатывания всех правил на этом запросе.

Если правила требуют анализа ответа от веб-сервера, то трафик ответа также будет подсчитан и учтён одинаковый, в том числе у первого сработавшего на этом запросе правила (bypass captive, decrypt). Таким образом, учитывается весь прошедший трафик и указывается одно и то же значение каждому правилу, сработавшему на этом запросе.

Если анализ ответа от веб-сервера для правил не требуется, то весь остальной трафик не учитывается.

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.

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

## Журнал DNS

---

Documentation: ☒

Product: NGFW, LogAn, SIEM

Version: 7.x

Журнал DNS отображает события, связанные с DNS трафиком. Для журналирования событий DNS на 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.

Documentation: ☒

Product: NGFW

Version: 7.x

Журнал трафика отображает события срабатывания правил межсетевого экрана и правил NAT, в настройках которых включено журналирование. Отображается следующая информация:

- Узел NGFW, на котором произошло событие.
- Время события.
- Содержание события.
- Пользователь.
- Действие.
- Правило.
- Приложение.
- Сетевой протокол.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC источника
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- MAC назначения.
- NAT IP-адрес источника (если это правило NAT).
- NAT порт источника (если это правило NAT).
- NAT IP-адрес назначения (если это правило NAT).
- NAT порт назначения (если это правило NAT).
- Байт отправлено/получено.
- Пакетов отправлено/получено.

**Примечание** В столбцах трафика (Байт отправлено/получено, Пакетов отправлено/получено) указывается трафик, учтенный в момент срабатывания журналирующего правила.

Если в настройках журналирования в правиле выбрано: "Журналировать каждый пакет", то значения учтенного трафика в журнале будут кумулятивно нарастать в течение сессии.

Если в настройках журналирования в правиле выбрано: "Журналировать начало сессии", будет учтен всего один или несколько пакетов, необходимых для срабатывания этого правила.

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.

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

Documentation: ☒

Product: NGFW, LogAn, 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 NGFW, на котором произошло событие.
- Время.
- Содержание события.
- Пользователь.
- Действие (финальное действие, начиная с версии 7.5.1) — итоговое решение межсетевого экрана: разрешить или заблокировать трафик. Несмотря на то что для каждой сигнатуры COB задано отдельное действие, итоговое решение определяется действием, выбранным в профиле сигнатур COB, в котором сработали сигнатуры.
- Правило.
- Сигнатуры.
- Приложение.
- Сетевой протокол.
- Зона источника.
- IP-адрес источника.
- Порт источника.
- MAC источника.
- Зона назначения.
- IP-адрес назначения.
- Порт назначения.
- MAC назначения.

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

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

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

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

## Журнал инспектирования SSH

---

Version: 7.x

Documentation: ☒

Product: NGFW

Журнал инспектирования SSH отображает сработавшие правила инспектирования SSH, для которых включено журналирование. Отображается следующая информация:

- Узел NGFW, 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 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.

## История поиска

---

Documentation: ☒

Product: NGFW

Version: 7.x

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.

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

## Журнал защиты почтового трафика

---

Documentation: ☒

Product: NGFW, LogAn, 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.

Product: NGFW  
Version: 7.x  
Technology: Identification and Authentication  
Documentation: ☒

Журнал Windows Active Directory

Журнал Windows Active Directory отображает события, собранные UserID агентом с помощью коннектора "Microsoft Active Directory" с серверов AD. В журнале отображаются события с успешным входом в систему (идентификатор события 4624), событий Kerberos (события с номерами: 4768, 4769, 4770) и события членства в группах (идентификатор события 4627). В журнале отображена следующая информация:

| Наименование                              | Описание                                                                                                     |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Узел                                      | Узел UserGate, которым зафиксировано событие.                                                                |
| Время                                     | Время произошедшего события.                                                                                 |
| Запись журнала событий конечных устройств | Ссылка на событие.                                                                                           |
| Конечное устройство\сенсор                | UserID конектор.                                                                                             |
| Уровень лога                              | Поле "Keywords" из журнала AD.                                                                               |
| Данные                                    | Содержание события из журнала AD.                                                                            |
| Источник журнала событий                  | Поле "Источник" из журнала AD.                                                                               |
| Категория журнала                         | Код категории инцидента (12554 Group Membership, 12544 Logon, 14337 Kerberos Service Ticket Operations и тд) |
| Категория инцидента                       | Поле "Тип задачи" из журнала AD                                                                              |
| Имя компьютера                            | узел Windows на котором произошло событие.                                                                   |
| Пользователь                              | Поле "Пользователь"из журнала AD.                                                                            |
| Код события лога                          | Поле "Код события" из журнала AD (EventCode).                                                                |
| Идентификатор события лога                | Поле "Идентификатор события" из журнала AD (EventID).                                                        |
| Тип события лога                          | Тип событий журнала Windows (Система\Безопасность\Приложение и т. д.).                                       |
| Файл журнала лога                         | файл журнала Windows.                                                                                        |

Syslog (Журнал)

Журнал Syslog отображает события, собранные UserID агентом с помощью коннектора "Отправитель syslog" с серверов-источников данных 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. |

| Наименование           | Описание                                                                                                        |
|------------------------|-----------------------------------------------------------------------------------------------------------------|
| 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.                                                                                               |

### UserID (Журнал)

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.                     |
| Содержание события | Открыть подробное описание 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.                                |

### RADIUS (Журнал)

Журнал RADIUS отображает события, собранные UserID агентом с помощью коннектора "RADIUS" 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.                     |

| Наименование          | Описание                                                     |
|-----------------------|--------------------------------------------------------------|
| Идентификатор правила | Идентификатор правила, срабатывание которого создало событие |
| Пользователь          | Пользователь, который вызвал событие.                        |
| Группы                | Строка групп в которых состоит пользователь.                 |
| Статус                | Статус пользователя.                                         |
| 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).                   |

Documentation: ☒  
Product: NGFW  
Version: 7.x

Функция экспортирования журналов UserGate позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

UserGate поддерживает выгрузку следующих журналов:

- Журнал событий.
- Журнал веб-доступа.
- Журнал COB.
- Журнал трафика.
- Журнал инспектирования SSH.
- Журнал DNS.
- Журнал почтового трафика.
- Журнал UserID.

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

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

**Примечание**Если в настройках указан Log Analyzer, то обработка и экспорт журналов, создание отчётов и обработка других статистических данных производятся сервером LogAn.

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. Опция доступна в версии ПО 7.2.0 и выше.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Журналы для экспорта        | <p>Выбор файлов журналов, которые необходимо экспортировать:</p> <ul style="list-style-type: none"><li>• Журнал событий.</li><li>• Журнал веб-доступа.</li><li>• Журнал COB.</li><li>• Журнал трафика.</li><li>• Журнал инспектирования SSH.</li><li>• Журнал DNS.</li><li>• Журнал почтового трафика.</li><li>• UserID.</li></ul> <p>Для каждого из журналов возможно указать синтаксис выгрузки:</p> <ul style="list-style-type: none"><li>• CEF — Common Event Format (ArcSight).</li><li>• CEF Compact.</li><li>• JSON — JSON format.</li><li>• @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON.</li></ul> <p>Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов.</p> <p>Подробное описание форматов журналов читайте в приложении <a href="#">Описание форматов журналов</a>.</p> |

| Наименование    | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Тип сервера     | SSH (SFTP), FTP, Syslog.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Адрес сервера   | IP-адрес или доменное имя сервера.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Транспорт       | Только для типа серверов Syslog — TCP или UDP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Порт            | Порт сервера, на который следует отправлять данные.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Протокол        | Только для типа серверов Syslog — RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Критичность     | <p>Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения:</p> <ul style="list-style-type: none"> <li>• <b>Тревога:</b> состояние, требующее незамедлительного вмешательства.</li> <li>• <b>Критическая:</b> состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе.</li> <li>• <b>Ошибки:</b> в системе возникли ошибки.</li> <li>• <b>Предупреждения:</b> предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия.</li> <li>• <b>Уведомительная:</b> события, которые относятся к необычному поведению системы, но не являются ошибками.</li> <li>• <b>Информативная:</b> информационные сообщения.</li> </ul> |
| Facility        | <p>Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения:</p> <ul style="list-style-type: none"> <li>• <b>Сообщения пользовательские.</b></li> <li>• <b>Системный сервис.</b></li> <li>• <b>Безопасность/авторизация.</b></li> <li>• <b>Аудит.</b></li> <li>• <b>Тревога.</b></li> <li>• <b>Local 0.</b></li> <li>• <b>Local 1.</b></li> <li>• <b>Local 2.</b></li> <li>• <b>Local 3.</b></li> <li>• <b>Local 4.</b></li> <li>• <b>Local 5.</b></li> <li>• <b>Local 6.</b></li> <li>• <b>Local 7.</b></li> </ul>                                                                                                                                                                        |
| 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Путь на сервере | Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Наименование                | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Расписание</b>           | <p>Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты:</p> <ul style="list-style-type: none"> <li>• Ежедневно.</li> <li>• Еженедельно.</li> <li>• Ежемесячно.</li> <li>• Каждые ... часов.</li> <li>• Каждые ... минут.</li> <li>• Задать вручную.</li> </ul> <p>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:</p> <ul style="list-style-type: none"> <li>• Звездочка (*) — обозначает весь диапазон (от первого до последнего).</li> <li>• Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7.</li> <li>• Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23".</li> <li>• 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".</li> </ul> |
| <b>Управление журналами</b> | <p>Управление временными файлами журналов, подготавливаемых для отправки на удаленные серверы ssh и ftp.</p> <p>При отправке журналов на сервера ssh и ftp UserGate сохраняет данные для отправки во временные файлы. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки.</p> <p>Всего хранятся N архивов журналов за предыдущие дни (по количеству дней ротации) и один журнал за текущий день.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

Поиск и фильтрация данных

Documentation: ☒  
Product: NGFW  
Version: 7.x

Объем данных, регистрируемых в журналах, как правило, значителен, поэтому в стандартном режиме просмотра отображается лишь часть доступных полей. Для быстрого доступа к необходимой информации в UserGate NGFW предусмотрены средства поиска и фильтрации журналов. Поиск может выполняться как в простом, так и в расширенном режиме.

В режиме простого поиска фильтрация записей осуществляется с помощью графического интерфейса. Настройка условий поиска выполняется в удобной форме и не требует знания специальных команд или синтаксиса.

Для создания более сложных условий отбора предназначен режим расширенного поиска, использующий специализированный язык запросов. В этом режиме доступны поля журналов, которые не отображаются и не могут использоваться в стандартном режиме поиска. Запросы формируются с использованием имен полей, их значений, ключевых слов и логических операторов. Значения, содержащие пробелы, необходимо заключать в одинарные ( ' ') или двойные ( " ") кавычки. Для значений без пробелов кавычки не требуются. Для объединения и группировки нескольких условий в запросе можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

| Ключевые поля | Значение                                                            |
|---------------|---------------------------------------------------------------------|
| AND или and   | Логическое «И», требует выполнение всех условий, заданных в запросе |
| OR или or     | Логическое «ИЛИ», требует выполнение одного из условий запроса      |

Операторы определяют условия фильтра и могут быть следующими:

| Оператор | Значение                                                                                                                                                                                                                                                                         |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| =        | Равно — требует полного совпадения значения поля с указанным значением.<br>Пример: ip = 172.16.31.1.<br>Будут отображены все записи журнала, в которых поле ip будет точно соответствовать значению 172.16.31.1                                                                  |
| !=       | Не равно — значение поля не должно совпадать с указанным значением.<br>Пример: ip != 172.16.31.<br>Будут отображены все записи журнала, в которых поле ip не будет равно значению 172.16.31.1                                                                                    |
| <=       | Меньше либо равно — значение поля должно быть меньше или равно указанному в запросе значению. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п.<br>Пример: date <= '2019-03-28T20:59:59' AND statusCode = 303 |
| >=       | Больше либо равно — значение поля должно быть больше или равно указанному в запросе значению. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п.<br>Пример: date >= "2019-03-13T21:00:00" AND statusCode = 200 |
| <        | Меньше — значение поля должно быть меньше указанного в запросе значения. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п.<br>Пример: date < '2019-03-28T20:59:59' AND statusCode = 404                       |
| >        | Больше — значение поля должно быть больше указанного в запросе значения. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п.<br>Пример: (statusCode > 200 AND statusCode < 300) OR (statusCode = 404)           |
| IN       | Позволяет указать в запросе несколько значений поля. Список значений необходимо заключать в круглые скобки.<br>Пример: category IN (botnets, compromised, 'illegal software', 'phishing and fraud',' reputation high risk', 'unknown category')                                  |

| Оператор  | Значение                                                                                                                                                                                                                                                                                                                                              |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NOT IN    | <p>Позволяет указать в запросе несколько значений поля. Будут отображены записи, в которых значение поля не совпадает ни с одним из указанных. Список значений необходимо заключать в круглые скобки.</p> <p>Пример: category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud', 'reputation high risk', 'unknown category')</p> |
| ~         | <p>Содержит — позволяет указать подстроку, которая должна присутствовать в значении выбранного поля. Поиск выполняется без учета регистра.</p> <p>Пример: browser ~ "Mozilla/5.0".</p> <p>Оператор применяется только к полям, содержащим строковые значения</p>                                                                                      |
| !~        | <p>Не содержит — позволяет указать подстроку, которая не должна присутствовать в значении выбранного поля. Поиск выполняется без учета регистра.</p> <p>Пример: browser !~ "Mozilla/5.0".</p> <p>Оператор применяется только к полям, содержащим строковые значения</p>                                                                               |
| MATCH     | <p>Поиск по полю с помощью регулярного выражения. Будут показаны только те записи, в которых значение поля соответствует заданному шаблону.</p> <p>Пример: details MATCH NAT — будут отфильтрованы все записи журнала, в которых в проверяемом поле details найдется слово «NAT»</p>                                                                  |
| NOT MATCH | <p>Поиск записей, в которых значение поля не совпадает с заданным регулярным выражением. Будут показаны только те записи, в которых значение поля не соответствует заданному шаблону.</p> <p>Пример: details NOT MATCH NAT — будут отфильтрованы все записи журнала, в которых в проверяемом поле details не найдется слово «NAT»</p>                 |

При формировании запроса в режиме расширенного поиска UserGate NGFW предлагает варианты названий полей, допустимых операторов и возможных значений. Это упрощает создание сложных поисковых выражений и снижает вероятность ошибок при вводе. Набор доступных полей и перечень допустимых значений зависят от типа просматриваемого журнала.

**Примечание** В критериях расширенного поиска не поддерживается использование символов кириллицы.

При переходе из режима простого поиска в режим расширенного поиска UserGate NGFW автоматически преобразует заданные параметры фильтрации в строку запроса, соответствующую условиям, указанным в базовом режиме. Вы можете продолжить формирование строки поиска с использованием расширенных возможностей языка запросов без необходимости повторного ввода критериев отбора.

Documentation: ☒  
Product: NGFW  
Version: 7.x

Экспорт журналов в формате CEF

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: <ul style="list-style-type: none"><li>• 1 — информационные;</li><li>• 4 — предупреждения;</li><li>• 7 — ошибки;</li><li>• 10 — критичные.</li></ul> |
| 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        |

| Тип поля                   | Название поля                   | Описание                                                                                                  | Пример значения                                                                                                                 |
|----------------------------|---------------------------------|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
|                            | <b>Device Product</b>           | Тип продукта.                                                                                             | NGFW                                                                                                                            |
|                            | <b>Device Version</b>           | Версия продукта.                                                                                          | 7                                                                                                                               |
|                            | <b>Source</b>                   | Название журнала.                                                                                         | webaccess                                                                                                                       |
|                            | <b>Name</b>                     | Тип источника.                                                                                            | log                                                                                                                             |
|                            | <b>Threat Level</b>             | Уровень угрозы категории URL.                                                                             | Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена. |
| <b>CEF</b><br>[расширение] | <b>rt</b>                       | Время, когда было получено событие: миллисекунды с 1 января 1970 года.                                    | 1652344423822                                                                                                                   |
|                            | <b>deviceExternalId</b>         | Имя, которое однозначно идентифицирует устройство, генерирующее это событие.                              | utmcore@ersthetatica                                                                                                            |
|                            | <b>act</b>                      | Действие, принятое устройством в соответствии с настроенными политиками.                                  | captive                                                                                                                         |
|                            | <b>reason</b>                   | Причина, по которой было создано событие, например, причина блокировки сайта.                             | {"id":39,"name":"Social Networking","threat_level":3}                                                                           |
|                            | <b>proto</b>                    | Используемый протокол 4-го уровня.                                                                        | TCP                                                                                                                             |
|                            | <b>app</b>                      | Протокол прикладного уровня и его версия.                                                                 | HTTP/1.1                                                                                                                        |
|                            | <b>suser</b>                    | Имя пользователя.                                                                                         | user_example (Unknown, если пользователь неизвестен)                                                                            |
|                            | <b>src</b>                      | IPv4 источника трафика.                                                                                   | 10.10.10.10                                                                                                                     |
|                            | <b>spt</b>                      | Порт источника.                                                                                           | Может принимать значения от 0 до 65535.                                                                                         |
|                            | <b>dst</b>                      | IPv4 адрес назначения трафика.                                                                            | 194.226.127.130                                                                                                                 |
|                            | <b>dpt</b>                      | Порт назначения.                                                                                          | Может принимать значения от 0 до 65535.                                                                                         |
|                            | <b>requestMethod</b>            | Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).                                          | GET                                                                                                                             |
|                            | <b>request</b>                  | В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола. | <a href="http://www.secure.com">http://www.secure.com</a>                                                                       |
|                            | <b>requestContext</b>           | URL источника запроса (реферер HTTP).                                                                     | <a href="https://www.google.com/">https://www.google.com/</a>                                                                   |
|                            | <b>requestClientApplication</b> | Useragent пользовательского браузера.                                                                     | Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0                                                    |
|                            | <b>in</b>                       | Количество переданных входящих байтов; данные передаются в направлении источник — назначение.             | 231                                                                                                                             |

| Тип поля | Название поля    | Описание                                                                                          | Пример значения                            |
|----------|------------------|---------------------------------------------------------------------------------------------------|--------------------------------------------|
|          | 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                           |
|          | 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                           |

| Тип поля | Название поля | Описание                                                           | Пример значения |
|----------|---------------|--------------------------------------------------------------------|-----------------|
|          | 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); Unknown, если категория не определена. |
|               | 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.                                                                                         |

| Тип поля            | Название поля            | Описание                                                                                                  | Пример значения                                                              |
|---------------------|--------------------------|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
| CEF<br>[расширение] | 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. | <a href="http://www.secure.com">http://www.secure.com</a>                    |
|                     | requestContext           | URL источника запроса (реферер HTTP).                                                                     | <a href="https://www.google.com/">https://www.google.com/</a>                |
|                     | 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                                                                          |

**Примечание**Общее 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<br>заголовок | CEF:Version    | Версия CEF.             | CEF:0           |
|                  | Device Vendor  | Производитель продукта. | UserGate        |
|                  | Device Product | Тип продукта.           | NGFW            |

| Тип поля            | Название поля    | Описание                                                                                         | Пример значения                                                                                                                 |
|---------------------|------------------|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
|                     | 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<br>[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.                         | <a href="https://www.google.com">google.com</a>                                                                                 |
|                     | 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                                                                                                                         |

| Тип поля | Название поля           | Описание                                               | Пример значения                                                                                                                                                                                                                                                      |
|----------|-------------------------|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <b>cs3Label</b>         | Поле используется для указания страны источника.       | Source Country                                                                                                                                                                                                                                                       |
|          | <b>cs3</b>              | Название страны источника.                             | RU (отображается двухбуквенный код страны)                                                                                                                                                                                                                           |
|          | <b>cs4Label</b>         | Поле используется для индикации зоны назначения.       | Destination Zone                                                                                                                                                                                                                                                     |
|          | <b>cs4</b>              | Название зоны назначения.                              | Untrusted                                                                                                                                                                                                                                                            |
|          | <b>cs5Label</b>         | Поле используется для указания страны назначения.      | Destination Country                                                                                                                                                                                                                                                  |
|          | <b>cs5</b>              | Название страны назначения.                            | RU (отображается двухбуквенный код страны)                                                                                                                                                                                                                           |
|          | <b>cs6Label</b>         | Поле используется для указания передаваемых данных.    | Data                                                                                                                                                                                                                                                                 |
|          | <b>cs6</b>              | Передаваемые данные.                                   | { "question": [{"domain": "google.com", "type": "A", "class": "IN"}],<br>"answer":<br>[{"domain": "google.com", "type": "TXT", "class": "IN", "ttl": 5, "data": "Blocked"},<br>{"domain": "google.com", "type": "A", "class": "IN", "ttl": 5, "data": "10.10.0.1"}]} |
|          | <b>flexString1Label</b> | Поле указывает на категорию запрашиваемого URL-адреса. | URL Categories                                                                                                                                                                                                                                                       |
|          | <b>flexString1</b>      | Категория URL.                                         | Search Engines & Portals                                                                                                                                                                                                                                             |

Формат журнала DNS CEF Compact:

| Тип поля                | Название поля           | Описание                                                                     | Пример значения                                                                                                                 |
|-------------------------|-------------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>CEF заголовок</b>    | <b>CEF:Version</b>      | Версия CEF.                                                                  | CEF:0                                                                                                                           |
|                         | <b>Device Vendor</b>    | Производитель продукта.                                                      | UserGate                                                                                                                        |
|                         | <b>Device Product</b>   | Тип продукта.                                                                | NGFW                                                                                                                            |
|                         | <b>Device Version</b>   | Версия продукта.                                                             | 7                                                                                                                               |
|                         | <b>Source</b>           | Название журнала.                                                            | dns                                                                                                                             |
|                         | <b>Name</b>             | Тип источника.                                                               | log                                                                                                                             |
|                         | <b>Threat Level</b>     | Уровень угрозы категории URL.                                                | Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена. |
| <b>CEF [расширение]</b> | <b>rt</b>               | Время, когда было получено событие: миллисекунды с 1 января 1970 года.       | 1701085036026                                                                                                                   |
|                         | <b>deviceExternalId</b> | Имя, которое однозначно идентифицирует устройство, генерирующее это событие. | utmcore@ntoorereaeda                                                                                                            |

| Тип поля | Название поля           | Описание                                                                                         | Пример значения                                                                                                                                                                                                                             |
|----------|-------------------------|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <b>act</b>              | Действие, принятое устройством в соответствии с настроенными политиками.                         | block                                                                                                                                                                                                                                       |
|          | <b>reason</b>           | Причина, по которой было создано событие, например, url категория, на которых сработало правило. | {"url_cats":[{"id":37,"name":"Search Engines & Portals","threat_level":1}]}                                                                                                                                                                 |
|          | <b>proto</b>            | Используемый протокол 4-го уровня.                                                               | UDP                                                                                                                                                                                                                                         |
|          | <b>dhost</b>            | Имя хоста назначения, адрес которого определяется с помощью DNS сервера.                         | <a href="http://google.com">google.com</a>                                                                                                                                                                                                  |
|          | <b>app</b>              | Протокол прикладного уровня.                                                                     | DNS                                                                                                                                                                                                                                         |
|          | <b>suser</b>            | Имя пользователя.                                                                                | user1 (Unknown, если пользователь неизвестен)                                                                                                                                                                                               |
|          | <b>src</b>              | IPv4 источника трафика.                                                                          | 10.10.0.11                                                                                                                                                                                                                                  |
|          | <b>spt</b>              | Порт источника.                                                                                  | Может принимать значения от 0 до 65535.                                                                                                                                                                                                     |
|          | <b>smac</b>             | MAC-адрес источника.                                                                             | FA:16:3E:65:1C:B4                                                                                                                                                                                                                           |
|          | <b>dst</b>              | IPv4 адрес назначения трафика.                                                                   | 194.226.127.130                                                                                                                                                                                                                             |
|          | <b>dpt</b>              | Порт назначения.                                                                                 | Может принимать значения от 0 до 65535. Для DNS обычно используется порт 53.                                                                                                                                                                |
|          | <b>cs1Label</b>         | Поле используется для указания сработавшего правила.                                             | Rule                                                                                                                                                                                                                                        |
|          | <b>cs1</b>              | Название правила, срабатывание которого вызвало событие.                                         | Rule1                                                                                                                                                                                                                                       |
|          | <b>cs2Label</b>         | Поле используется для индикации зоны источника.                                                  | SrcZone                                                                                                                                                                                                                                     |
|          | <b>cs2</b>              | Название зоны источника.                                                                         | Trusted                                                                                                                                                                                                                                     |
|          | <b>cs3Label</b>         | Поле используется для индикации зоны назначения.                                                 | DstZone                                                                                                                                                                                                                                     |
|          | <b>cs3</b>              | Название зоны назначения.                                                                        | Untrusted                                                                                                                                                                                                                                   |
|          | <b>cs4Label</b>         | Поле используется для указания передаваемых данных.                                              | Data                                                                                                                                                                                                                                        |
|          | <b>cs4</b>              | Передаваемые данные.                                                                             | {"question":[{"domain":"google.com","type":"A","class":"IN"}],<br>"answer":<br>[{"domain":"google.com","type":"TXT","class":"IN","ttl":5,"data":"Blocked"},<br>{"domain":"google.com","type":"A","class":"IN","ttl":5,"data":"10.10.0.1"}]} |
|          | <b>flexString1Label</b> | Поле указывает на категорию запрашиваемого URL-адреса.                                           | URLCats                                                                                                                                                                                                                                     |

| Тип поля | Название поля | Описание       | Пример значения          |
|----------|---------------|----------------|--------------------------|
|          | flexString1   | Категория URL. | Search Engines & Portals |

Формат журнала трафика

| Тип поля            | Название поля    | Описание                                                                     | Пример значения                                                                                                                 |
|---------------------|------------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| CEF<br>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<br>[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                                                                                                               |

| Тип поля | Название поля                       | Описание                                                                                           | Пример значения                                       |
|----------|-------------------------------------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------|
|          | <b>in</b>                           | Количество переданных входящих байтов; данные передаются в направлении источник — назначение.      | 231                                                   |
|          | <b>out</b>                          | Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.     | 40                                                    |
|          | <b>sourceTranslatedAddress</b>      | Адрес источника после переназначения (если настроены правила NAT).                                 | 192.168.174.134 (0.0.0.0 — если нет)                  |
|          | <b>sourceTranslatedPort</b>         | Порт источника после переназначения (если настроены правила NAT).                                  | Может принимать значения от 0 до 65535 (0 — если нет) |
|          | <b>destinationTranslatedAddress</b> | Адрес назначения после переназначения (если настроены правила NAT).                                | 192.226.127.130 (0.0.0.0 — если нет)                  |
|          | <b>destinationTranslatedPort</b>    | Порт назначения после переназначения (если настроены правила NAT).                                 | Может принимать значения от 0 до 65535 (0 — если нет) |
|          | <b>cs1Label</b>                     | Поле используется для указания срабатывания правила.                                               | Rule                                                  |
|          | <b>cs1</b>                          | Название правила, срабатывание которого вызвало событие.                                           | Allow trusted to untrusted                            |
|          | <b>cs2Label</b>                     | Поле используется для индикации зоны источника.                                                    | Source Zone                                           |
|          | <b>cs2</b>                          | Название зоны источника.                                                                           | Trusted                                               |
|          | <b>cs3Label</b>                     | Поле используется для указания страны источника.                                                   | Source Country                                        |
|          | <b>cs3</b>                          | Название страны источника.                                                                         | RU (отображается двухбуквенный код страны)            |
|          | <b>cs4Label</b>                     | Поле используется для индикации зоны назначения.                                                   | Destination Zone                                      |
|          | <b>cs4</b>                          | Название зоны назначения.                                                                          | Untrusted                                             |
|          | <b>cs5Label</b>                     | Поле используется для указания страны назначения.                                                  | Destination Country                                   |
|          | <b>cs5</b>                          | Название страны назначения.                                                                        | RU (отображается двухбуквенный код страны)            |
|          | <b>cn1Label</b>                     | Поле используется для указания количества переданных пакетов в направлении источник — назначение.  | Packets sent                                          |
|          | <b>cn1</b>                          | Количество переданных пакетов в направлении источник — назначение.                                 | 3                                                     |
|          | <b>cn2Label</b>                     | Поле используется для указания количества пакетов, переданных в направлении назначение — источник. | Packets received                                      |

| Тип поля | Название поля | Описание                                                            | Пример значения |
|----------|---------------|---------------------------------------------------------------------|-----------------|
|          | 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); 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              | 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                                                                                                               |

| Тип поля | Название поля                | Описание                                                                                       | Пример значения                                       |
|----------|------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------|
|          | 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); Unknowpn, если категория не определена. |

| Тип поля            | Название поля    | Описание                                                                                             | Пример значения                                      |
|---------------------|------------------|------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| CEF<br>[расширение] | rt               | Время, когда было получено событие:<br>миллисекунды с 1 января 1970 года.                            | 1652344423822                                        |
|                     | deviceExternalId | Имя, которое однозначно идентифицирует<br>устройство, генерирующее это событие.                      | utmcore@ersthetatica                                 |
|                     | act              | Действие, принятое устройством в<br>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;<br>данные передаются в направлении источник<br>— назначение.  | 231                                                  |
|                     | out              | Количество переданных исходящих байтов;<br>данные передаются в направлении<br>назначение — источник. | 40                                                   |
|                     | msg              | Уровень угрозы сигнатуры и её название.                                                              | [2] BlackSun                                         |
|                     | cs1Label         | Поле используется для указания<br>срабатывания правила.                                              | Rule                                                 |
|                     | cs1              | Название правила, срабатывание которого<br>вызвало событие.                                          | IDPS Rule Example                                    |
|                     | cs2Label         | Поле используется для индикации зоны<br>источника.                                                   | Source Zone                                          |
|                     | cs2              | Название зоны источника.                                                                             | Trusted                                              |
|                     | cs3Label         | Поле используется для указания страны<br>источника.                                                  | Source Country                                       |
|                     | cs3              | Название страны источника.                                                                           | RU (отображается двухбуквенный код страны)           |
|                     | cs4Label         | Поле используется для индикации зоны<br>назначения.                                                  | Destination Zone                                     |
|                     | cs4              | Название зоны назначения.                                                                            | Untrusted                                            |

| Тип поля | Название поля | Описание                                          | Пример значения                            |
|----------|---------------|---------------------------------------------------|--------------------------------------------|
|          | 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                                                                                                                        |
|                  | 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                                                                                                                             |

| Тип поля | Название поля | Описание                                                                                       | Пример значения   |
|----------|---------------|------------------------------------------------------------------------------------------------|-------------------|
|          | 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 инспектирования SSH

| 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 (Unkown, 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                                                                                                                |

| Тип поля | Название поля | Описание                                                 | Пример значения                            |
|----------|---------------|----------------------------------------------------------|--------------------------------------------|
|          | 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                        |
|          | 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); Unknown, если категория не определена. |

| Тип поля            | Название поля    | Описание                                                                     | Пример значения                                      |
|---------------------|------------------|------------------------------------------------------------------------------|------------------------------------------------------|
| CEF<br>[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                                              |
|                     | 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<br>заголовок | CEF:Version   | Версия CEF.             | CEF:0           |
|                  | Device Vendor | Производитель продукта. | UserGate        |

| Тип поля                   | Название поля           | Описание                                                                                       | Пример значения                                                                                                                 |
|----------------------------|-------------------------|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
|                            | <b>Device Product</b>   | Тип продукта.                                                                                  | NGFW                                                                                                                            |
|                            | <b>Device Version</b>   | Версия продукта.                                                                               | 7                                                                                                                               |
|                            | <b>Source</b>           | Тип журнала.                                                                                   | mailsecurity                                                                                                                    |
|                            | <b>Name</b>             | Тип источника.                                                                                 | log                                                                                                                             |
|                            | <b>Threat Level</b>     | Уровень угрозы приложения.                                                                     | Может принимать значения 2, 4, 6, 8, 10 (установленный уровень угрозы, умноженный на 2); Unknown, если категория не определена. |
| <b>CEF</b><br>[расширение] | <b>rt</b>               | Время, когда было получено событие: миллисекунды с 1 января 1970 года.                         | 1652344423822                                                                                                                   |
|                            | <b>deviceExternalId</b> | Имя, которое однозначно идентифицирует устройство, генерирующее это событие.                   | <a href="mailto:utmcore@einersonstal">utmcore@einersonstal</a>                                                                  |
|                            | <b>act</b>              | Действие, выполненное устройством в соответствии с настроенными политиками.                    | mark                                                                                                                            |
|                            | <b>app</b>              | Протокол прикладного уровня.                                                                   | SMTP                                                                                                                            |
|                            | <b>suser</b>            | Имя пользователя.                                                                              | user_example (Unknown, если пользователь неизвестен)                                                                            |
|                            | <b>src</b>              | IPv4-адрес источника.                                                                          | 10.10.10.10                                                                                                                     |
|                            | <b>spt</b>              | Порт источника.                                                                                | Может принимать значения от 0 до 65535.                                                                                         |
|                            | <b>dst</b>              | IPv4-адрес назначения.                                                                         | 10.10.10.10                                                                                                                     |
|                            | <b>dpt</b>              | Порт назначения.                                                                               | Может принимать значения от 0 до 65535.                                                                                         |
|                            | <b>in</b>               | Количество переданных входящих байтов; данные передаются в направлении источник — назначение.  | 10                                                                                                                              |
|                            | <b>out</b>              | Количество переданных исходящих байтов; данные передаются в направлении назначение — источник. | 10                                                                                                                              |
|                            | <b>cs1Label</b>         | Поле используется для указания названия правила.                                               | Rule                                                                                                                            |
|                            | <b>cs1</b>              | Название правила защиты почтового трафика.                                                     | Mail security rule                                                                                                              |
|                            | <b>cs2Label</b>         | Поле используется для указания зоны источника.                                                 | Source Zone                                                                                                                     |
|                            | <b>cs2</b>              | Зона источника.                                                                                | Untrusted                                                                                                                       |
|                            | <b>cs3Label</b>         | Поле используется для индикации страны источника трафика.                                      | Source Country                                                                                                                  |
|                            | <b>cs3</b>              | Страна источника трафика.                                                                      | RU (отображается двухбуквенный код страны)                                                                                      |

| Тип поля | Название поля    | Описание                                                                                          | Пример значения                                                |
|----------|------------------|---------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
|          | 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.                                                                                 | <a href="mailto:receiver@example.com">receiver@example.com</a> |
|          | flexString1Label | Поле используется для указания почтового адреса отправителя.                                      | From                                                           |
|          | flexString1      | Email отправителя.                                                                                | <a href="mailto:sender@example.com">sender@example.com</a>     |
|          | 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); Unknown, если категория не определена. |
|               |                |                            |                                                                                                                                 |

| Тип поля            | Название поля    | Описание                                                                                             | Пример значения                                                |
|---------------------|------------------|------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| CEF<br>[расширение] | rt               | Время, когда было получено событие:<br>миллисекунды с 1 января 1970 года.                            | 1652344423822                                                  |
|                     | deviceExternalId | Имя, которое однозначно идентифицирует<br>устройство, генерирующее это событие.                      | <a href="mailto:utmcore@einsonstal">utmcore@einsonstal</a>     |
|                     | act              | Действие, выполненное устройством в<br>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;<br>данные передаются в направлении источник<br>— назначение.  | 10                                                             |
|                     | out              | Количество переданных исходящих байтов;<br>данные передаются в направлении<br>назначение — источник. | 10                                                             |
|                     | cs1Label         | Поле используется для указания названия<br>правила.                                                  | Rule                                                           |
|                     | cs1              | Название правила защиты почтового трафика.                                                           | Mail security rule                                             |
|                     | cs2Label         | Поле используется для указания зоны<br>источника.                                                    | SrcZone                                                        |
|                     | cs2              | Зона источника.                                                                                      | Untrusted                                                      |
|                     | cs4Label         | Поле используется для указания зоны<br>назначения трафика.                                           | DstZone                                                        |
|                     | cs4              | Название зоны назначения трафика.                                                                    | Untrusted                                                      |
|                     | cs5Label         | Поле используется для указания почтового<br>адреса отправителя.                                      | From                                                           |
|                     | cs5              | Email отправителя.                                                                                   | <a href="mailto:sender@example.com">sender@example.com</a>     |
|                     | cs6Label         | Поле используется для указания почтового<br>адреса получателя.                                       | To                                                             |
|                     | cs6              | Email получателя.                                                                                    | <a href="mailto:receiver@example.com">receiver@example.com</a> |

| Тип поля            | Название поля    | Описание                                                                     | Пример значения                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------|------------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CEF<br>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.                                                            | endpoint_log                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                     | Name             | Тип источника.                                                               | log                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                     | Threat Level     | Уровень угрозы.                                                              | Может принимать значения от 1 до 10 (указанный уровень угрозы, умноженный на 2).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| CEF<br>[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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                     | suser            | Имя пользователя.                                                            | user1.dep.local                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                     | msg              | Описание события в журнале AD.                                               | Group membership information<br><br>Subject: Security ID: S-1-0-0 Account Name: — Account Domain: — Logon ID: 0x0 Logon Type: 3 New Logon: Security ID: S-1-5-21-3795870133-5220325-2125745684-1103 Account Name: user1 Account Domain: DEP Logon ID: 0xA57A446 Event in sequence: 1 of 1 Group Membership: %{S-1-5-21-3795870133-5220325-2125745684-513} %{S-1-1-0} %{S-1-5-32-544} %{S-1-5-32-555} %{S-1-5-32-545} %{S-1-5-32-554} %{S-1-5-2} %{S-1-5-11} %{S-1-5-15} %{S-1-5-21-3795870133-5220325-2125745684-512} %{S-1-5-21-3795870133-5220325-2125745684-572} %{S-1-5-64-10} %{S-1-16-12288} The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. This event is generated when the Audit Group Membership subcategory is configured. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session. |
|                     | cn1Label         | Поле используется для указания кода события из журнала AD.                   | logEventCode                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                     | cn1              | Код события.                                                                 | 4627                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                     | cn2Label         | Поле используется для указания номера идентификатора события из журнала AD.  | logEventId                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                     | cn2              | Идентификатор события.                                                       | 4627                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

| Тип поля | Название поля           | Описание                                                                                                                                   | Пример значения                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <b>cn3Label</b>         | Поле используется для указания типа события журнала Windows (Система\Безопасность\Приложение и т. д.).                                     | logEventType                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|          | <b>cn3</b>              | Тип события журнала Windows.                                                                                                               | 4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|          | <b>cs1Label</b>         | Поле используется для указания идентификатора конечного устройства — источника события.                                                    | endpointId                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|          | <b>cs1</b>              | Идентификатор конечного устройства.                                                                                                        | 16535060-5a1a-4e92-8331-239406ec34da                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|          | <b>cs2Label</b>         | Поле используется для указания имени конечного устройства — источника события (UserGate клиента, сенсора WMI итд.).                        | endpointName                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|          | <b>cs2</b>              | Имя конечного устройства.                                                                                                                  | dep.local                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|          | <b>cs3Label</b>         | Поле используется для указания уровня важности события в журнале AD.                                                                       | logLevel                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|          | <b>cs3</b>              | Уровень важности события.                                                                                                                  | Audit Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|          | <b>cs4Label</b>         | Поле используется для указания кода категории события (12554 Group Membership, 12544 Logon, 14337 Kerberos Service Ticket Operations и тд) | logCategoryString                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|          | <b>cs4</b>              | Категория события.                                                                                                                         | Group Membership                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|          | <b>cs5Label</b>         | Поле используется для указания файла журнала Windows.                                                                                      | logFile                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|          | <b>cs5</b>              | Файл журнала Windows                                                                                                                       | Security                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|          | <b>cs6Label</b>         | Поле используется для указания источника из журнала AD.                                                                                    | sourceName                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|          | <b>cs6</b>              | Источник из журнала AD.                                                                                                                    | Microsoft-Windows-Security-Auditing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|          | <b>flexString1Label</b> | Поле используется для указания содержания события из журнала AD.                                                                           | insertionString                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|          | <b>flexString1</b>      | Параметры события из журнала AD после парсинга сообщения.                                                                                  | ['S-1-0-0', '-', '-', '0x0', 'S-1-5-21-3795870133-5220325-2125745684-1103', 'user1', 'DEP', '0x7a25a21', '3', '1', '1', '\\r\\n\\t\\t%{S-1-5-21-3795870133-5220325-2125745684-513}\\r\\n\\t\\t%{S-1-1-0}\\r\\n\\t\\t%{S-1-5-32-544}\\r\\n\\t\\t%{S-1-5-32-555}\\r\\n\\t\\t%{S-1-5-32-545}\\r\\n\\t\\t%{S-1-5-32-554}\\r\\n\\t\\t%{S-1-5-2}\\r\\n\\t\\t%{S-1-5-11}\\r\\n\\t\\t%{S-1-5-15}\\r\\n\\t\\t%{S-1-5-21-3795870133-5220325-2125745684-512}\\r\\n\\t\\t%{S-1-5-21-3795870133-5220325-2125745684-572}\\r\\n\\t\\t%{S-1-5-64-10}\\r\\n\\t\\t%{S-1-16-12288}'] |

Формат журнала Syslog

| Тип поля            | Название поля    | Описание                                                                                                                                         | Пример значения                                                                                                                                                                                                                                                             |
|---------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CEF<br>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.                                                                                                                                | syslog                                                                                                                                                                                                                                                                      |
|                     | Name             | Тип источника.                                                                                                                                   | log                                                                                                                                                                                                                                                                         |
|                     | Threat Level     | Уровень угрозы.                                                                                                                                  | Может принимать значения: <ul style="list-style-type: none"><li>• 0 — emergencies;</li><li>• 1 — alerts;</li><li>• 2 — critical;</li><li>• 3 — errors;</li><li>• 4 — warnings;</li><li>• 5 — notifications;</li><li>• 6 — informational;</li><li>• 7 — debugging.</li></ul> |
| CEF<br>[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.<br><br>Подробнее о значениях syslog facility смотрите в <a href="#">RFC 5424</a> . | Facility                                                                                                                                                                                                                                                                    |
|                     | cn1              | Тип источника событий syslog.<br>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                                                                                                                                                                                                                                                                         |

| Тип поля | Название поля   | Описание                                                        | Пример значения                     |
|----------|-----------------|-----------------------------------------------------------------|-------------------------------------|
|          | <b>cs2</b>      | Приложение, вызвавшее событие.                                  | org.gnome.Shell.desktop             |
|          | <b>cs3Label</b> | Поле используется для указания идентификатора процесса события. | ProcessID                           |
|          | <b>cs3</b>      | PID процесса вызвавшего событие.                                | 3036                                |
|          | <b>cs4Label</b> | Поле используется для указания срабатывания правила.            | Rule                                |
|          | <b>cs4</b>      | Название правила, срабатывание которого вызвало событие.        | Example — Allow user-level messages |

## Формат журнала RADIUS

| Тип поля                | Название поля           | Описание                                                                     | Пример значения                                            |
|-------------------------|-------------------------|------------------------------------------------------------------------------|------------------------------------------------------------|
| <b>CEF заголовок</b>    | <b>CEF:Version</b>      | Версия CEF.                                                                  | CEF:0                                                      |
|                         | <b>Device Vendor</b>    | Производитель продукта.                                                      | UserGate                                                   |
|                         | <b>Device Product</b>   | Тип продукта.                                                                | NGFW                                                       |
|                         | <b>Device Version</b>   | Версия продукта.                                                             | 7                                                          |
|                         | <b>Source</b>           | Название журнала.                                                            | radius                                                     |
|                         | <b>Name</b>             | Тип источника.                                                               | log                                                        |
| <b>CEF [расширение]</b> | <b>rt</b>               | Время, когда было получено событие: миллисекунды с 1 января 1970 года.       | 1701085036026                                              |
|                         | <b>deviceExternalId</b> | Имя, которое однозначно идентифицирует устройство, генерирующее это событие. | utmcore@ntoorereaeda                                       |
|                         | <b>act</b>              | Статус пользователя (acct_status_type).                                      | start, stop, interim update, accounting-on, accounting-off |
|                         | <b>suser</b>            | Имя пользователя.                                                            | Unknown, если пользователь неизвестен.                     |
|                         | <b>src_ip</b>           | IP-адрес источника, откуда пришло сообщение.                                 | 192.168.57.4                                               |
|                         | <b>dst</b>              | IP-адрес NAS, авторизовавшего пользователя.                                  | 172.16.1.4                                                 |
|                         | <b>dvc</b>              | IP-адрес пользователя (framed ip address).                                   | 192.168.57.29                                              |
|                         | <b>cs1Label</b>         | Поле используется для указания группы, в которой состоит пользователь.       | user groups                                                |
|                         | <b>cs1</b>              | 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                                                                                                                                                                                                                              |
| 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"],<br><br>"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                                                                                                                                                                                                                        |

Экспорт журналов в формате JSON

Описание журнала событий

| Название поля | Описание                                                                     | Пример значения                                                                                                                                   |
|---------------|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| timestamp     | Время получения события в формате: уууу-мм-ддThh: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"} |

| Название поля   | Описание                                | Пример значения                                                                        |
|-----------------|-----------------------------------------|----------------------------------------------------------------------------------------|
| 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: уууу-мм-ддThh: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                                                                                        |
| packets_rcv    | 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. | <a href="http://www.secure.com">http://www.secure.com</a>                                |
| media_type     | Тип контента.                                                                       | application/json                                                                         |

| Название поля  |              | Описание                                          | Пример значения                                                                                                                                                                                      |
|----------------|--------------|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| status_code    |              | Код ответа HTTP.                                  | 302                                                                                                                                                                                                  |
| http_referer   |              | URL источника запроса (реферер HTTP).             | <a href="https://www.google.com/">https://www.google.com/</a>                                                                                                                                        |
| 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: <ul style="list-style-type: none"> <li>• 1 — очень низкий;</li> <li>• 2 — низкий;</li> <li>• 3 — средний;</li> <li>• 4 — высокий;</li> <li>• 5 — очень высокий.</li> </ul> |
|                | name         | Название категории, к которой относится URL.      | Social Networking                                                                                                                                                                                    |
| source         | zone         | guid                                              | Уникальный идентификатор зоны источника трафика.                                                                                                                                                     |
|                |              | name                                              | Название зоны источника.                                                                                                                                                                             |
|                | country      |                                                   | Страна источника трафика.                                                                                                                                                                            |
|                | ip           |                                                   | IPv4-адрес источника.                                                                                                                                                                                |
|                | port         |                                                   | Порт источника.                                                                                                                                                                                      |
|                | mac          |                                                   | MAC-адрес источника                                                                                                                                                                                  |
| destination    | zone         | guid                                              | Уникальный идентификатор зоны назначения трафика.                                                                                                                                                    |
|                |              | name                                              | Название зоны назначения трафика.                                                                                                                                                                    |
|                | country      |                                                   | Страна назначения.                                                                                                                                                                                   |
|                | ip           |                                                   | IPv4-адрес назначения.                                                                                                                                                                               |

| 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. | 919878b2-e882-49ed-3331-8ec72c3c79cb |
|               |        | name                                                                              | Название группы, в которой состоит пользователь.                 | Default Group                        |

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"}],<br>"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                                                                                                                                                                                                                                   |
|                |    |                                                                                                  |                                                                                                                                                                                                                                      |

| Название поля |              | Описание                                                                 | Пример значения                                                                                                                                                                      |
|---------------|--------------|--------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | threat_level | Уровень угрозы сработавшей категории.                                    | Может принимать значения: <ul style="list-style-type: none"><li>1 — очень низкий;</li><li>2 — низкий;</li><li>3 — средний;</li><li>4 — высокий;</li><li>5 — очень высокий.</li></ul> |
|               | name         | Название сработавшей категории.                                          | Search Engines & Portals                                                                                                                                                             |
| action        |              | Действие, принятое устройством в соответствии с настроенными политиками. | block                                                                                                                                                                                |
| application   | id           | Идентификатор приложения.                                                | 5                                                                                                                                                                                    |
|               | name         | Название приложения.                                                     |                                                                                                                                                                                      |
|               | threat_level | Уровень угрозы приложения.                                               | 0                                                                                                                                                                                    |
|               | app_protocol | Протокол прикладного уровня.                                             | DNS                                                                                                                                                                                  |
| source        | zone         | guid                                                                     | Уникальный идентификатор зоны источника трафика.                                                                                                                                     |
|               |              | name                                                                     | Название зоны источника трафика.                                                                                                                                                     |
|               | country      |                                                                          | Название страны источника.                                                                                                                                                           |
|               | ip           |                                                                          | IPv4-адрес источника трафика.                                                                                                                                                        |
|               | port         |                                                                          | Порт источника.                                                                                                                                                                      |
|               | mac          |                                                                          | MAC-адрес источника.                                                                                                                                                                 |
| destination   | zone         | guid                                                                     | Уникальный идентификатор зоны назначения трафика.                                                                                                                                    |
|               |              | name                                                                     | Название зоны назначения трафика.                                                                                                                                                    |
|               | country      |                                                                          | Название страны назначения.                                                                                                                                                          |
|               | ip           |                                                                          | IPv4-адрес назначения трафика.                                                                                                                                                       |
|               | port         |                                                                          | Порт назначения                                                                                                                                                                      |
|               | mac          |                                                                          | MAC-адрес назначения                                                                                                                                                                 |

| Название поля |        | Описание                                                                                                                       | Пример значения                                                  |                                      |
|---------------|--------|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|--------------------------------------|
| 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<br>(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_rcv     |  | Количество байтов, переданных в направлении назначение — источник.           | 6                                                                                           |
| packets_rcv   |  | Количество пакетов, переданных в направлении назначение — источник.          | 1                                                                                           |
| packets_sent  |  | Количество пакетов, переданных в направлении источник — назначение.          | 1                                                                                           |
| json_data     |  | Дополнительные данные.                                                       | null                                                                                        |

| Название поля |              |      | Описание                                                                 | Пример значения                                                                                                                                                                                      |
|---------------|--------------|------|--------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| application   | id           |      | Идентификатор приложения.                                                | 195                                                                                                                                                                                                  |
|               | threat_level |      | Уровень угрозы приложения.                                               | Может принимать значения: <ul style="list-style-type: none"> <li>• 1 — очень низкий;</li> <li>• 2 — низкий;</li> <li>• 3 — средний;</li> <li>• 4 — высокий;</li> <li>• 5 — очень высокий.</li> </ul> |
|               | 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)                                                                                                                        |
|               | 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                                                                                                                                                                                             |

| Название поля |        | Описание                                                                                                                      | Пример значения                                                  |                                      |
|---------------|--------|-------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|--------------------------------------|
|               | name   | Название правила, срабатывание которого вызвало событие.                                                                      | Allow trusted to untrusted                                       |                                      |
| user          | guid   | Уникальный идентификатор пользователя. Если пользователь типа Unknwn, 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: уууу-мм-ддThh: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_rcv     |              | Количество байтов, переданных в направлении назначение — источник.           | 6                                                                                                                                                                                    |
| packets_sent  |              | Количество пакетов, переданных в направлении источник — назначение.          | 1                                                                                                                                                                                    |
| packets_rcv   |              | 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: <ul style="list-style-type: none"><li>1 — очень низкий;</li><li>2 — низкий;</li><li>3 — средний;</li><li>4 — высокий;</li><li>5 — очень высокий.</li></ul> |

| Название поля |              | Описание                                                                                                                       | Пример значения                                                                                                                                                                            |
|---------------|--------------|--------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | name         | Название приложения.                                                                                                           | Youtube                                                                                                                                                                                    |
|               | 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: <ul style="list-style-type: none"> <li>1 — очень низкий;</li> <li>2 — низкий;</li> <li>3 — средний;</li> <li>4 — высокий;</li> <li>5 — очень высокий.</li> </ul> |
|               | 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)                                                                                                                                                 |

| Название поля |      | Описание                       | Пример значения                         |
|---------------|------|--------------------------------|-----------------------------------------|
|               | 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 инспектирования SSH

| Название поля |              |      | Описание                                                                     | Пример значения                                                                                 |
|---------------|--------------|------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| timestamp     |              |      | Время получения события в формате: уууу-мм-ддThh: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                                                                               |
|               |              |      |                                                                              |                                                                                                 |
| 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                                                                                  |
|               |              |      |                                                                              |                                                                                                 |

| 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 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. |
|               |        | name                                                                                                                          | Название группы, в которой состоит пользователь.                 |
|               |        |                                                                                                                               | 919878b2-e882-49ed-3331-8ec72c3c79cb                             |
|               |        |                                                                                                                               | Default Group                                                    |

Описание журнала защиты почтового трафика

| Название поля |    | Описание                                                                     | Пример значения                      |
|---------------|----|------------------------------------------------------------------------------|--------------------------------------|
| timestamp     |    | Время получения события в формате: уууу-мм-ддThh:mm:ssZ.                     | 2022-05-12T08:11:46.15869Z           |
| node          |    | Имя, которое однозначно идентифицирует устройство, генерирующее это событие. | <a href="#">utmcore@ersthetatica</a> |
| 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                                                                                 |
|--------------------|----------------|---------------------|--------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
|                    |                | <b>name</b>         | Название приложения.                                                     |                                                                                                 |
|                    |                | <b>threat_level</b> | Уровень угрозы приложения.                                               | Может принимать значения от 2 до 10 (установленный уровень угрозы приложения, умноженный на 2). |
|                    |                | <b>app_protocol</b> | Сетевой протокол прикладного уровня.                                     | SMTP                                                                                            |
|                    |                |                     |                                                                          |                                                                                                 |
| <b>source</b>      | <b>zone</b>    | <b>guid</b>         | Уникальный идентификатор зоны источника трафика.                         | d0038912-0d8a-4583-a525-e63950b1da47                                                            |
|                    |                | <b>name</b>         | Название зоны источника трафика.                                         | Trusted                                                                                         |
|                    | <b>country</b> |                     | Название страны источника.                                               | RU (отображается двухбуквенный код страны)                                                      |
|                    | <b>ip</b>      |                     | IPv4-адрес источника трафика.                                            | 10.10.10.10                                                                                     |
|                    | <b>port</b>    |                     | Порт источника.                                                          | Может принимать значения от 0 до 65535.                                                         |
|                    | <b>mac</b>     |                     | MAC-адрес источника.                                                     | 01:23:45:67:89:AB                                                                               |
| <b>destination</b> | <b>zone</b>    | <b>guid</b>         | Уникальный идентификатор зоны назначения трафика.                        | 3c0b1253-f069-4060-903b-5fec4f465db0                                                            |
|                    |                | <b>name</b>         | Название зоны назначения трафика.                                        | Untrusted                                                                                       |
|                    | <b>country</b> |                     | Название страны назначения.                                              | RU (отображается двухбуквенный код страны)                                                      |
|                    | <b>ip</b>      |                     | IPv4-адрес назначения трафика.                                           | 10.10.10.10                                                                                     |
|                    | <b>port</b>    |                     | Порт назначения.                                                         | Может принимать значения от 0 до 65535.                                                         |
|                    | <b>port</b>    |                     | MAC-адрес назначения.                                                    | 01:23:45:67:89:AB                                                                               |
| <b>rule</b>        | <b>guid</b>    |                     | Уникальный идентификатор правила, срабатывание которого создало событие. | 59e38e06-533a-4771-9664-031c3e8b2e1f                                                            |
|                    | <b>name</b>    |                     | Название правила, срабатывание которого вызвало событие.                 | Mail security rule                                                                              |
|                    | <b>type</b>    |                     | Тип сработавшего правила.                                                | Mail security rule                                                                              |
| <b>user</b>        | <b>guid</b>    |                     | Уникальный идентификатор пользователя.                                   | a7a3cd49-8232-4f1a-962a-3659af89e96f                                                            |
|                    | <b>name</b>    |                     | Имя пользователя.                                                        | user_name                                                                                       |
|                    | <b>groups</b>  | <b>guid</b>         | Уникальный идентификатор группы, в которой состоит пользователь.         | 919878b2-e882-49ed-3331-8ec72c3c79cb                                                            |
|                    |                | <b>name</b>         | Название группы, в которой состоит пользователь.                         | Default Group                                                                                   |

| Название поля       | Описание                                                                              | Пример значения                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| timestamp           | Время получения события в формате: уууу-мм-ddThh:mm:ssZ.                              | 2022-05-12T08:11:46.15869Z                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| node_name           | Имя, которое однозначно идентифицирует устройство UserGate, генерирующее это событие. | utmcore@ntoorereaeda                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| endpoint_id         | Идентификатор конечного устройства — источника события.                               | 16535060-5a1a-4e92-8331-239406ec34da                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| endpoint_name       | Имя конечного устройства — источника события (UserGate клиента, сенсора WMI итд.).    | dep.local                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| user_name           | Поле «Пользователь» из журнала AD.                                                    | user1.dep.local                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| log_level           | Поле «Keywords» из журнала AD.                                                        | Audit Success                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| log_category_string | Код категории события из журнала AD.                                                  | Group Membership                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| log_file            | Файл журнала Windows.                                                                 | Security                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| source_name         | Поле «Источник» из журнала AD.                                                        | Microsoft-Windows-Security-Auditing                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| data                | Описание события в журнале AD.                                                        | Group membership information.<br>Subject: Security ID: S-1-0-0<br>Account Name: Account Domain: Local Logon ID: 0x0<br>Type: New Logon: Security ID: S-1-5-21-3795870133-5220325-2125745684-1103<br>Account Name: user1<br>Account Domain: DEP<br>Logon ID: 0x7A25A21<br>Event in sequence: 1 of 1<br>Group Membership: S-1-5-21-3795870133-5220325-2125745684-513<br>S-1-1-0<br>S-1-5-32-544<br>S-1-5-32-555<br>S-1-5-32-545<br>S-1-5-32-554<br>S-1-5-2<br>S-1-5-11<br>S-1-5-15<br>S-1-5-21-3795870133-5220325-2125745684-512<br>S-1-5-21-3795870133-5220325-2125745684-572<br>S-1-5-64-10<br>S-1-16-12288<br>The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.<br>The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).<br>The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.<br>This event is generated when the Audit Group Membership subcategory is configured. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session. |
| computer_name       | Узел Windows из журнала AD, на котором произошло событие.                             | DC1.dep.local                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| insertion_string    | Параметры события из журнала AD после парсинга сообщения.                             | [S-1-0-0; ', '-', '0x0', 'S-1-5-21-3795870133-5220325-2125745684-1103', 'user1', 'DEP', '0x7a25a21', '3', '1', '1', '\r\n\\t%\n{S-1-5-21-3795870133-5220325-2125745684-513}\\r\n\\t%\n{S-1-1-0}\\r\n\\t%\n{S-1-5-32-544}\\r\n\\t%\n{S-1-5-32-555}\\r\n\\t%\n{S-1-5-32-545}\\r\n\\t%\n{S-1-5-32-554}\\r\n\\t%\n{S-1-5-2}\\r\n\\t%\n{S-1-5-11}\n\\r\n\\t%\n{S-1-5-15}\\r\n\\t%\n{S-1-5-21-3795870133-5220325-2125745684-512}\\r\n\\t%\n{S-1-5-21-3795870133-5220325-2125745684-572}\\r\n\\t%\n{S-1-5-64-10}\\r\n\\t%\n{S-1-16-12288}']                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| error               | Код ошибки из журнала AD, которая произошла при получении данных.                     | 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Название поля  | Описание                                                               | Пример значения |
|----------------|------------------------------------------------------------------------|-----------------|
| status         | Описание ошибки из журнала AD, которая произошла при получении данных. |                 |
| counter_id     | Идентификатор счетчика WMI сенсора.                                    | login_logout    |
| log_event_code | Поле «Код события» из журнала AD.                                      | 4627            |
| log_event_id   | Поле «Идентификатор события» из журнала AD.                            | 4627            |
| log_event_type | Тип событий журнала Windows (Система\Безопасность\Приложение и т. д.). | 4               |

## 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.<br><br>Подробнее о значениях syslog facility смотрите в <a href="#">RFC 5424</a> . | 1                                                                                                                                                                 |
| syslog_severity | Уровень важности события syslog. Например, warning.<br><br>Подробнее о значениях syslog severity смотрите в <a href="#">RFC 5424</a> .          | 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.                                                                                          |
|                 | name                                                                                                                                            | Название правила, срабатывание которого вызвало событие.                                                                                                          |
|                 | 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                                       |
| 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 | 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\"],<br><br>\"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                                                                                                                                                                                                                                                                                                       |

| Название поля |        | Описание                                                                                                                      | Пример значения                          |
|---------------|--------|-------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| user          | guid   | Уникальный идентификатор пользователя. Если пользователь типа Unkown, то идентификатор: 00000000-0000-0000-0000-000000000000. | 745591c3-9d21-092d-8db4-5b9b0000044f     |
|               | name   | Имя пользователя.                                                                                                             | user1                                    |
|               | groups | Уникальный идентификатор группы, в которой состоит пользователь.                                                              | aa218609-8716-9252-df20-88c43a0d0bf6     |
|               | name   |                                                                                                                               | CN=Domain Users,CN=Users,DC=dev,DC=local |

