

Table of Contents

Table of Contents	1
Log Analyzer 7.0.1 Руководство администратора	3
Введение	4
Введение	5
Лицензирование LogAn	6
Лицензирование LogAn	7
Первоначальная настройка	8
Описание	9
Развертывание виртуального образа	10
Подключение к LogAn	11
Развертывание программно-аппаратного комплекса	13
Настройка LogAn	14
Раздел настройки	15
Управление устройством	16
Администраторы	20
Управление сертификатами	22
Серверы аутентификации	24
Профили аутентификации	26
Роли и ролевые разрешения пользователей	27
Расширение системного раздела	34
Офлайн операции с сервером	35
Офлайн операции с сервером	36
Настройка сети	37
Настройка зон	38
Настройка интерфейсов	40
Настройка шлюзов	43
Маршруты	44
Сенсоры	45
Общие сведения	46
Сенсоры SNMP	47
Сенсоры WMI	49
Конечные устройства	50
Управление SNMP MIB	51
Интерфейс командной строки (CLI)	52
Интерфейс командной строки (CLI)	53
Диагностика и мониторинг	55
Диагностика и мониторинг	56
Сборщик логов	67
Описание	68
Syslog	69
Библиотеки	71
Почтовые адреса	72
Номера телефонов	74
Профили оповещений	76
Категории срабатываний	78
Внешние сервисы обогащений	79
Приложения syslog	81
Дашборд	82
Дашборд	83
Журналы и отчеты	84

Журналы	85
Описание	86
Журнал событий	87
Журнал веб-доступа	88
Журнал трафика	89
Журнал инспектирования SSH	90
История поиска	91
Экспорт журналов	92
Журнал СОВ	95
Журнал АСУ ТП	96
Поиск и фильтрация данных	97
Отчеты	99
Общие сведения	100
Шаблоны	101
Пользовательские шаблоны	102
Правила отчетов	103
Созданные отчеты	105
Отчеты инцидентов	106
Общие сведения	107
Правила отчетов инцидентов	108
Созданные отчеты инцидентов	109
Шаблоны отчетов инцидентов	110
Аналитика	111
Общие сведения	112
Пример настройки правила аналитики	115
Поиск	116
Действия реагирования	123
Срабатывания	127
Подробности срабатывания	129
Процессы конечных устройств	130
Инциденты	131
Общие сведения	132
Настройки инцидентов	133
Дашборд по инцидентам	135
Журнал инцидентов	136
Создание инцидентов безопасности	138
Подробности инцидента	139
Передача отчётов об инцидентах информационной безопасности в ГосСОПКА	141
Техническая поддержка	144
Техническая поддержка	145
Приложения	146
Требования к сетевому окружению	147
Описание форматов журналов	149
Экспорт журналов в формате CEF	150
Экспорт журналов в формате JSON	160

Введение

Documentation: ☒

Product: LogAn

Version: 7.0.1

UserGate Log Analyzer (LogAn) — это решение, реализующее функции систем SIEM (Security Information and Event Management) и IRP (Incident Response Platform).

SIEM — система управления информацией о безопасности и событиями информационной безопасности. LogAn собирает в себе данные, получаемые из различных источников (сенсоров), например, таких как, межсетевые экраны UserGate, системы управления и контроля конечных устройств UserGate, сенсоры SNMP, сенсоры WMI. Результат обработки данных предоставляется в едином интерфейсе, доступном для аналитиков безопасности, что облегчает изучение характерных особенностей, соответствующих инцидентам безопасности. На основе получаемых данных (событий) LogAn в реальном времени с помощью правил аналитики осуществляет агрегацию повторяющихся событий и их корреляцию (связывание разрозненных событий между собой), создавая инциденты кибербезопасности. Правила реагирования позволяют автоматически определить методы реагирования на инциденты информационной безопасности.

Для проведения расследований инцидентов кибербезопасности используется встроенная в LogAn система IRP. IRP — это платформа управления процессами реагирования на инциденты информационной безопасности. LogAn позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании.

LogAn поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде.

Лицензирование LogAn

Documentation: ☒
Product: LogAn
Version: 7.0.1
Technology: SIEM

LogAn лицензируется по количеству настроенных сенсоров, с которых он собирает информацию. В качестве сенсора может выступать шлюз UserGate либо любое другое устройство, которое может отправлять информацию по протоколу SNMP на сервер LogAn.

Лицензия на LogAn дает право бессрочного пользования продуктом.

Примечание При добавлении модуля SIEM в лицензию LogAn, администратору отображается предупреждение о смене роли сервера. Роль сервера будет изменена автоматически.

Дополнительно лицензируются следующие модули:

Наименование	Описание
Модуль Security Update (SU)	Модуль SU дает право на получение обновлений ПО LogAn. Модуль выписывается на 1 год, по истечении данного срока для получения обновлений ПО необходимо приобрести продление лицензии.
Сенсоры	Данный модуль определяет количество сенсоров, с которых LogAn может собирать информацию. Данный модуль выписывается сроком на 1 год и требует ежегодного продления.
Модуль Функциональность SIEM	Модуль предоставляет возможность использования функциональности систем SIEM и IRP: создание и настройка правил аналитики, а также определения методов реагирования на их срабатывания. Модуль дает право на бессрочное использование функциональности SIEM.
Модуль Подписка на экспертизу SIEM	Дополнительный модуль к модулю лицензирования Функциональность SIEM. Данный модуль дает право на получение экспертизы UserGate: • обновление библиотеки правил аналитики; • обновление библиотеки команд удалённого управления устройствами UserGate. Данный модуль выписывается сроком на 1 год. По истечении данного срока скачанные на момент наличия лицензии библиотеки продолжают работу, а их обновление становится недоступны, для получения обновлений необходимо продлить лицензию.

Для регистрации продукта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Перейти в Дашборд	Нажать на пиктограмму Дашборд в правом верхнем углу.
Шаг 2. В разделе Лицензия зарегистрировать продукт	В разделе Лицензия нажать на ссылку Нет лицензии , ввести ПИН-код и заполнить регистрационную форму.

Посмотреть статус установленной лицензии можно в разделе **Дашборд** в виджете **Лицензия**.

Первоначальная настройка

Описание

Documentation: ☒

Product: LogAn

Version: 7.0.1

LogAn поставляется в виде программно-аппаратного комплекса (ПАК, appliance) либо в виде образа виртуальной машины (virtual appliance), предназначенного для развертывания в виртуальной среде. В случае виртуальной машины LogAn поставляется с четырьмя Ethernet-интерфейсами. В случае поставки в виде ПАК LogAn может содержать 8 или более Ethernet-портов.

Развертывание виртуального образа

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

LogAn Virtual Appliance позволяет быстро развернуть виртуальную машину с уже настроенными компонентами. Образ предоставляется в формате OVF (Open Virtualization Format), который поддерживают такие вендоры, как VMWare, Oracle VirtualBox. Для Microsoft Hyper-v и KVM поставляются образы дисков виртуальной машины.

Примечание Для корректной работы виртуальной машины рекомендуется использовать минимум 8 Гб оперативной памяти и 2-ядерный виртуальный процессор. Гипервизор должен поддерживать работу 64-битных операционных систем.

Для начала работы с виртуальным образом выполните следующие шаги:

Наименование	Описание
Шаг 1. Скачайте образ и распакуйте	Скачайте последнюю версию виртуального образа с официального сайта https://www.usergate.com/ru .
Шаг 2. Импортируйте образ в свою систему виртуализации	Инструкцию по импорту образа вы можете посмотреть на сайтах VirtualBox и VMWare. Для Microsoft Hyper-v и KVM необходимо создать виртуальную машину и указать в качестве диска скачанный образ, после чего отключить службы интеграции в настройках созданной виртуальной машины.
Шаг 3. Настройте параметры виртуальной машины	Увеличьте размер оперативной памяти виртуальной машины. Используя свойства виртуальной машины, установите минимум 8Gb.
Шаг 4. Важно! Увеличьте размер диска виртуальной машины	Размер диска по умолчанию составляет 100Gb, что обычно недостаточно для хранения всех журналов и настроек. Используя свойства виртуальной машины, установите размер диска в 300Gb или более. Рекомендованный размер - 1000Gb или более.
Шаг 5. Настройте виртуальные сети	UserGate LogAn поставляется с двумя интерфейсами, назначенными в зоны: • Management — первый интерфейс виртуальной машины; • Trusted — второй интерфейс виртуальной машины.
Шаг 6. Выполните сброс к заводским настройкам	Запустите виртуальную машину LogAn. Во время загрузки выберите Support Menu и выполните Factory reset . Этот шаг крайне важен. Во время этого шага настраивает сетевые адаптеры и увеличивает размер раздела на жестком диске до полного размера диска, увеличенного в 4-м пункте.

Подключение к LogAn

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

Интерфейс port0 настроен на получение IP-адреса в автоматическом режиме (DHCP) и назначен в зону **Management**. Первоначальная настройка осуществляется через подключение администратора к веб-консоли через интерфейс port0.

Если нет возможности назначить адрес для Management-интерфейса в автоматическом режиме с помощью DHCP, то его можно явно задать, используя CLI (Command Line Interface). Более подробно об использовании CLI смотрите в главе [Интерфейс командной строки \(CLI\)](#).

Остальные интерфейсы отключены и требуют последующей настройки.

Первоначальная настройка требует выполнения следующих шагов:

Наименование	Описание
Шаг 1. Подключиться к интерфейсу управления	При наличии DHCP-сервера Подключить интерфейс port0 в сеть предприятия с работающим DHCP-сервером. Включить LogAn. После загрузки LogAn укажет IP-адрес, на который необходимо подключиться для дальнейшей активации продукта. Статический IP-адрес Включить LogAn. Используя CLI (Command Line Interface), назначить необходимый IP-адрес на интерфейс port0. Детали использования CLI смотрите в главе Интерфейс командной строки (CLI). Подключиться к веб-консоли LogAn по указанному адресу, он должен выглядеть примерно следующим образом: https://LogAn IP address:8010.
Шаг 2. Выбрать язык	Выбрать язык, на котором будет продолжена первоначальная настройка.
Шаг 3. Задать пароль	Задать логин и пароль для входа в веб-интерфейс управления.
Шаг 4. Зарегистрировать систему	Ввести ПИН-код для активации продукта и заполнить регистрационную форму. Для активации системы необходим доступ LogAn в Интернет. Если на данном этапе выполнить регистрацию не удастся, то ее следует повторить после настройки сетевых интерфейсов на шаге 8.
Шаг 5. Настроить зоны, IP-адреса интерфейсов, подключить UserGate LogAn в сеть предприятия	В разделе Интерфейсы включить необходимые интерфейсы, установить корректные IP-адреса, соответствующие вашим сетям, и назначить интерфейсы соответствующим зонам. Подробно об управлении интерфейсами читайте в главе Настройка интерфейсов. Система поставляется с предопределенными зонами: • Зона Management (сеть управления), интерфейс port0. • Зона Trusted (LAN). Предполагается, что через зону Trusted LogAn будет подключен в сеть, через которую шлюзы UserGate будут отсылать на него журналы, а также через которую LogAn получит доступ в Интернет. Для работы LogAn достаточно одного настроенного интерфейса. Разделение функций управления устройством и сбора данных на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием.
Шаг 6. Настроить шлюз в Интернет	В разделе Шлюзы указать IP-адрес шлюза в Интернет на интерфейсе, имеющим доступ в Интернет, как правило, это зона Trusted . Подробно о настройке шлюзов в Интернет читайте в главе Настройка шлюзов .
Шаг 7. Указать системные DNS-серверы	В разделе DNS укажите IP-адреса серверов DNS, вашего провайдера или серверов, используемых в вашей организации. Подробно об управлении DNS читайте в главе Раздел настройки .
Шаг 8. Зарегистрировать продукт (если не был зарегистрирован на шаге 4)	Зарегистрировать продукт с помощью ПИН-кода. Для успешной регистрации необходимо подключение к Интернету и выполнение предыдущих шагов. Более подробно о лицензировании продукта читайте в главе Лицензирование LogAn .
Шаг 9. Создать дополнительных администраторов (опционально)	В разделе Администраторы создать дополнительных администраторов системы, наделить их необходимыми полномочиями (ролями).

После выполнения вышеперечисленных действий LogAn готов к работе. Для более детальной настройки обратитесь к необходимым главам справочного руководства.

Развертывание программно-аппаратного комплекса

Documentation: ☒

Product: LogAn, SIEM

Version: 7.0.1, 7.1.0

В случае поставки решения в виде ПАК, программное обеспечение уже загружено и готово к первоначальной настройке. Перейдите к главе [Подключение к LogAn](#) для дальнейшей настройки.

Настройка LogAn

Раздел настройки

Documentation: ☒

Version: 7.0.1

Product: LogAn, SIEM

Раздел **Настройки** определяет базовые установки LogAn:

Наименование	Описание
Настройки интерфейса	Настройки интерфейса LogAn: • Часовой пояс, соответствующий вашему местоположению. Часовой пояс используется в расписаниях, применяемых в правилах, а также для корректного отображения времени и даты в отчетах, журналах и т.п. • Язык интерфейса по умолчанию — язык, который будет использоваться по умолчанию в консоли.
Настройка времени сервера	Настройка параметров установки точного времени: • Использовать NTP — использовать сервера NTP из указанного списка для синхронизации времени. • Основной сервер NTP — адрес основного сервера точного времени. Значение по умолчанию — pool.ntp.org • Запасной сервер NTP — адрес запасного сервера точного времени. • Время на сервере — позволяет установить время на сервере. Время должно быть указано в часовом поясе UTC.
Системные DNS-серверы	Укажите корректные IP-адреса серверов DNS в настройках.
Расписание скачивания обновлений	Настройка расписания скачивания обновлений ПО и библиотек. Также возможно проверить наличие обновлений вручную нажатием на Проверка обновлений .
Состояние сборщика логов	Отображается текущее состояние сервера LogAn: • Состояние — показывает текущее состояние сервиса статистики. • Версия устройства — версия LogAn.
Агент UserGate Management Center	Настройки для подключения устройства к центральной консоли управления, позволяющей управлять парком устройств LogAn из одной точки. • Включен/Выключен — включение или отключение управления с помощью UGMC. • Адрес UserGate Management Center — адрес сервера. • Код устройства — токен, требуемый для подключения к UGMC.

Управление устройством

Version: 7.0.1
Product: LogAn, SIEM
Documentation: ☒

Раздел **Управление устройством** определяет следующие установки LogAn:

- Диагностика;
- Операции с сервером;
- Резервное копирование;
- Экспорт и импорт настроек.

Диагностика

В данном разделе задаются параметры диагностики сервера, необходимые службе технической поддержки LogAn при решении возможных проблем.

Наименование	Описание
Детализация диагностики	• Off — ведение журналов диагностики отключено. • Error — журналировать только ошибки работы сервера. • Warning — журналировать только ошибки и предупреждения. • Info — журналировать только ошибки, предупреждения и дополнительную информацию. • Debug — максимум детализации. Рекомендуется установить значение параметра Детализация диагностики в Error (только ошибки) или Off (Отключено), если техническая поддержка UserGate не попросила вас установить иные значения. Любые значения, отличные от Error (только ошибки) или Off (Отключено), негативно влияют на производительность LogAn.
Журналы диагностики	• Скачать журналы — скачать диагностические журналы для передачи их в службу поддержки UserGate. • Очистить журналы — очистить содержимое журналов.
Удаленный помощник	• Включено/Отключено — включение/отключение режима удаленного помощника. Удаленный помощник позволяет инженеру технической поддержки UserGate, зная значения идентификатора и токена удаленного помощника, произвести безопасное подключение к серверу UserGate LogAn для диагностики и решения проблем. Для успешной активации удаленного помощника UserGate LogAn должен иметь доступ к серверу удаленного помощника компании UserGate по протоколу SSH. • Идентификатор удаленного помощника — полученное случайным образом значение. Уникально для каждого включения удаленного помощника. • Токен удаленного помощника — полученное случайным образом значение токена. Уникально для каждого включения удаленного помощника.

Операции с сервером

Данный раздел позволяет произвести следующие операции с сервером:

Наименование	Описание
Операции с сервером	• Перезагрузить — перезагрузка сервера LogAn. • Выключить — выключение сервера LogAn.
Обновления	Выбор канала обновлений ПО LogAn: • Стабильные — проверка наличия стабильных обновлений ПО. • Бета — проверка наличия экспериментальных обновлений.

LogAn в рамках подписки на модуль лицензии Security Update (подробно о лицензировании смотрите в разделе [Лицензирование LogAn](#)). При наличии обновлений в разделе **Управление устройством** отобразится соответствующее оповещение. Обновление продукта может занять довольно длительное время, рекомендуется планировать установку обновлений с учетом возможного времени простоя LogAn.

Для установки обновлений необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать файл резервного копирования	Создать резервную копию состояния LogAn, как это описано в разделе Системные утилиты . Данный шаг рекомендуется всегда выполнять перед применением обновлений, поскольку он позволит восстановить предыдущее состояние устройства в случае возникновения каких-либо проблем во время применения обновлений.
Шаг 2. Установить обновления	В разделе Управление устройством при наличии оповещения Доступны новые обновления нажать на ссылку Установить сейчас . Система установит скачанные обновления, по окончании установки LogAn будет перезагружен.

Управление резервным копированием

Данный раздел позволяет управлять резервным копированием UserGate: настройка правил экспорта конфигурации, создание резервной копии, восстановление устройства UserGate.

Для создания резервной копии необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать резервную копию	В разделе Управление устройством → Управление резервным копированием нажать Создание резервной копии. Система сохранит текущие настройки сервера под следующим именем: backup_PRODUCT_NODE-NAME_DATE.gpg, где <i>PRODUCT</i> — тип продукта: NGFW, LogAn, MC; <i>NODE-NAME</i> — имя узла UserGate; <i>DATE</i> — дата и время создания резервной копии в формате YYYY-MM-DD-HH-MM; время указывается в часовом поясе UTC. Процесс создания резервной копии может быть прерван нажатием кнопки Остановить. Запись о создании резервной копии отобразится в журнале событий устройства.

Для восстановления состояния устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Восстановить состояние устройства	В разделе Управление устройством → Управление резервным копированием нажать Восстановление из резервной копии и указать путь к ранее созданному файлу настроек для его загрузки на сервер. Восстановление будет предложено в консоли tty при перезагрузке устройства.

Дополнительно администратор может настроить сохранение файлов на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило экспорта конфигурации	В разделе Управление устройством → Управление резервным копированием нажать кнопку Добавить , указать имя и описание правила.

Наименование	Описание
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила Удаленный сервер указать параметры удаленного сервера: • Тип сервера — FTP или SSH; • Адрес сервера — IP-адрес сервера; • Порт — порт сервера; • Логин — учетная запись на удаленном сервере; • Пароль/Повторите пароль — пароль учетной записи; • Путь на сервере — путь на сервере, куда будут выгружены настройки. В случае использования SSH-сервера возможно использование авторизации по ключу. Для импорта или генерации ключа необходимо выбрать Настроить SSH-ключ и указать Сгенерировать ключи или Импортировать ключ. Важно! При повторном создании ключа существующий SSH-ключ будет удален. Публичный ключ должен находиться на SSH-сервере в директории пользовательских ключей <code>/home/user/.ssh/</code> в файле authorized_keys. При первоначальной настройке правила экспорта резервного копирования по SSH обязательна проверка соединения (кнопка Проверить соединение), при проверке соединения fingerprint помещается в <code>known_hosts</code>, без проверки файлы не будут отправляться. Важно! Если сменить сервер SSH или его переустановить, то файлы резервного копирования будут недоступны, так как fingerprint изменится — это защита от спуфинга.
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила Расписание указать необходимое время отправки настроек. В случае задания времени в crontab-формате, задайте его в следующем виде: (минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье) Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего); • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7; • Списки - это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23"; • Звездочка и тире используются 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".

Экспорт и импорт настроек

Администратор имеет возможность сохранить текущие настройки LogAn в файл и впоследствии восстановить эти настройки на этом же или другом сервере LogAn. В отличие от резервного копирования, экспорт/импорт настроек не сохраняет текущее состояние всех компонентов комплекса, сохраняются только текущие настройки.

Примечание Экспорт/импорт настроек не восстанавливает состояние интерфейсов и информацию о лицензии. После окончания процедуры импорта необходимо повторно зарегистрировать LogAn с помощью имеющегося ПИН-кода и настроить интерфейсы.

Для экспорта настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Экспорт настроек	В разделе Управление устройством → Экспорт и импорт настроек нажмите Экспорт и выберите Экспортировать все настройки или Экспортировать сетевые настройки. Система сохранит: • текущие настройки сервера под именем: logan_core-logan_core@nodename_version_YYYYMMDD_HHMMSS.bin • сетевые настройки под именем: network-logan_core-logan_core@nodename_version_YYYYMMDD_HHMMSS.bin nodename — имя узла LogAn; version — версия LogAn; YYYYMMDD_HHMMSS — дата и время выгрузки настроек в часовом поясе UTC. Например, logan_core-logan_core@ranreahattha_6.2.0.13494RS-1_20211227_091350.bin или network-logan_core-logan_core@ranreahattha_6.2.0.13494RS-1_20211227_091407.bin.

Для применения созданных ранее настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Импорт настроек	В разделе Управление устройством → Экспорт и импорт настроек нажать Импорт и указать путь к ранее созданному файлу настроек. Указанные настройки применятся к серверу, после чего сервер будет перезагружен

Дополнительно администратор может настроить сохранение настроек на внешние серверы (FTP, SSH) по расписанию. Для создания расписания выгрузки настроек необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать правило экспорта	В разделе Управление устройством → Экспорт и импорт настроек нажать кнопку Добавить , указать имя и описание правила.
Шаг 2. Указать параметры удаленного сервера	Во вкладке правила Удаленный сервер указать параметры удаленного сервера: • Тип сервера — FTP или SSH; • Адрес сервера — IP-адрес сервера; • Порт — порт сервера; • Логин — учетная запись на удаленном сервере; • Пароль/Повторите пароль — пароль учетной записи; • Путь на сервере — путь на сервере, куда будут выгружены настройки.
Шаг 3. Выбрать расписание выгрузки	Во вкладке правила Расписание указать необходимое время отправки настроек. В случае задания времени в CRONTAB-формате, задайте его в следующем виде: (минуты:0-59) (часы:0-23) (дни месяца:1-31) (месяц:1-12) (день недели:0-6, 0-воскресенье) Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего); • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7; • Списки - это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23"; • Звездочка и тире используются 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".

Администраторы

Version: 7.0.1, 7.1.0

Product: LogAn, SIEM

Documentation: 

Доступ к веб-консоли LogAn регулируется с помощью создания дополнительных учетных записей администраторов, назначения им профилей доступа, создания политики управления паролями администраторов и настройки доступа к веб-консоли на уровне разрешения сервиса в свойствах зоны сети.

Примечание При первоначальной настройке LogAn создается локальный суперпользователь Admin.

Для создания дополнительных учетных записей администраторов устройства необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать профиль доступа администратора	В разделе Администраторы → Профили администраторов нажать кнопку Добавить и указать необходимые настройки.
Шаг 2. Создать учетную запись администратора и назначить ей один из созданных ранее профилей администратора	В разделе Администраторы нажать кнопку Добавить и выбрать необходимый вариант: • Добавить локального администратора — создать локального пользователя, задать ему пароль доступа и назначить созданный ранее профиль доступа. • Добавить пользователя LDAP — добавить пользователя из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе Серверы аутентификации. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль. • Добавить группу LDAP — добавить группу пользователей из существующего домена. Для этого должен быть корректно настроен LDAP-коннектор в разделе Серверы аутентификации. При входе в консоль администрирования необходимо указывать имя пользователя в формате user@domain. Назначить созданный ранее профиль. • Добавить администратора с профилем аутентификации — создать пользователя, назначить созданный ранее профиль администратора и профиль аутентификации (необходимы корректно настроенные серверы аутентификации).

При создании профиля доступа администратора необходимо указать следующие параметры:

Наименование	Описание
Название	Название профиля.
Описание	Описание профиля.
Права доступа	Список объектов дерева веб-консоли, доступных для делегирования. В качестве доступа можно указать: • Нет доступа. • Чтение. • Чтение и запись.
Роли пользователей	Определяет роли пользователя для действия над инцидентами и правилами аналитики, назначаемые администраторам данного профиля. Более подробно о ролях смотрите в разделе Роли и ролевые разрешения пользователей .

Примечание Не следует путать роли и ролевые разрешения с правами доступа на определенные объекты в консоли управления. Права доступа дают возможность просматривать или изменять определенные объекты, например, инциденты, а роли и ролевые разрешения позволяют пользователю производить определенные действия с элементами объектов, например, создать инцидент, назначить ему исполнителя и т.п. Для полноценной работы пользователя в системе, как правило, требуется делегирование ему прав доступа и определенных ролевых разрешений.

Администратор LogAn может настроить дополнительные параметры защиты учетных записей администраторов, такие, как сложность пароля и блокировку учетной записи на определенное время при превышении количества неудачных попыток авторизации.

Для настройки этих параметров необходимо:

Наименование	Описание
Шаг 1. Настроить политику паролей	В разделе Администраторы → Администраторы нажать кнопку Настроить .
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • Сложный пароль — включает дополнительные параметры сложности пароля, задаваемые ниже, такие как — минимальная длина, минимальное число символов в верхнем регистре, минимальное число символов в нижнем регистре, минимальное число цифр, минимальное число специальных символов, максимальная длина блока из одного и того же символа. • Число неверных попыток аутентификации — количество неудачных попыток аутентификации администратора, после которых учетная запись заблокируется на Время блокировки. • Время блокировки — время, на которое блокируется учетная запись.

Примечание Дополнительные параметры защиты учетной записи администратора применимы только к локальным учетным записям. Если в качестве администратора устройства выбирается учетная запись из внешнего каталога (например, LDAP), то параметры защиты для такой учетной записи определяются этим внешним каталогом.

В разделе **Администраторы → Сессии администраторов** отображаются все администраторы, выполнившие вход в веб-консоль администрирования LogAp. При необходимости любую из сессий администраторов можно закрыть (сбросить).

Администратор может указать зоны, с которых будет возможен доступ к сервису веб-консоли (порт TCP 8010).

Примечание Не рекомендуется разрешать доступ к веб-консоли для зон, подключенных к неконтролируемым сетям, например, к сети Интернет.

Для разрешения сервиса веб-консоли для определенной зоны необходимо в свойствах зоны в разделе контроль доступа разрешить доступ к сервису **Консоль администрирования**. Более подробно о настройке контроля доступа к зонам можно прочитать в разделе [Настройка зон](#).

Управление сертификатами

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

LogAn использует защищенный протокол HTTPS для управления устройством. Для выполнения данной функции LogAn использует сертификат типа **SSL веб-консоли**.

Для того чтобы создать новый сертификат, необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать сертификат	Нажать на кнопку Создать в разделе Сертификаты .
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • Название — название сертификата, под которым он будет отображен в списке сертификатов. • Описание — описание сертификата. • Страна — страна, в которой выписывается сертификат. • Область или штат — область или штат, в котором выписывается сертификат. • Город — город, в котором выписывается сертификат. • Название организации — название организации, для которой выписывается сертификат. • Common name — имя сертификата. Рекомендуется использовать только символы латинского алфавита для совместимости с большинством браузеров. • E-mail — email вашей компании.
Шаг 3. Указать, для чего будет использован данный сертификат	После создания сертификата необходимо указать его роль в LogAn. Для этого необходимо выделить необходимый сертификат в списке сертификатов, нажать на кнопку Редактировать и указать тип сертификата — SSL веб-консоли. После этого LogAn перезагрузит сервис веб-консоли и предложит вам подключиться уже с использованием нового сертификата.

LogAn позволяет экспортировать созданные сертификаты и импортировать сертификаты, созданные на других системах, например, сертификат, выписанный доверенным удостоверяющим центром вашей организации.

Для экспорта сертификата необходимо:

Наименование	Описание
Шаг 1. Выбрать сертификат для экспорта	Выделить необходимый сертификат в списке сертификатов.
Шаг 2. Экспортировать сертификат	Выбрать тип экспорта: • Экспорт сертификата — экспортирует данные сертификата в der-формате без экспортирования приватного ключа сертификата. Используйте файл, полученный в результате экспорта сертификата для инспектирования SSL, для установки его в качестве локального удостоверяющего центра на компьютеры пользователей. • Экспорт CSR — экспортирует CSR сертификата, например, для подписи его удостоверяющим центром.

ПримечаниеРекомендуется сохранять сертификат для возможности его последующего восстановления.

ПримечаниеВ целях безопасности LogAn не разрешает экспорт приватных ключей сертификатов.

Для импорта сертификата необходимо иметь файлы сертификата и — опционально — приватного ключа сертификата и выполнить следующие действия:

Наименование	Описание
Шаг 1. Начать импорт	Нажать на кнопку Импорт .

Наименование	Описание
Шаг 2. Заполнить необходимые поля	Указать значения следующих полей: • Название — название сертификата, под которым он будет отображен в списке сертификатов. • Описание — описание сертификата. • Файл сертификата: файл, содержащий данные сертификата. • Приватный ключ: файл, содержащий приватный ключ сертификата. • Пароль для приватного ключа, если таковой требуется. • Цепочка сертификатов — файл, содержащий сертификаты вышестоящих центров сертификации, которые участвовали в создании сертификата (необязательное поле).

Серверы аутентификации

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

Серверы аутентификации - это внешние источники учетных записей пользователей для авторизации в веб-консоли управления UserGate Log Analyzer. LogAn поддерживает следующие серверы аутентификации: LDAP-коннектор, RADIUS и TACACS+.

LDAP-коннектор

LDAP-коннектор позволяет:

- Получать информацию о пользователях и группах Active Directory или других LDAP-серверов. Поддерживается работа с LDAP-сервером FreeIPA.
- Осуществлять авторизацию администраторов LogAn через домены Active Directory/FreeIPA.

Для создания LDAP-коннектора необходимо нажать на кнопку **Добавить**, выбрать **Добавить LDAP-коннектор** и указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает использование данного сервера аутентификации.
Название	Название сервера аутентификации.
SSL	Определяет, требуется ли SSL-соединение для подключения к LDAP-серверу.
Доменное имя LDAP или IP-адрес	IP-адрес контроллера домена, FQDN контроллера домена или FQDN домена (например, test.local). Если указан FQDN, то UserGate получит адрес контроллера домена с помощью DNS-запроса. Если указан FQDN домена, то при отключении основного контроллера домена, UserGate будет использовать резервный.
Bind DN («login»)	Имя пользователя, которое необходимо использовать для подключения к серверу LDAP. Имя необходимо использовать в формате DOMAIN\username или username@domain. Данный пользователь уже должен быть заведен в домене
Пароль	Пароль пользователя для подключения к домену.
Домены LDAP	Список доменов, которые обслуживаются указанным контроллером домена, например, в случае дерева доменов или леса доменов Active Directory. Здесь же можно указать короткое netbios имя домена.
Пути поиска	Список путей в сервере LDAP, начиная с которых система будет осуществлять поиск пользователей и групп. Необходимо указывать полное имя, например, ou=Office,dc=example,dc=com.

После создания сервера необходимо проверить корректность параметров, нажав на кнопку **Проверить соединение**. Если параметры указаны верно, система сообщит об этом либо укажет на причину невозможности соединения.

Настройка LDAP-коннектора завершена. Для входа в консоль пользователям LDAP необходимо указывать имя в формате:

`domain\user/system` или `user@domain/system`

Сервер аутентификации RADIUS

Сервер аутентификации RADIUS позволяет производить авторизацию пользователей в веб-консоли UserGate, который выступает в роли RADIUS-клиента. При авторизации через RADIUS-сервер UserGate посылает на серверы RADIUS информацию с именем и паролем пользователя, а RADIUS-сервер отвечает, успешно прошла аутентификация или нет.

Для добавления сервера аутентификации RADIUS необходимо нажать **Добавить**, выбрать **Добавить RADIUS-сервер** и указать следующие параметры:

Наименование	Описание
Включено	Включение/отключение использования данного сервера аутентификации.

Наименование	Описание
Название	Название сервера аутентификации RADIUS.
Описание	Описание сервера (опционально).
Секрет	Общий ключ, используемый протоколом RADIUS для аутентификации.
Адреса	Указание IP-адреса сервера и UDP-порта, на котором сервер RADIUS слушает запросы на аутентификацию (по умолчанию, 1812).

Для авторизации пользователей в веб-интерфейсе UserGate с помощью сервера RADIUS необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей читайте в разделе [Профили аутентификации](#).

Сервер аутентификации TACACS+

Сервер TACACS+ позволяет производить авторизацию пользователей в консоли администрирования UserGate. При использовании сервера UserGate передаёт на серверы аутентификации информацию с именем и паролем пользователя, после чего серверы TACACS+ отвечают, успешно прошла аутентификация или нет.

Для добавления сервера аутентификации TACACS+ необходимо нажать **Добавить**, выбрать **Добавить TACACS+ сервер** и указать следующие параметры:

Наименование	Описание
Включено	Включение/отключение использования данного сервера аутентификации.
Название	Название сервера аутентификации TACACS+.
Описание	Описание сервера (опционально).
Секретный ключ	Общий ключ, используемый протоколом TACACS+ для аутентификации.
Адрес	IP-адрес сервера TACACS+.
Порт	UDP-порт, на котором сервер TACACS+ слушает запросы на аутентификацию.
Использовать одно TCP-соединение	Использовать одно TCP-соединение для работы с сервером TACACS+.
Таймаут (сек)	Время ожидания сервера TACACS+ для получения аутентификации. По умолчанию 4 секунды.

Для авторизации пользователей в веб-интерфейсе UserGate с помощью сервера TACACS+ необходимо настроить профиль аутентификации. Подробнее о создании и настройке профилей читайте в разделе [Профили аутентификации](#).

Профили аутентификации

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

Профиль позволяет определить набор способов авторизации пользователей в консоли администрирования UserGate. При создании или настройке профиля достаточно указать:

Наименование	Описание
Название	Название профиля аутентификации.
Описание	Описание профиля (опционально).
Методы аутентификации	Методы аутентификации пользователей, настроенные ранее: LDAP-коннектор, серверы аутентификации RADIUS, TACACS+.

Роли и ролевые разрешения пользователей

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

Роль пользователя - это набор ролевых разрешений. Ролевое разрешение - это возможность администратору совершать определенные действия, например, добавлять или удалять вложение из созданного инцидента, создавать правило срабатывания, создать или закрыть инцидент и т.д. Роли назначаются профилям администраторов, которые присваиваются администраторам. Подробно о создании администраторов и их профилей смотрите в разделе [Администраторы](#).

Чтобы создать роль и назначить ей определенные разрешения необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создать роль	В разделе Роли пользователей нажать на кнопку Добавить , дать название и описание создаваемой роли.
Шаг 2. Добавить в созданную роль необходимые разрешения	В разделе Ролевые разрешения выбрать необходимое разрешение и с помощью кнопки Добавить добавить в него созданную ранее роль.

Для пользователей могут быть указаны следующие ролевые разрешения.

Наименование	Описание
Назначаемый пользователь	Пользователь с этим разрешением может быть назначен на инцидент. Ответственный за инцидент может быть указан при создании или редактировании инцидента.
Назначение инцидентов	Возможность назначать пользователей на инциденты. Указать ответственного можно при создании или редактировании инцидента.
Закрытие инцидента	Возможность закрыть инцидент. Часто бывает полезно, когда разработчики разрешают инциденты, а тестировщики закрывают их. Закрыть инцидент можно во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента). Закрытие инцидента возможно только из состояний, для которых в схеме инцидента настроен переход в состояние Закрыт . Подробнее читайте в Настройках инцидентов .
Создание инцидентов	Возможность создавать инциденты. Инциденты могут быть созданы во вкладке Инциденты → Журнал инцидентов или автоматически при срабатывании правила аналитики. О создании инцидентов подробнее читайте в разделе Создание инцидентов безопасности .
Изменение инцидента	Возможность изменять инциденты. Редактирование инцидентов доступно во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента). Подробнее читайте в разделе Подробности инцидента .
Переоткрытие инцидента	Возможность переоткрывать инциденты. Заново открыть инцидент можно во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента).
Редактирование наблюдателей	Возможность добавлять и удалять наблюдателей. Пользователи для наблюдения за инцидентом могут быть указаны при создании или редактировании инцидента.
Оставление комментариев	Возможность комментировать инциденты. Комментирование инцидентов возможно во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента) в разделе Активность .

Наименование	Описание
Удаление любых комментариев	Возможность удалять любые комментарии к инцидентам. Комментарии к инциденту можно посмотреть во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента) в разделе Активность.
Удаление собственных комментариев	Возможность удалять собственные комментарии к инцидентам. Комментарии к инциденту можно посмотреть во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента) в разделе Активность.
Редактирование любых комментариев	Возможность редактировать любые комментарии к инцидентам. Комментарии к инциденту можно посмотреть во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента) в разделе Активность.
Редактирование своих комментариев	Возможность редактировать свои комментарии к инцидентам. Комментарии к инциденту можно посмотреть во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента) в разделе Активность.
Создание вложений	Возможность добавлять вложения к инцидентам. Вложения к инциденту можно добавить во вкладке Инциденты при создании инцидента или его редактировании. Вложения отображены во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента) в разделе Вложения.
Удаление любых вложений	Возможность удалять любые вложения. Вложения к инциденту отображены во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента) в разделе Вложения.
Удаление своих вложений	Возможность удалять свои вложения. Вложения к инциденту отображены во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента) в разделе Вложения.
Редактирование улик	Возможность создания и редактирования улик. Улики могут быть добавлены во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента) в разделе Улики. Подробнее об уликах читайте в разделе Подробнее инцидента.
Обновление обогащений	Возможность обновлять/запрашивать обогащения улик. Список внешних сервисов обогащений доступен во вкладке Настройки в разделе Библиотеки → Внешние сервисы обогащений. Подробнее о внешних сервисах обогащений читайте в разделе Внешние сервисы обогащений.
Создание отчёта	Возможность создавать, загружать и посылать отчёты инцидентов. Создание отчётов инцидентов доступно во вкладке Инциденты → INC-N:Название инцидента (где N - порядковый номер инцидента). Подробнее читайте в разделе Подробнее инцидента.
Добавление журналов к инциденту	Возможность добавлять журналы к инциденту. Журналы могут быть добавлены во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента) в разделе Журналы. Подробнее о журналах читайте в разделе Поиск; о срабатываниях - в разделе Срабатывания.
Удалить все срабатывания/журналы из инцидента	Возможность удаления всех срабатываний/журналов из инцидента. Срабатывания и журналы отображены во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента) в соответствующих разделах Срабатывания и Журналы. Подробнее о журналах читайте в разделе Поиск; о срабатываниях - в разделе Срабатывания.

Наименование	Описание
Удаление собственных срабатываний, журналов к инцидентам	Возможность удалять собственные срабатывания/журналы к инцидентам. Срабатывания и журналы отображены во вкладке Инциденты → <INC-N:Название инцидента> (где N - порядковый номер инцидента) в соответствующих разделах Срабатывания и Журналы. Подробнее о журналах читайте в разделе Поиск; о срабатываниях - в разделе Срабатывания.
Создание схемы инцидента	Возможность создавать схемы инцидентов. Схемы инцидентов доступны во вкладке Настройки в разделе Настройка инцидентов → Схема инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Редактирование схемы инцидента	Возможность редактировать схемы инцидентов. Схемы инцидентов доступны во вкладке Настройки в разделе Настройка инцидентов → Схема инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Удаление схемы инцидента	Возможность удалять схемы инцидентов. Схемы инцидентов доступны во вкладке Настройки в разделе Настройка инцидентов → Схема инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Установка схемы инцидентов по умолчанию	Возможность установки схем инцидентов по умолчанию. В UserGate LogAn создана одна схема инцидента по умолчанию; доступна во вкладке Настройки в разделе Настройка инцидентов → Схема инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Создание состояния инцидента	Возможность создавать состояния инцидентов. Список состояний инцидентов отображён во вкладке Настройки в разделе Настройка инцидентов → Состояния инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Редактирование состояния инцидента	Возможность редактировать состояния инцидентов. Список состояний инцидентов отображён во вкладке Настройки в разделе Настройка инцидентов → Состояния инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Удаление состояния инцидента	Возможность удалять состояния инцидентов. Список состояний инцидентов отображён во вкладке Настройки в разделе Настройка инцидентов → Состояния инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Создание типа инцидента	Возможность создавать типы инцидентов. Типы инцидентов доступны во вкладке Настройки в разделе Настройка инцидентов → Типы инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Редактирование типа инцидента	Возможность редактировать типы инцидентов. Типы инцидентов доступны во вкладке Настройки в разделе Настройка инцидентов → Типы инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Удаление типа инцидента	Возможность удалять типы инцидентов. Типы инцидентов доступны во вкладке Настройки в разделе Настройка инцидентов → Типы инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Создание решения инцидента	Возможность создавать решения инцидентов. Список решений инцидентов отображён во вкладке Настройки в разделе Настройка инцидентов → Решения инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Редактирование решения инцидента	Возможность редактировать решения инцидентов. Список решений инцидентов отображён во вкладке Настройки в разделе Настройка инцидентов → Решения инцидентов. Подробнее читайте в разделе Настройки инцидентов.

Наименование	Описание
Удаление решения инцидентов	Возможность удалять решения инцидентов. Список решений инцидентов отображён во вкладке Настройки в разделе Настройка инцидентов → Решения инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Создание правила аналитики	Возможность создавать правила аналитики. Правила аналитики могут быть созданы во вкладке Аналитика → Правила аналитики. Подробнее читайте в разделе Аналитика.
Удаление правила аналитики	Возможность удалять правила аналитики. Правила аналитики отображены во вкладке Аналитика → Правила аналитики. Подробнее читайте в разделе Аналитика.
Редактирование правила аналитики	Возможность редактировать правила аналитики. Правила аналитики отображены во вкладке Аналитика → Правила аналитики. Подробнее читайте в разделе Аналитика.
Включение/выключение правила аналитики	Возможность включать/выключать правила аналитики. Правила аналитики отображены во вкладке Аналитика → Правила аналитики. Подробнее читайте в разделе Аналитика.
Запуск правила аналитики	Возможность запустить правило аналитики не в режиме реального времени. Правила аналитики отображены во вкладке Аналитика → Правила аналитики. Подробнее читайте в разделе Аналитика.
Создание действия реагирования	Возможность создавать действия реагирования. Действия реагирования могут быть созданы во вкладке Аналитика → Действия реагирования. Подробнее читайте в разделе Действия реагирования.
Редактирование действия реагирования	Возможность редактировать действия реагирования. Действия реагирования отображены во вкладке Аналитика → Действия реагирования. Подробнее читайте в разделе Действия реагирования.
Удаление действия реагирования	Возможность удалять действия реагирования. Действия реагирования отображены во вкладке Аналитика → Действия реагирования. Подробнее читайте в разделе Действия реагирования.
Включение/выключение действия реагирования	Возможность включать/выключать действия реагирования. Действия реагирования отображены во вкладке Аналитика → Действия реагирования. Подробнее читайте в разделе Действия реагирования.
Создание сенсора UserGate	Возможность создавать сенсоры UserGate. Сенсоры UserGate могут быть созданы во вкладке Настройки в разделе Сенсоры → Сенсоры UserGate. Подробнее читайте в разделе Сенсоры UserGate.
Редактирование сенсора UserGate	Возможность редактировать сенсоры UserGate. Сенсоры UserGate, доступны во вкладке Настройки в разделе Сенсоры → Сенсоры UserGate. Подробнее читайте в разделе Сенсоры UserGate.
Включение/выключение сенсора UserGate	Возможность включать/выключать сенсоры UserGate. Сенсоры UserGate доступны во вкладке Настройки в разделе Сенсоры → Сенсоры UserGate. Подробнее читайте в разделе Сенсоры UserGate.

Наименование	Описание
Удаление сенсора UserGate	Возможность удалять сенсоры UserGate. Сенсоры UserGate доступны во вкладке Настройки в разделе Сенсоры → Сенсоры UserGate . Подробнее читайте в разделе Сенсоры UserGate.
Создание сенсора SNMP	Возможность создавать сенсоры SNMP. Сенсоры SNMP могут быть созданы во вкладке Настройки в разделе Сенсоры → Сенсоры SNMP . Подробнее читайте в разделе Сенсоры SNMP.
Редактирование сенсора SNMP	Возможность редактировать сенсоры SNMP. Сенсоры SNMP доступны во вкладке Настройки в разделе Сенсоры → Сенсоры SNMP . Подробнее читайте в разделе Сенсоры SNMP.
Включение/выключение сенсора SNMP	Возможность включать/выключать сенсоры SNMP. Сенсоры SNMP доступны во вкладке Настройки в разделе Сенсоры → Сенсоры SNMP . Подробнее читайте в разделе Сенсоры SNMP.
Удаление сенсора SNMP	Возможность удалять сенсоры SNMP. Сенсоры SNMP доступны во вкладке Настройки в разделе Сенсоры → Сенсоры SNMP . Подробнее читайте в разделе Сенсоры SNMP.
Создание сенсора WMI	Возможность создавать сенсоры WMI. Сенсоры WMI могут быть созданы во вкладке Настройки в разделе Сенсоры → Сенсоры WMI . Подробнее читайте в разделе Сенсоры WMI.
Редактирование сенсора WMI	Возможность редактировать сенсоры WMI. Сенсоры WMI доступны во вкладке Настройки в разделе Сенсоры → Сенсоры WMI . Подробнее читайте в разделе Сенсоры WMI.
Включение/выключение сенсора WMI	Возможность включать/выключать сенсоры WMI. Сенсоры WMI доступны во вкладке Настройки в разделе Сенсоры → Сенсоры WMI . Подробнее читайте в разделе Сенсоры WMI.
Удаление сенсора WMI	Возможность удалять сенсоры WMI. Сенсоры WMI доступны во вкладке Настройки в разделе Сенсоры → Сенсоры WMI . Подробнее читайте в разделе Сенсоры WMI.
Добавление SNMP MIB файла	Возможность добавлять SNMP MIB файлы. MIB файлы могут быть добавлены во вкладке Настройки в разделе Сенсоры → Управление SNMP MIB . Подробнее читайте в разделе Управление SNMP MIB.
Удаление SNMP MIB файла	Возможность удалять SNMP MIB файлы. MIB файлы отображены во вкладке Настройки в разделе Сенсоры → Управление SNMP MIB . Подробнее читайте в разделе Управление SNMP MIB.
Создание правила Syslog	Возможность создавать правила Syslog. Правила Syslog могут быть созданы во вкладке Настройки в разделе Сборщик логов → Syslog .
Удаление правила Syslog	Возможность удалять правила Syslog. Правила Syslog отображены во вкладке Настройки в разделе Сборщик логов → Syslog .
Редактирование правил и коннектора Syslog	Возможность редактировать правила Syslog и настраивать Syslog. Созданные правила Syslog доступны во вкладке Настройки в разделе Сборщик логов → Syslog .

Наименование	Описание
Включение/выключение правила Syslog	Возможность включать/выключать правила Syslog. Правила Syslog доступны во вкладке Настройки в разделе Сборщик логов → Syslog.
Создание группы email	Возможность создавать почтовые адреса/почтовые группы. Почтовые адреса и группы почтовых адресов могут быть созданы во вкладке Настройки в разделе Библиотеки → Почтовые адреса. Подробнее читайте в разделе Почтовые адреса.
Редактирование группы email	Возможность редактировать почтовые адреса/почтовые группы. Почтовые адреса и группы почтовых адресов доступны во вкладке Настройки в разделе Библиотеки → Почтовые адреса. Подробнее читайте в разделе Почтовые адреса.
Удаление группы email	Возможность удалять почтовые адреса/почтовые группы. Почтовые адреса и группы почтовых адресов доступны во вкладке Настройки в разделе Библиотеки → Почтовые адреса. Подробнее читайте в разделе Почтовые адреса.
Создание группы номеров телефонов	Возможность создавать номера телефонов/группы телефонных номеров. Номера телефонов и группы телефонных адресов могут быть созданы во вкладке Настройки в разделе Библиотеки → Почтовые адреса. Подробнее читайте в разделе Почтовые адреса.
Редактирование группы номеров телефонов	Возможность редактировать номера телефонов/группы телефонных номеров. Номера телефонов и группы телефонных адресов могут доступны во вкладке Настройки в разделе Библиотеки → Почтовые адреса. Подробнее читайте в разделе Почтовые адреса.
Удаление группы номеров телефонов	Возможность удалять номера телефонов/группы телефонных номеров. Номера телефонов и группы телефонных адресов могут доступны во вкладке Настройки в разделе Библиотеки → Почтовые адреса. Подробнее читайте в разделе Почтовые адреса.
Создание профиля оповещения	Возможность создавать профиль оповещения. Во вкладке Настройки в разделе Библиотеки → Профили оповещений могут быть созданы два типа профилей: SMPP и SMTP. Подробнее о профилях оповещений читайте в разделе Профили оповещений.
Редактирование профиля оповещения	Возможность редактировать профиль оповещения. Список профилей доступен во вкладке Настройки в разделе Библиотеки → Профили оповещений. Подробнее о профилях оповещений читайте в разделе Профили оповещений.
Удаление профиля оповещения	Возможность редактировать профиль оповещения. Список профилей доступен во вкладке Настройки в разделе Библиотеки → Профили оповещений. Подробнее о профилях оповещений читайте в разделе Профили оповещений.
Создание категории сбрасывания	Возможность создавать категории сбрасывания. Категории сбрасываний могут быть созданы во вкладке Настройки в разделе Библиотеки → Категории сбрасываний. Подробнее о категориях сбрасываний читайте в разделе Категории сбрасываний.
Редактирование категории сбрасывания	Возможность редактировать категории сбрасывания. Список категорий сбрасываний доступен во вкладке Настройки в разделе Библиотеки → Категории сбрасываний. Подробнее о категориях сбрасываний читайте в разделе Категории сбрасываний.
Удаление категории сбрасывания	Возможность удалять категории сбрасывания. Список категорий сбрасываний доступен во вкладке Настройки в разделе Библиотеки → Категории сбрасываний. Подробнее о категориях сбрасываний читайте в разделе Категории сбрасываний.

Наименование	Описание
Редактирование настройки обогащения	Возможность редактировать настройки обогащений. Список внешних сервисов обогащения доступен во вкладке Настройки в разделе Библиотеки → Внешние сервисы обогащений. Подробнее о внешних сервисах обогащений читайте в разделе Внешние сервисы обогащений.
Включение/выключение сервиса обогащения	Возможность включать/выключать сервисы обогащений. Список внешних сервисов обогащения доступен во вкладке Настройки в разделе Библиотеки → Внешние сервисы обогащений. Подробнее о внешних сервисах обогащений читайте в разделе Внешние сервисы обогащений.

После создания роли, она может быть использована для назначения в профили администраторов.

Расширение системного раздела

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

Для расширения системного раздела с сохранением конфигурации и данных узла UserGate необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Добавить дополнительный виртуальный диск.	Средствами гипервизора добавить новый диск необходимого размера в свойствах виртуальной машины UserGate.
Шаг 2. Расширить размер раздела в системных утилитах.	В меню загрузки узла UserGate войти в раздел Support menu . В открывшемся разделе выбрать Expand data partition и запустить процесс расширения раздела.
Шаг 3. Проверить размер системного раздела.	После завершения процесса расширения загрузить узел и в разделе Дашборд → Диски проверить размер системного раздела.

Офлайн операции с сервером

Офлайн операции с сервером

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

Некоторые операции с сервером проводятся, когда сервер не выполняет свою функцию и находится в офлайн режиме. Для выполнения таких операций необходимо во время загрузки сервера выбрать раздел меню **Support menu** и затем одну из требуемых операций. Для получения доступа к этому меню необходимо подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB (при наличии соответствующих разъемов на устройстве) или, используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к LogAn. Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.

Во время загрузки администратор может выбрать один из нескольких пунктов загрузки в boot-меню:

Наименование	Описание
UGOS LOGAN	Загрузка UserGate с выводом диагностической информации о загрузке в последовательный порт.
UGOS LOGAN (failsafe)	Загрузка UserGate в упрощённом видео режиме.
Support menu	Войти в раздел системных утилит с выводом информации в консоль tty1 (монитор).
Restore previous version	Раздел доступен после обновления или создания резервной копии.

Раздел системных утилит (Support menu) позволяет выполнить следующие действия:

Наименование	Описание
Check filesystems	Запуск проверки файловой системы устройства на наличие ошибок и их автоматическое исправление.
Expand data partition	Увеличение раздела для хранения данных на весь выделенный диск. Эта операция обычно используется после увеличения дискового пространства, выделенного гипервизором для виртуальной машины UserGate. Данные и настройки UserGate не сбрасываются.
Create backup	Создать полную копию диска UserGate на внешний USB носитель. Все данные на внешнем носителе будут удалены.
Restore from backup	Восстановление UserGate с внешнего USB носителя.
Factory reset	Сброс состояния UserGate к первоначальному состоянию системы. Все данные и настройки будут утеряны.
Exit	Выход и перезагрузка устройства.

Настройка зон

Documentation: ☒
Product: LogAn
Version: 6.1.9, 7.0.1

Зона в LogAn — это логическое объединение сетевых интерфейсов. Политики безопасности UserGate LogAn используют зоны интерфейсов, а не непосредственно интерфейсы.

Рекомендуется объединять интерфейсы в зоне на основе их функционального назначения, например, зона LAN-интерфейсов, зона интернет-интерфейсов, зона интерфейсов управления.

По умолчанию LogAn поставляется со следующими зонами:

Наименование	Описание
Management	Зона для подключения доверенных сетей, из которых разрешено управление LogAn.
Trusted	Зона для подключения доверенных сетей, например, LAN-сетей. Предполагается, что через зону Trusted LogAn будет подключен в сеть, через которую межсетевые экраны UserGate будут отсылать на него журналы, а также через которую LogAn получит доступ в Интернет.

Для работы LogAn достаточно одного настроенного интерфейса. Разделение функций управления устройством и сбора данных на разные сетевые интерфейсы рекомендовано для обеспечения безопасности, но не является жестким требованием.

Администраторы LogAn могут изменять настройки зон, созданных по умолчанию, а также создавать дополнительные зоны.

ПримечаниеМожно создать не более 255 зон.

Для создания зоны необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать зону	Нажать на кнопку Добавить и дать название зоне.
Шаг 2. Настроить параметры защиты зоны от DoS (опционально)	Указать параметры защиты зоны от сетевого флуда для протоколов TCP (SYN-flood), UDP, ICMP: • Порог уведомления — при превышении количества запросов с одного IP-адреса над указанным значением происходит запись события в системный журнал. • Порог отбрасывания пакетов — при превышении количества запросов с одного IP-адреса над указанным значением UserGate LogAn начинает отбрасывать пакеты, поступившие с этого IP-адреса, и записывает данное событие в системный журнал. Рекомендованные значения для порога уведомления - 300 запросов в секунду, для порога отбрасывания пакетов — 600 запросов в секунду. Исключения защиты от DoS — позволяет указать список IP-адресов серверов, которые необходимо исключить из защиты. Это может быть полезно, например, для шлюзов UserGate, которые могут слать большой объем данных на сервера LogAn.
Шаг 3. Настроить параметры контроля доступа зоны (опционально)	Указать предоставляемые LogAn сервисы, которые будут доступны клиентам, подключенным к данной зоне. Для зон, подключенных к неконтролируемым сетям, таким, как интернет, рекомендуется отключить все сервисы. Сервисы: • Ping — позволяет пинговать LogAn. • SNMP — доступ LogAn по протоколу SNMP (UDP 161). • XML-RPC для управления — позволяет управлять продуктом по API (TCP 4041). • Консоль администрирования — доступ к веб-консоли управления (TCP 8010). • CLI по SSH — доступ к серверу для управления им с помощью CLI (command line interface), порт TCP 2200. • Log Analyzer — сервис анализатора журналов LogAn. Необходимо разрешить на зонах, с которых LogAn будет получать данные от серверов UserGate (TCP 22711 или 22699 для устройств с ПО версии ниже 7). Подробнее о требованиях сетевой доступности читайте в приложении: Требования к сетевому окружению.

Наименование	Описание
Шаг 4. Настроить параметры защиты от IP-спуфинг атак (опционально)	Атаки на основе IP-спуфинга позволяют передать пакет из одной сети, например, из Trusted, в другую, например, в Management. Для этого атакующий подменяет IP-адрес источника на предполагаемый адрес необходимой сети. В таком случае ответы на этот пакет будут пересылаться на внутренний адрес. Для защиты от подобных атак администратор может указать диапазоны IP-адресов, адреса источников которых допустимы в выбранной зоне. Сетевые пакеты с адресами источников отличных от указанных будут отброшены. С помощью флага Инвертировать администратор может указать адреса источников, которые не могут быть получены на интерфейсах данной зоны. В этом случае будут отброшены пакеты с указанными диапазонами IP-адресов источников. Например, можно указать диапазоны "серых" IP-адресов 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0./16 и включить опцию Инвертировать.

Настройка интерфейсов

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

Раздел **Интерфейсы** отображает все физические и виртуальные интерфейсы, имеющиеся в системе, позволяет менять их настройки и добавлять VLAN и бонд-интерфейсы.

Кнопка **Редактировать** позволяет изменять параметры сетевого интерфейса:

- включить или отключить интерфейс;
- указать тип интерфейса — Layer 3;
- назначить зону интерфейсу;
- изменить физические параметры интерфейса — MAC-адрес и размер MTU;
- выбрать тип присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

Кнопка **Добавить** позволяет добавить следующие типы логических интерфейсов:

- VLAN;
- Бонд.

Объединение интерфейсов в бонд

С помощью кнопки **Добавить бонд-интерфейс** администратор может объединить несколько физических интерфейсов в один логический агрегированный интерфейс для повышения пропускной способности или для отказоустойчивости канала. При создании бонда необходимо указать следующие параметры:

Наименование	Описание
Вкл	Включает бонд.
Название	Название бонда.
Зона	Зона, к которой принадлежит бонд.
Интерфейсы	Один или более интерфейсов, которые будут использованы для построения бонда.

Наименование	Описание
Режим	Режим работы бонда должен совпадать с режимом работы на том устройстве, куда подключается бонд. Может быть: • Round robin. Пакеты отправляются последовательно, начиная с первого доступного интерфейса и заканчивая последним. Эта политика применяется для балансировки нагрузки и отказоустойчивости. • Active backup. Только один сетевой интерфейс из объединенных будет активным. Другой интерфейс может стать активным только в том случае, когда упадет текущий активный интерфейс. При такой политике MAC-адрес бонд-интерфейса виден снаружи только через один сетевой порт, во избежание появления проблем с коммутатором. Эта политика применяется для отказоустойчивости. • XOR. Передача распределяется между сетевыми картами используя формулу: [(«MAC-адрес источника» XOR «MAC-адрес назначения») по модулю «число интерфейсов»]. Получается, одна и та же сетевая карта передает пакеты одним и тем же получателям. Опционально распределение передачи может быть основано и на политике «xmit_hash». Политика XOR применяется для балансировки нагрузки и отказоустойчивости. • Broadcast. Передает все на все сетевые интерфейсы. Эта политика применяется для отказоустойчивости. • IEEE 802.3ad — режим работы, установленный по умолчанию, поддерживается большинством сетевых коммутаторов. Создаются агрегированные группы сетевых карт с одинаковой скоростью и дуплексом. При таком объединении передача задействует все каналы в активной агрегации согласно стандарту IEEE 802.3ad. Выбор, через какой интерфейс отправлять пакет, определяется политикой; по умолчанию используется XOR-политика, можно также использовать «xmit_hash» политику. • Adaptive transmit load balancing. Исходящий трафик распределяется в зависимости от загруженности каждой сетевой карты (определяется скоростью загрузки). Не требует дополнительной настройки на коммутаторе. Входящий трафик приходит на текущую сетевую карту. Если она выходит из строя, то другая сетевая карта берет себе MAC-адрес вышедшей из строя карты. • Adaptive load balancing. Включает в себя предыдущую политику плюс осуществляет балансировку входящего трафика. Не требует дополнительной настройки на коммутаторе. Балансировка входящего трафика достигается путем ARP-переговоров. Драйвер перехватывает ARP-ответы, отправляемые с локальных сетевых карт наружу, и переписывает MAC-адрес источника на один из уникальных MAC-адресов сетевой карты, участвующей в объединении. Таким образом, различные пиры используют различные MAC-адреса сервера. Балансировка входящего трафика распределяется последовательно (round-robin) между интерфейсами.
MII monitoring period (мсек)	Устанавливает периодичность MII-мониторинга в миллисекундах. Определяет, как часто будет проверяться состояние линии на наличие отказов. Значение по умолчанию — 0 — отключает MII-мониторинг.
Down delay (мсек)	Определяет время (в миллисекундах) задержки перед отключением интерфейса, если произошел сбой соединения. Эта опция действительна только для мониторинга MII (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
Up delay (мсек)	Задаёт время задержки в миллисекундах, перед тем как поднять канал при обнаружении его восстановления. Этот параметр возможен только при MII-мониторинге (miimon). Значение параметра должно быть кратным значениям miimon. Если оно не кратно, то округлится до ближайшего кратного значения. Значение по умолчанию 0.
LACP rate	Определяет, с каким интервалом будут передаваться партнером LACPDU-пакеты в режиме 802.3ad. Возможные значения: • Slow — запрос партнера на передачу LACPDU-пакетов каждые 30 секунд. • Fast — запрос партнера на передачу LACPDU-пакетов каждую 1 секунду.
Failover MAC	Определяет, как будут прописываться MAC-адреса на объединенных интерфейсах в режиме active-backup при переключении интерфейсов. Обычным поведением является одинаковый MAC-адрес на всех интерфейсах. Возможные значения: • Отключено — устанавливает одинаковый MAC-адрес на всех интерфейсах во время переключения. • Active — MAC-адрес на бонд-интерфейсе будет всегда таким же, как на текущем активном интерфейсе. MAC-адреса на резервных интерфейсах не изменяются. MAC-адрес на бонд-интерфейсе меняется во время обработки отказа. • Follow — MAC-адрес на бонд-интерфейсе будет таким же, как на первом интерфейсе, добавленном в объединение. На втором и последующем интерфейсе этот MAC не устанавливается, пока они в резервном режиме. MAC-адрес прописывается во время обработки отказа, когда резервный интерфейс становится активным, он принимает новый MAC (тот, что на бонд-интерфейсе), а старому активному интерфейсу прописывается MAC, который был на текущем активном.

Наименование	Описание
Xmit hash policy	Определяет хэш-политику передачи пакетов через объединенные интерфейсы в режиме XOR или IEEE 802.3ad. Возможные значения: • Layer 2 — использует только MAC-адреса для генерации хэша. При этом алгоритме трафик для конкретного сетевого хоста будет отправляться всегда через один и тот же интерфейс. Алгоритм совместим с IEEE 802.3ad. • Layer 2+3 — использует как MAC-адреса, так и IP-адреса для генерации хэша. Алгоритм совместим с IEEE 802.3ad. • Layer 3+4 — используются IP-адреса и протоколы транспортного уровня (TCP или UDP) для генерации хэша. Алгоритм не всегда совместим с IEEE 802.3ad, так как в пределах одного и того же TCP- или UDP-взаимодействия могут передаваться как фрагментированные, так и нефрагментированные пакеты. Во фрагментированных пакетах порт источника и порт назначения отсутствуют. В результате в рамках одной сессии пакеты могут прийти до получателя не в том порядке, так как отправляются через разные интерфейсы.
Сеть	Способ присвоения IP-адреса — без адреса, статический IP-адрес или динамический IP-адрес, полученный по DHCP.

Настройка шлюзов

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

Для подключения LogAn к Интернету необходимо указать IP-адрес одного или нескольких шлюзов.

Можно указать несколько шлюзов, если для подключения к Интернету используется несколько провайдеров. Пример настройки сети с двумя провайдерами:

- Интерфейс port1 с IP-адресом 192.168.11.2 подключен к Интернет-провайдеру 1. Для выхода в Интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.11.1
- Интерфейс port2 с IP-адресом 192.168.12.2 подключен к Интернет-провайдеру 2. Для выхода в Интернет с этого провайдера необходимо добавить шлюз с IP-адресом 192.168.12.1

При наличии двух или более шлюзов возможны 2 варианта работы:

Наименование	Описание
Балансировка трафика между шлюзами	Установить флажок Балансировка и указать Вес каждого шлюза. В этом случае весь трафик в Интернет будет распределен между шлюзами в соответствии с указанными весами (чем больше вес, тем большая доля трафика идет через шлюз).
Основной шлюз с переключением на запасной	Выбрать один из шлюзов в качестве основного и настроить Проверку сети , нажав на одноименную кнопку в интерфейсе. Проверка сети проверяет доступность хоста в Интернет с указанной в настройках периодичностью, и в случае, если хост перестает быть доступен, переводит весь трафик на запасные шлюзы в порядке их расположения в консоли.

По умолчанию проверка доступности сети настроена на работу с публичным DNS-сервером Google (8.8.8.8), но может быть изменена на любой другой хост по желанию администратора.

Маршруты

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

Данный раздел позволяет указать маршрут в сеть, доступную за определенным маршрутизатором. Например, в локальной сети может быть маршрутизатор, который объединяет несколько IP-подсетей.

Для добавления маршрута необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Задать название и описание данного маршрута	В разделе Сеть выберите в меню Маршруты , нажмите кнопку Добавить . Укажите имя для данного маршрута. Опционально можно задать описание маршрута.
Шаг 2. Указать адрес назначения	Задайте подсеть, куда будет указывать маршрут, например, 172.16.20.0/24 или 172.16.20.5/32.
Шаг 3. Указать шлюз	Задайте IP-адрес шлюза, через который указанная подсеть будет доступна. Этот IP-адрес должен быть доступен с сервера LogAn.
Шаг 4. Указать интерфейс	Выберите интерфейс, через который будет добавлен маршрут. Если оставить значение Автоматически , то LogAn сам определит интерфейс, исходя из настроек IP-адресации сетевых интерфейсов.
Шаг 5. Указать метрику	Задайте метрику маршрута. Чем меньше метрика, тем приоритетней маршрут в данную сеть, если маршрутов несколько.

Общие сведения

Documentation: ☒

Product: LogAn, SIEM

Version: 6.1.9, 7.0.1, 7.1.0

Для сбора информации с различных устройств и последующего ее анализа LogAn использует сенсоры. Сенсор — это совместимое с LogAn устройство, которое может передавать определенные данные на сервер LogAn. Сенсорами могут выступать устройства UserGate NGFW, конечные устройства UserGate Client, а также любые другие сетевые устройства, способные передавать данные по протоколу SNMP.

Сенсоры SNMP

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

С помощью сенсора SNMP администратор может подключить SNMP-совместимое сетевое устройство к серверу LogAn для сбора и анализа его метрик. LogAn может отображать любые счетчики, полученные по SNMP с помощью запросов SNMP. Для настройки сенсора SNMP необходимо иметь базы MIB (Management Information Base) на управляемое устройство. Подробнее об управлении базами MIB смотрите раздел данного руководства [Управление SNMP MIB](#).

Для настройки сенсора SNMP необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Загрузите базу MIB того устройства, которое хотите добавить для мониторинга.	На сервере LogAn в разделе Сенсоры → Управление SNMP MIB загрузите файл с MIB.
Шаг 2. Создайте сенсор SNMP	На сервере LogAn в разделе Сенсоры → Сенсоры SNMP нажмите кнопку Добавить и заполните необходимые поля.

При создании сенсора SNMP необходимо заполнить следующие поля:

Наименование	Описание
Включено	Включает или выключает данный сенсор SNMP.
Название	Название сенсора SNMP.
Описание	Опциональное описание сенсора SNMP.
Адрес сервера	IP-адрес сенсора SNMP.
Порт	Порт сенсора SNMP. Обычно для запросов данных по протоколу SNMP используется порт TCP 161.
Версия	Указывает версию протокола SNMP, которая будет использоваться в данном сенсоре. Возможны варианты SNMP v2 и SNMP v3.
Community	SNMP community - строка для идентификации сервера LogAn и сетевого устройства для версии SNMP v2. Используйте только латинские буквы и цифры.
Интервал опроса (сек)	Интервал, через который сервер LogAn будет инициировать получение данных с сетевого устройства.
Пользователь	Только для SNMP v3. Имя пользователя для аутентификации сетевом устройстве.
Тип аутентификации	Выбор режима аутентификации. Возможны варианты: - Без аутентификации, без шифрования (noAuthNoPriv). - С аутентификацией, без шифрования (authNoPriv). - С аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv.
Алгоритм аутентификации	Алгоритм, используемый для аутентификации.
Пароль аутентификации	Пароль, используемый для аутентификации.

Наименование	Описание
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
Пароль шифрования	Пароль, используемый для шифрования.
Счётчики	Укажите здесь все требуемые данные, которые LogAp будет запрашивать на сетевом устройстве. Счетчики выбираются из баз MIB, которые загружены на устройство. Выберите в дереве SNMP необходимый раздел и добавьте соответствующий счетчик либо укажите в строке SNMP OID счетчика и его тип.

После успешного добавления сенсора в разделе **Дашборд** появится возможность добавить виджет с графиками данных SNMP, полученными с данного сенсора.

Сенсоры WMI

Documentation: ☒

Product: LogAn, SIEM

Version: 7.0.1, 7.1.0

С помощью сенсора WMI администратор может подключить WMI-совместимое сетевое устройство (компьютер под управлением ОС Windows) к серверу LogAn для сбора и анализа его метрик.

Конечные устройства

Documentation: ☒

Product: LogAn, SIEM

Version: 7.0.1, 7.1.0

Данный раздел содержит список конечных устройств с установленным программным обеспечением UserGate Client.

Примечание Конечное устройство будет отображено при выборе на UGMC данного устройства LogAn в качестве сервера для передачи информации о событиях, соответственно, LogAn должен быть предварительно зарегистрирован на UGMC.

Отображена следующая информация:

- Название конечного устройства, заданное на UGMC.
- Версия ПО UserGate Client, установленная на устройстве.
- Время последнего подключения к устройству.
- IP-адрес устройства.
- Netbios имя.
- Версия операционной системы (ОС) устройства.
- Телеметрическая информация.

В LogAn реализована возможность удалённого управления устройствами UserGate Client. Для этого нажмите **Послать команду** и выберите необходимое действие:

- Отключить от сети.
- Разрешить передачу данных по сети.
- Завершить процесс. При выборе данного действия необходимо указать идентификатор процесса.
- Запустить/остановить службу. Для выполнения данных действий необходимо указать название службы.

Управление SNMP MIB

Documentation: 

Product: LogAn, SIEM

Version: 6.1.9, 7.0.1, 7.1.0

В данном разделе администратор может добавлять и удалять базы MIB (Management Information Base) на сервере LogAn.

Для получения специфических MIB обратитесь к производителю вашего устройства. LogAn уже содержит наиболее популярные базы сетевых устройств.

Интерфейс командной строки (CLI)

Интерфейс командной строки (CLI)

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

LogAn позволяет создавать базовые настройки устройства с помощью интерфейса командной строки или CLI (command line interface). С помощью CLI администратор может выполнить ряд диагностических команд, таких, как ping, nslookup, traceroute, осуществить настройку сетевых интерфейсов и зон, а также перезагрузить или выключить устройство.

CLI полезно использовать для диагностики сетевых проблем или в случае, когда доступ к веб-консоли утерян, например, некорректно указан IP-адрес интерфейса или ошибочно установлены параметры контроля доступа для зоны, запрещающие подключение к веб-интерфейсу.

Подключение к CLI можно выполнить через стандартные порты VGA/клавиатуры (при наличии таких портов на оборудовании LogAn), через последовательный порт или с помощью SSH по сети.

Для подключения к CLI с использованием монитора и клавиатуры необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключить монитор и клавиатуру к LogAn	Подключить монитор к разъему VGA(HDMI), клавиатуру к разъему USB.
Шаг 2. Войти в CLI	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin). Если устройство LogAn не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля — utm.

Для подключения к CLI с использованием последовательного порта необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Подключиться к LogAn	Используя специальный кабель для последовательного порта или переходник USB-Serial, подключить свой компьютер к LogAn.
Шаг 2. Запустить терминал	Запустить терминал, позволяющий подключение через последовательный порт, например, Putty для Windows или minicom для Linux. Установить подключение через последовательный порт, указав параметры подключения 115200 8n1.
Шаг 3. Войти в CLI	Войти в CLI, используя имя и пароль пользователя с правами Full administrator (по умолчанию Admin). Если устройство LogAn не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля — utm.

Для подключения к CLI по сети с использованием протокола SSH необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Разрешить доступ к CLI (SSH) для выбранной зоны	Разрешить доступ для протокола CLI по SSH в настройках зоны, к которой вы собираетесь подключаться для управления с помощью CLI. Будет открыт порт TCP 2200.
Шаг 2. Запустить SSH-терминал	Запустить у себя на компьютере SSH-терминал, например, SSH для Linux или Putty для Windows. Указать в качестве адреса адрес LogAn, в качестве порта подключения — 2200, в качестве имени пользователя — имя пользователя с правами Full administrator (по умолчанию Admin). Для Linux команда на подключение должна выглядеть так: ssh Admin@IPLogAn -p 2200
Шаг 3. Войти в CLI	Войти в CLI, используя пароль пользователя, указанного на предыдущем шаге. Если устройство LogAn не прошло первоначальную инициализацию, то для доступа к CLI необходимо использовать в качестве имени пользователя Admin, в качестве пароля — utm.

После успешного входа в CLI можно посмотреть список возможных команд с помощью команды **help**. Для подробного описания любой команды необходимо использовать синтаксис

help command

Например, для получения подробной справки по использованию команды настройки сетевого интерфейса iface необходимо выполнить

help iface

Полный список команд:

Наименование	Описание
help	Показывает список доступных команд.
exit quit Ctrl+D	Выйти из CLI.
date	Посмотреть текущее время на сервере.
gateway	Посмотреть или задать значения шлюза. Смотрите gateway help для детальной информации.
iface	Набор команд для просмотра и настройки параметров сетевого интерфейса. Смотрите iface help для детальной информации.
license	Посмотреть информацию о лицензии.
netcheck	Проверить доступность стороннего HTTP/HTTPS-сервера. netcheck [-t TIMEOUT] [-d] URL Опции: -t — максимальный таймаут ожидания ответа от веб-сервера -d — запросить содержание сайта. По умолчанию запрашиваются только заголовки.
nslookup	Выполнить определение IP-адреса по имени хоста.
ping	Выполнить ping определенного хоста.
radmin	Включить или отключить удаленный доступ к серверу для технической поддержки LogAn.
radmin_e	Включить или отключить удаленный доступ к серверу для технической поддержки LogAn, в случаях, когда сервер LogAn не работает корректно.
reboot	Перезагрузить сервер LogAn.
route	Создать, изменить, удалить маршрут.
shutdown	Выключить сервер LogAn.
traceroute	Выполнить трассировку соединения до определенного хоста.
zone	Набор команд для просмотра и настройки параметров зоны. Смотрите zone help для детальной информации.

Documentation: ☒
Product: UGMC, LogAn
Version: 6.1.9, 7.0.1

Мониторинг маршрутов

Раздел **Маршруты** позволяет получить список всех маршрутов, указанных на определенном узле UserGate. Для просмотра маршрутов необходимо нажать на кнопку **Фильтр** и указать типы маршрутов, которые необходимо отобразить. Возможно указать следующие типы маршрутов:

- **Подключенные к интерфейсам** — маршруты к сетям, которые подключены непосредственно к интерфейсам UserGate. Данные маршруты будут помечены символом **С** в списке маршрутов.
- **Заданные статически** — маршруты, заданные статически в разделе **Сеть → Маршруты**. Данные маршруты будут помечены символом **К** в списке маршрутов.
- **OSPF** — маршруты, полученные по протоколу OSPF. Данные маршруты будут помечены символом **О** в списке маршрутов.
- **BGP** — маршруты, полученные по протоколу BGP. Данные маршруты будут помечены символом **В** в списке маршрутов.
- **RIP** — маршруты, полученные по протоколу RIP. Данные маршруты будут помечены символом **Р** в списке маршрутов.

Отображаемый список маршрутов можно скачать в виде текстового файла с помощью кнопки **Скачать все маршруты**.

Ping

С помощью утилиты ping можно диагностировать доступность сетевых ресурсов. Параметры команды ping:

Наименование	Описание
Ping host	Хост, который необходимо проверить.
TTL	Максимальное количество промежуточных хостов, которое разрешено пройти на пути к проверяемому хосту.
Интерфейс	Адрес выбранного интерфейса будет использоваться в качестве адреса источника для выполнения ping, а интерфейс отправки пакета будет выбран согласно таблице маршрутизации.
Счетчик	Количество повторов.
Показывать временные метки	Добавляет временные метки в вывод команды.
Не резолвить имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Traceroute

С помощью утилиты traceroute можно проверить путь следования сетевых пакетов к определенному хосту. Параметры команды traceroute:

Наименование	Описание
Traceroute host	Хост, который необходимо проверить.
Использовать ICMP	Использовать протокол ICMP для выполнения команды traceroute. Если не указано, то используется протокол UDP.
Интерфейс	Сетевой интерфейс, с которого необходимо выполнять команду.
Не разрешать доменные имена	Оперировать IP-адресами, не преобразовывая их в доменные имена.

Запрос DNS

Используя запрос DNS, администратор может проверить работу DNS-серверов.

Наименование	Описание
DNS-запрос (хост)	DNS имя для проверки.
IP источника запроса	Один из IP-адресов, назначенных UserGate.
DNS сервер	Адрес DNS-сервера, на который будет отправлен запрос.
Порт	UDP порт, используемый для запроса.
Тип DNS-запроса	Тип запроса.

Оповещения

Правила оповещений

Данный раздел позволяет определить правила оповещений, которые в дальнейшем можно использовать для отсылки оповещений о различных типах событий, например, высокой загрузке CPU или недоступности сервера. Для создания правила оповещений необходимо выполнить следующие шаги:

Наименование	Описание
Шаг 1. Создать один или несколько профилей оповещения.	Смотрите раздел Профили оповещений .
Шаг 2. Создать группы получателей оповещений.	Смотрите разделы Почтовые адреса и Номера телефонов .
Шаг 3. Создать правило оповещения.	В разделе Оповещения → Правила оповещений добавить правило.

При добавлении правила необходимо указать следующие параметры:

Наименование	Описание
Включено	Включает или отключает данное правило.
Название	Название правила.
Описание	Описание правила.
Профиль оповещения	Созданный ранее профиль оповещения. Для профилей SMPP появится закладка для указания адресатов в виде телефонных номеров, для SMTP появится закладка для указания адресатов в виде email-адресов.
От	От кого будет приходить оповещение.
Тема	Тема оповещения.
Таймаут перед повторной отправкой, секунд	Укажите таймаут, в течение которого сервер не будет отправлять сообщение при повторном срабатывании данного правила. Данная настройка позволяет предотвратить шторм сообщений при частом срабатывании правила оповещения.
События	Укажите события, для которых необходимо получать оповещения.
Телефоны	Для SMPP-профиля. Укажите группы номеров телефонов, куда отправлять SMS-оповещения.

Наименование	Описание
Emails	Для SMTP-профиля. Укажите группы адресов email, на которые будут отправляться почтовые оповещения.

SNMP

UserGate поддерживает мониторинг с помощью протоколов SNMP v2c и SNMP v3. Поддерживается управление как с помощью запросов (SNMP queries), так и с помощью отсылки оповещений (SNMP traps). Это позволяет наблюдать за критическими параметрами UserGate с помощью программного обеспечения SMNP-управления, используемого в компании.

Для настройки мониторинга с помощью SNMP необходимо:

1. В свойствах зоны интерфейса, к которому будет осуществляться подключение по протоколу SNMP, во вкладке **Контроль доступа** разрешить сервис **SNMP**.
2. Создать правило SNMP.

Для настройки мониторинга с помощью SNMP необходимо создать правила SNMP. Для создания правила SNMP необходимо в разделе **SNMP** нажать на кнопку **Добавить** и указать следующие параметры:

Наименование	Описание
Название	Название правила.
Описание	Описание правила SNMP (опционально).
IP-адрес сервера для трапов	IP-адрес сервера для трапов и порт, на котором сервер слушает оповещения. Обычно это порт UDP 162. Данная настройка необходима только в случае, если необходимо отправлять трапы на сервер оповещений.
Community	SNMP community — строка для идентификации сервера UserGate и сервера управления SNMP для версии SNMP v2c. Используйте только латинские буквы и цифры.
Контекст	Необязательный параметр, определяющий SNMP context. Можно использовать только латинские буквы и цифры. На некоторых устройствах может быть несколько копий полного поддерева MIB. Например, на устройстве может быть создано несколько виртуальных маршрутизаторов. Каждый такой виртуальный маршрутизатор будет иметь полное поддерево MIB. В этом случае каждый виртуальный маршрутизатор может быть указан как контекст на сервере SNMP. Контекст определяется по имени. Когда клиент отправляет запрос, он может указать имя контекста. Если имя контекста не указано, будет запрошен контекст по умолчанию.
Версия	Указывает версию протокола SNMP, которая будет использоваться в данном правиле. Возможны варианты SNMPv2c и SNMPv3.
Разрешить SNMP-запросы	При включении разрешает получение и обработку SNMP-запросов от SNMP-менеджера.
Разрешить SNMP-трапы	При включении разрешает отправку SNMP-трапов на сервер, настроенный для приема оповещений.
Пользователь	Только для SNMP v3. Имя пользователя для аутентификации SNMP-менеджера.
Тип аутентификации	Выбор режима аутентификации SNMP-менеджера. Возможны варианты: • Без аутентификации, без шифрования (noAuthNoPriv). • С аутентификацией, без шифрования (authNoPriv). • С аутентификацией, с шифрованием (authPriv). Наиболее безопасным считается режим работы authPriv.
Алгоритм аутентификации	Алгоритм, используемый для аутентификации.

Наименование	Описание
Пароль аутентификации	Пароль, используемый для аутентификации.
Алгоритм шифрования	Алгоритм, используемый для шифрования. Возможно использовать DES и AES.
Пароль шифрования	Пароль, используемый для шифрования.
События	Выбор типов параметров, доступных для мониторинга по правилу.

Примечание Настройки аутентификации для SNMP v2c (community) и для SNMP v3 (пользователь, тип аутентификации, алгоритм аутентификации, пароль аутентификации, алгоритм шифрования, пароль шифрования) на SNMP-менеджере должны совпадать с настройками SNMP в UserGate.

Информацию по настройке параметров аутентификации для вашего SNMP-менеджера смотрите в руководстве по настройке выбранного вами программного обеспечения для управления SNMP.

Кнопка **Скачать MIB** позволяет скачать MIB-файлы с параметрами мониторинга UserGate для последующего использования их в SNMP-менеджере. UserGate выделен уникальный идентификатор **SNMP PEN** (Private Enterprise Number) **45741**.

Для скачивания доступны следующие MIB-файлы:

- UTM-TRAPS-MIB.
- UTM-TRAPS-BINDINGS-MIB.
- UTM-MIB.
- UTM-INTERFACES-MIB.

UTM-TRAPS-MIB

Наименование	Описание
trapCoreCrush	Сбой ядра.
trapStatDown	Сервис статистики (UserGate Log Analyzer) недоступен.
trapCoreBootstrapEnd	Загрузка сервера завершена успешно.
trapDefaultGatewayChanged	Изменение шлюза по умолчанию.
trapHighSessionsCounter	Таблица сессий заполнена на 90%.
trapHighUsersCounter	Количество активных пользователей достигло 90% от порога лицензии.
trapStatusChanged	Изменение статуса узла отказоустойчивого кластера.
trapMemberUp	Статус узла отказоустойчивого кластера изменился на «Подключен».
trapMemberDown	Узел отказоустойчивого кластера отключен.
trapAttackDetected	Обнаружена атака COB.
trapChecksumFailed	Нарушение целостности бинарных файлов.
trapHighCPUUsage	Высокая загрузка центрального процессора.

Наименование	Описание
trapLowMemory	Высокая загрузка памяти.
trapLowLogdiskSpace	Недостаточно места на диске для хранения журналов.
trapRaidStatus	Изменение статуса RAID.
trapPowerSupply	Первый источник питания отключен.
trapCableStatus	Кабель был подключен или отключен от интерфейса.
trapTrafficDrop	Срабатывание запрещающего правила межсетевого экрана.
trapLDAPServerDown	Сервер LDAP недоступен.

UTM-TRAPS-BINDINGS-MIB

Наименование	Тип данных	Описание
utmSessions	integer	Текущее количество активных сессий.
utmSessionsMax	integer	Максимальное количество активных сессий.
utmUsers	Integer	Количество активных пользователей на данный момент.
utmUsersMax	integer	Максимальное количество активных пользователей.
utmHASstatus	integer	Текущий статус узла кластера отказоустойчивости: 0 — master-узел. 1 — slave-узел. 3 — fault.
utmHASstatusReason	integer	Причина изменения статуса узла отказоустойчивого кластера: 1 — связь с узлом потеряна. 2 — HTTP прокси-сервер недоступен. 3 — ни один из шлюзов недоступен. 4 — DNS-сервер недоступен. 5 — узел UserGate Management Center недоступен.
utmCPUUsage	integer	Загруженность центрального процессора; отображается в %.
utmMemory	integer	Использование оперативной памяти; отображается в %.
utmLogdiskSpace	integer	Пространство на диске, используемое под журналы; отображается в %.

Наименование	Тип данных	Описание
utmAdaptecRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Adaptec: • no_raid. • 0 — optimal — массив в оптимальном состоянии. • 1 — degraded — полный или частичный выход из строя одного из дисков. • 2 — rebuild — восстановление массива.
utmBroadcomRaidStatus	integer	Текущий статус RAID (Redundant Array of Independent Disks), построенного на контроллере Broadcom: • no_raid. • 0 — optimal — массив в оптимальном состоянии. • 1 — degraded — полный или частичный выход из строя одного из дисков. Переход в данный статус произойдёт при выходе из строя 2-х дисков. • 2 — partialDegraded — полный или частичный выход из строя одного из дисков. • 3 — failed — не работает из-за наличия ошибки. • 4 — offline — диск не доступен для RAID-контроллера.
utmPowerSupply	integer	Количество источников питания: • 1 — один блок питания. • 2 — два блока питания.
utmPowerSupplyStatus	integer	Состояние источника питания: • no_power_supplies. • 0 — off. • 1 — on.
utmCSCIfName	string	Название интерфейса.
utmCSCStatus	integer	Статус сетевого адаптера: • 1 — кабель подключен. • 2 — кабель не подключен.
utmLDAPServerName	string	Название LDAP-сервера.
utmLDAPServerAddress	string	IP-адрес LDAP-сервера.

UTM-MIB

Наименование	Тип данных	Описание
vcpuCount	integer	Количество виртуальных процессоров в системе.
vcpuUsage	integer	Загруженность виртуальных процессоров системы; отображается в %.
usersCounter	integer	Количество активных пользователей на текущий момент времени.
cpuLoad	integer	Загруженность центрального процессора системы; отображается в %.
memoryUsed	integer	Использование оперативной памяти; отображается в %.

Наименование	Тип данных	Описание
logDiskSpace	integer	Пространство на диске, используемое под журналы; отображается в %.
Sys_power_supply1_status	string	Состояние первого источника питания: - no_power_supplies. - on. - off.
Sys_power_supply2_status	string	Состояние второго источника питания. - no_power_supplies. - on. - off.
Sys_raid_status	integer	Текущий статус RAID (Redundant Array of Independent Disks): - no_raid. 0 — optimal — массив в оптимальном состоянии. 1 — degraded — полный или частичный выход из строя одного из дисков. 2 — rebuild — восстановление массива.

UTM-INTERFACES-MIB

Наименование	Тип данных	Описание
ifNumber	integer	Количество сетевых интерфейсов.
ifIndex	integer	Значение уникально для каждого интерфейса и может принимать значения от 1 до ifNumber.
ifDescr	string	Описание интерфейса.

Наименование	Тип данных	Описание
ifType	integer	Тип интерфейса, определённый в соответствии с протоколом физического/канального уровней: • 1 — other — неизвестный тип. • 2 — regular1822 — определён в BBN Report 1822. • 3 — hdh1822 — определён в BBN Report 1822. • 4 — ddn-x25 — определён в BBN Report 1822. • 5 — rfc877-x25 — определён в стандарте канального уровня сетевой модели OSI X.25. • 6 — ethernet-csmacd — сетевой интерфейс типа Ethernet, независимо от скорости (определён в RFC 3635). • 7 — iso88023-csmacd — определён в IEEE 802.3. • 8 — iso88024-tokenBus — определён в стандарте IEEE 802.4. • 9 — iso88025-tokenRing — сетевой интерфейс использует подключение Token Ring; определяется в стандарте IEEE 802.5. • 10 — iso88026-man — определён в стандарте ISO 88026 "MAN". • 11 — starLan — определён в стандарте IEEE 802.3e. • 12 — proteon-10Mbit — Proteon 10 Mbit • 13 — proteon-80Mbit — Proteon 80 Mbit. • 14 — hyperchannel — высокоскоростной канал, используемы в сети ISDN. • 15 — fddi — сетевой интерфейс использует подключение FDDI (Fiber Distributed Data Interface). FDDI — это набор стандартов передачи данных по оптоволоконным линиям в локальной сети. • 16 — lapb — протокол канального уровня, используемым для передачи пакетов стандарта X.25. • 17 — sdhc — протокол канального уровня для системной сетевой архитектуры IBM. • 18 — ds1 — способен обрабатывать 24 одновременных соединения на общей скорости 1,544 Мбит/с; также называется T1. • 19 — e1 — европейский аналог T1. • 20 — basicISDN — для связи аппаратуры абонента и ISDN-станции. • 21 — primaryISDN — используется для подключения к широкополосным магистралям, связывающим местные и центральные АТС или сетевые коммутаторы. • 22 — propPointToPointSerial — определён в стандарте RFC1213. • 23 — ppp — сетевой интерфейс использует подключение PPP (Point-To-Point Protocol). • 24 — softwareLoopback — сетевой интерфейс является петлевым адаптером. Такие интерфейсы часто используются для тестирования; они не отправляют трафик в сеть. • 25 — eon — ConnectionLess Network Protocol (CLNP) over Internet Protocol (IP); определён в ISO/IEC 8473-1. • 26 — ethernet-3Mbit — сетевой интерфейс использует подключение Ethernet со скоростью 3 Мбит/с. Эта версия Ethernet определяется в стандарте IETF RFC 895. • 27 — nsip — XNS over IP — предназначен для использования в разнообразных средах передачи данных. • 28 — slip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • 29 — ultra -ULTRA Technologies. • 30 — ds3 — высокоскоростной интерфейс передачи данных, сформированный мультиплексированием сигналов DS1 и DS2; также называется T3. • 31 — sip — сетевой интерфейс использует подключение SLIP (Serial Line Internet Protocol). SLIP определяется в стандарте IETF RFC 1055. • 32 — frame-relay — обеспечивает возможность передачи данных с коммутацией пакетов через интерфейс между устройствами пользователя и оборудованием сети.

Наименование	Тип данных	Описание
ifMtu	integer	Максимальный размер пакета сетевого уровня, который можно послать через этот интерфейс.
ifSpeed	gauge32	Пропускная способность интерфейса в битах в секунду.
ifPhysAddress	string	Физический адрес интерфейса (MAC-адрес).
ifAdminStatus	integer	Состояние интерфейса, назначаемое администратором: 1 — up — готов для передачи пакетов. 2 — down — не работает. 3 — testing — в режиме тестирования; рабочие пакеты не могут быть переданы.
ifOperStatus	integer	Текущий статус работы интерфейса: 1 — up — интерфейс готов для передачи пакетов. 2 — down — интерфейс не может передавать пакеты данных. 3 — testing — выполняется тестирование сетевого интерфейса; рабочие пакеты не могут быть переданы. 4 — unknown — интерфейс находится в неизвестном состоянии. 5 — dormant — сетевой интерфейс не может передавать пакеты данных, он ожидает внешнее событие. 6 — notPresente — сетевой интерфейс не может передавать пакеты данных из-за отсутствующего компонента, обычно аппаратного. 7 — lowerLayerDown — сетевой интерфейс не может передавать пакеты данных, потому что он работает поверх одного или нескольких других интерфейсов, и не менее одного из этих интерфейсов "нижнего уровня" не работает.
ifLastChange	timeticks	Значение SysUpTime, когда интерфейс оказался в данном состоянии.
ifInOctets	counter32	Количество байтов, принятое данным интерфейсом, включая служебные.
ifInUcastPkts	counter32	Количество доставленных пакетов одноадресной рассылки.
ifInNUcastPkts	counter32	Количество доставленных многоадресных и широковещательных пакетов.
ifInDiscards	counter32	Количество входящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их доставке. Одна из возможных причин отбрасывания: освобождение буферного пространства.
ifInErrors	counter32	Количество входящих пакетов, которые содержат ошибки, препятствующие их доставке.
ifInUnknownProtos	counter32	Количество пакетов, которые были получены через этот интерфейс и отброшены из-за использования неизвестного или неподдерживаемого протокола.
ifOutOctets	counter32	Количество байтов, переданное данным интерфейсом, включая служебные.
ifOutUcastPkts	counter32	Количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены.
ifOutNUcastPkts	counter32	Количество отправленных многоадресных и широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены.

Наименование	Тип данных	Описание
ifOutDiscards	counter32	Количество исходящих пакетов, которые были отброшены, даже если не было обнаружено ошибок, препятствующих их передаче. Одна из возможных причин отбрасывания: освобождение буферного пространства.
ifOutErrors	counter32	Количество исходящих пакетов, передача которых невозможна вследствие наличия ошибок.
ifOutQLen	gauge32	Число пакетов в очереди на отправку.
ifInMulticastPkts	counter32	Количество доставленных пакетов многоадресной рассылки.
ifInBroadcastPkts	counter32	Количество доставленных широковещательных пакетов.
ifOutMulticastPkts	counter32	Количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены.
ifOutBroadcastPkts	counter32	Количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены.
ifHCInOctets	counter64	Смысл одинаков со смыслом объекта ifInOctets — количество байтов, принятое данным интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCInUcastPkts	counter64	Смысл одинаков со смыслом объекта ifInUcastPkts — количество доставленных пакетов одноадресной рассылки; используется счётчик большей ёмкости.
ifHCInMulticastPkts	counter64	Смысл одинаков со смыслом объекта ifInMulticastPkts — количество доставленных пакетов многоадресной рассылки; используется счётчик большей ёмкости.
ifHCInBroadcastPkts	counter64	Смысл одинаков со смыслом объекта ifInBroadcastPkts — количество доставленных широковещательных пакетов; используется счётчик большей ёмкости.
ifHCOctets	counter64	Смысл одинаков со смыслом объекта ifOutOctets — количество байтов, переданное данным интерфейсом, включая служебные; используется счётчик большей ёмкости.
ifHCOUcastPkts	counter64	Смысл одинаков со смыслом объекта ifOutUcastPkts — количество отправленных пакетов одноадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOmulticastPkts	counter64	Смысл одинаков со смыслом объекта ifOutMulticastPkts — количество отправленных пакетов многоадресной рассылки, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifHCOBroadcastPkts	counter64	Смысл одинаков со смыслом объекта ifOutBroadcastPkts — количество отправленных широковещательных пакетов, включая пакеты, которые были отброшены или не отправлены; используется счётчик большей ёмкости.
ifLinkUpDownTrapEnable	integer	Указывает, должен ли создаваться трап при изменении статуса соединения: • 1 — enabled — включено. • 2 — disabled — отключено.
ifHighSpeed	gauge32	Оценка текущей полосы пропускания интерфейса; указывается в бит/с, кбит/с, Мбит/с, Гбит/с.

Наименование	Тип данных	Описание
ifPromiscuousMode	integer	"Неразборчивый" режим. Может принимать значения: • 1 — true — станция принимает все пакеты/кадры независимо от того, кому они адресованы. • 2 — false — интерфейс принимает только пакеты/кадры, адресованные этой станции. Значение объекта не влияет на приём широковещательных и многоадресных пакетов/кадров.
ifAlias	string	Название интерфейса, заданное администратором.
ifCounterDiscontinuityTime	timeticks	Значение SysUpTime, когда произошло событие, ставшее причиной сбоя работы одного или более счётчиков интерфейса.

Описание

Documentation: 

Product: LogAn, SIEM

Version: 7.0.1, 7.1.0

Сборщик логов предназначен для централизованного сбора информации с сетевых устройств, что помогает облегчить мониторинг сети, виртуальных машин, серверов, пользовательских устройств, приложений.

Syslog

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

В данном разделе настраиваются правила сбора событий системных журналов Unix-систем (syslog), которые содержат информацию о работе системы, её состоянии и безопасности, наличии ошибок, сбоях в работе. Правила syslog позволяют осуществлять фильтрацию записей событий (по времени, критичности событий, объектам, названию устройств, приложениям), упрощая поиск необходимой информации.

Для работы сборщика логов необходимо настроить сервер, с которого будет происходить сбор информации, и правила syslog.

Настройка сервера производится в разделе **Сборщик логов → Syslog** во вкладке **Настройки** веб-интерфейса LogAn; необходимо указать следующие данные:

Наименование	Описание
Включено	Включение/отключение приёма syslog событий.
Протокол	Сетевой протокол, использующийся для сбора информации: - TCP; - UDP.
Порт	Номер порта, использующегося для сбора syslog событий. По умолчанию — порт 514.
Максимальное количество сессий	Максимальное количество устройств, подключённых одновременно с целью отправки сообщений.
Безопасное соединение	Включение/отключение шифрования потока данных. Подробнее об использовании TLS в Syslog читайте в соответствующей документации.
Файл сертификата ЦС	Сертификат удостоверяющего центра (центра сертификации), который используется для установления безопасного соединения.
Файл сертификата	Сертификат, сгенерированный пользователем и подписанный центром сертификации (ЦС); необходимо указать при настройке безопасного соединения.
Разрешённые соседи	Список устройств, с которых LogAn будет получать информацию в случае использования безопасного соединения.

Для настройки правил фильтрации записей событий syslog необходимо указать следующие данные:

Наименование	Описание
Включено	Включение/отключение правила syslog.
Название	Название правила syslog.
Описание	Описание правила syslog (опционально).
Действие	Действие: Разрешить — разрешение приёма сообщений, подходящих под условия правила. Запретить — блокировка приёма сообщений, подходящих под условия правила.
Часовой пояс	Часовой пояс, настроенный на удалённых устройствах. Приём сообщений будет разрешён или запрещён с устройств, у которых сохранение записей происходит в указанном часовом поясе.

Наименование	Описание
Вставить	Место вставки создаваемого правила в списке правил: вверх, вниз или выше выбранного существующего правила.
Критичность	Критичность событий syslog: • Экстренная: критическое состояние, которое сказывается на работоспособности системы. • Тревога: состояние, требующее незамедлительного вмешательства. • Критическая: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • Ошибки: сообщения о сбоях в системе. • Предупреждения: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • Уведомительная: события, которые относятся к необычному поведению системы, но не являются ошибками. • Информативная: информационные уведомления. • Отладочная: информация, полезная разработчикам для отладки приложений.
Объект	Категория события: • Сообщения ядра. • Сообщения пользовательские. • Почтовая система. • Системный сервис. • Безопасность/авторизация. • Сообщения syslog. • Система печати LPR. • Система сетевых новостей. • Подсистема UUCP. • Сервис времени. • Безопасность/аутентификация. • FTP сервис. • Система NTP. • Аудит. • Тревога. • Сервис времени 2. • Local 0 — Local 7.
Имя хоста	Название устройства.
Название приложения	Название приложения, сбор информации о котором необходимо разрешить/запретить. Подробнее читайте в разделе Приложения syslog.

Записи событий будут отображены в журнале **Syslog**, подробнее читайте в разделе [Системный журнал](#).

Почтовые адреса

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

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

Для добавления новой группы почтовых адресов необходимо выполнить следующие шаги:

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

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

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

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

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

Номера телефонов

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

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

Для добавления новой группы телефонных номеров необходимо выполнить следующие шаги:

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

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

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

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

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

Профили оповещений

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

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

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

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

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

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

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

Категории срабатываний

Documentation: ☒

Version: 7.0.1, 7.1.0

Product: LogAn, SIEM

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

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

Внешние сервисы обогащений

Version: 7.0.1, 7.1.0

Product: LogAn, SIEM

Documentation: ☒

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

Чтобы использовать сервисы обогащения их необходимо включить. Для использования некоторых сервисов обогащения необходимо прохождение регистрации и предоставление ключа доступа.

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

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

Приложения syslog

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

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

Чтобы добавить приложение необходимо выполнить следующие действия:

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

Дашборд

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

Данный раздел позволяет посмотреть текущее состояние сервера и серверов, которые подключены к нему для отправки логов, их загрузку, статус лицензии и так далее.

Отчеты предоставлены в виде виджетов, которые могут быть настроены администратором системы в соответствии с его требованиями. Виджеты можно добавлять, удалять, изменять расположение и размер на странице **Дашборд**. По умолчанию созданы страницы с виджетами Log Analyzer (отображение состояния сервера Log Analyzer), NOC (Network Operation Center) и SOC (Security Operation Center).

Некоторые виджеты позволяют настроить отображение, указать фильтрацию данных и настроить прочие параметры. Для настройки виджета необходимо кликнуть по символу шестеренки в правом верхнем углу. Не все параметры, перечисленные ниже, доступны для каждого типа виджетов.

Наименование	Описание
Название	Название виджета, которое будет отображаться в Дашборд.
Описание	Опциональное описание виджета.
Количество записей	Максимальное количество записей для отображения.
Группировать по	Поле данных, по которому будут сгруппированы данные в виджете.
Диаграмма	Выбор типа представления данных. Доступны значения: • число; • круговая диаграмма; • вертикальная гистограмма; • горизонтальная гистограмма; • таблица; • график; • карта мира.
Запрос фильтра	SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении виджета. Для формирования запросов используются названия полей, значения полей, ключевые слова и операторы. Ключевые слова и операторы, а также примеры их использования можно посмотреть в разделе документации Поиск и фильтрация данных .
Сенсор	Сенсор, данные с которого используются для данного виджета.

Описание

Version: 7.0.1

Product: LogAn

Documentation: ☒

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

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

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

Примечание Записи журнала событий никогда не ротируются.

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

Журнал событий

Version: 6.1.9, 7.0.1, 7.1.0

Product: LogAn, SIEM

Documentation: 

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

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

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

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

Version: 6.1.9, 7.0.1, 7.1.0

Product: LogAn, SIEM

Documentation: 

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

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

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

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

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

Журнал трафика

Version: 6.1.9, 7.0.1, 7.1.0

Product: LogAn, SIEM

Documentation: 

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

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

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

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

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

Documentation: 

Version: 6.1.9, 7.0.1, 7.1.0

Product: LogAn, SIEM

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

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

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

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

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

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

История поиска

Version: 6.1.9, 7.0.1, 7.1.0

Product: LogAn, SIEM

Documentation: 

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

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

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

Экспорт журналов

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

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

UserGate LogAn поддерживает выгрузку следующих журналов:

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

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

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

При создании конфигурации требуется указать следующие параметры:

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

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

Наименование	Описание
Объект	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • Сообщения пользовательские. • Системный сервис. • Безопасность/авторизация. • Аудит. • Тревога. • Local 0. • Local 1. • Local 2. • Local 3. • Local 4. • Local 5. • Local 6. • Local 7.
Имя хоста	Только для типа серверов Syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер Syslog, в формате Fully Qualified Domain Name (FQDN).
App-Name	Только для типа серверов Syslog. Уникальное имя приложения, которое отправляет данные на сервер Syslog.
Логин	Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Пароль	Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Повторите пароль	Подтверждение пароля учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog.
Расписание	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно. • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5, 6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2 в поле "часы" будет означать "каждые два часа".

Журнал COB

Version: 7.0.1

Product: NGFW, LogAn

Documentation: ☒

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

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

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

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

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

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

Documentation: ☒

Version: 6.1.9, 7.0.1

Product: NGFW, LogAn

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

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

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

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

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

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

Поиск и фильтрация данных

Version: 7.0.1, 7.1.0

Product: LogAn, SIEM

Documentation: ☒

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

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

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

Ключевые слова отделяются пробелами и могут быть следующими:

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

Операторы определяют условия фильтра и могут быть следующими:

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

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

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

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

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

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

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

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

Documentation: ☒

Product: LogAn

Version: 6.1.9, 7.0.1

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

Список возможных шаблонов отчетов, сгруппированных по категориям:

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

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

Пользовательские шаблоны

Documentation: ☒

Product: LogAn

Version: 7.0.1

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

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

Правила отчетов

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

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

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

Наименование	Описание
Расписание	Выбор расписания для создания отчетов. Возможны варианты: - Ежедневно. - Еженедельно. - Ежемесячно. - Каждые ... часов. - Каждые ... минут. - Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 0-31) (месяц: 0-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: - Звездочка (*) — обозначает весь диапазон (от первого до последнего). - Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. - Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". - Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2" в поле "часы" будет означать "каждые два часа".
Доставка	Возможность задать опциональную отправку созданного отчета получателям по протоколу SMTP. Необходимо задать: - Профиль SMTP, который будет использован для отправки отчетов. Подробно о настройке профилей SMTP смотрите в главе Профили оповещений. - От — имя отправителя письма. - Тема письма — тема письма (subject). - Тело письма — содержимое письма. - Получатели — список получателей письма. Получатели должны быть добавлены в списки библиотеки Почтовые адреса.

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

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

Созданные отчеты

Documentation: ☒

Product: LogAn, SIEM

Version: 6.1.9, 7.0.1, 7.1.0

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

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

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

Общие сведения

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

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

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

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

Правила отчетов инцидентов

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

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

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

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

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

Созданные отчеты инцидентов

Documentation: 

Product: LogAn, SIEM

Version: 7.0.1, 7.1.0

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

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

Шаблоны отчетов инцидентов

Documentation: 

Product: LogAn, SIEM

Version: 7.0.1, 7.1.0

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

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

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

Общие сведения

Documentation: ☒

Version: 7.0.1

Product: LogAn

Раздел **Аналитика** LogAn предоставляет функционал SIEM — системы управления информацией о безопасности и событиями информационной безопасности. LogAn предоставляет возможность проведения анализа журналов событий безопасности, получаемых с настроенных сенсоров, таких как МЭ UserGate, конечные устройства UserGate Client, сторонние сетевые устройства, поддерживающие передачу данных по протоколу SNMP, сенсоры WMI. Все данные хранятся в одной базе данных, что даёт возможность осуществлять сложный поиск, корреляцию повторяющихся событий, их агрегацию, создавая инциденты безопасности, и упростить процесс изучения особенностей инцидентов.

Первоначальной единицей информации, которая поступает в LogAn, является событие. **Событие** — это одна запись в журнале, например, единичное срабатывание правила COB на МЭ UserGate, блокировка доступа к запрещенному ресурсу (срабатывание блокирующего правила контентной фильтрации), успешная или неуспешная попытка доступа в консоль управления и другие подобные события, которые регистрируются на устройствах, подключенных к LogAn. Отдельное событие может не нести достаточно информации об угрозе ИБ, но несколько однотипных событий (например, неуспешных попыток доступа в консоль управления) или разных событий, зарегистрированных в определенной последовательности и поступивших из разных источников, могут представлять ценность в идентификации угрозы. Этот процесс называется корреляция событий. Группа событий, объединенная правилом аналитики (корреляции), представляет собой **Срабатывание**. Инженер безопасности проводит анализ срабатывания, изучает входящие в срабатывание события и при необходимости может создавать **Инцидент** компьютерной безопасности на основе одного или нескольких срабатываний.

С помощью правил аналитики инженер безопасности может автоматизировать процесс корреляции событий и создание срабатываний, а также назначить определенные **Действия реагирования** (реакцию) системы на создаваемые срабатывания. Все это позволяет облегчить процесс изучения регистрируемых событий и сократить время между обнаружением проблемы и ее решением.

Настройка данной функции доступна во вкладке **Аналитика**, где можно настроить правила аналитики, создать действия реагирования, просмотреть журнал срабатываний правил и подробности срабатывания.

Данные функции будут рассмотрены далее в соответствующих разделах: [Действия реагирования](#), [Срабатывания](#) и [Подробности срабатывания](#).

Во вкладке **Правила аналитики** можно создавать правила обработки событий журналов. Настройка правил аналитики позволяет производить сложный поиск среди событий информационной безопасности. Срабатывание правила происходит при выявлении корреляции событий с разных источников. Правила могут работать в двух режимах: исторический режим (анализ событий за выбранный период) и режим реального времени.

Правила создаются нажатием кнопки **Добавить**. Далее во вкладке **Общие** необходимо указать свойства правила.

Наименование	Описание
Включено	Включает/отключает правило аналитики для работы в режиме реального времени.
Название	Отображает название правила аналитики.
Описание	Описывает правила аналитики. Данное поле необязательно для заполнения.
Уровень угрозы	Показывает уровень угрозы, который будет отображаться при срабатывании правила. Для выбора доступны следующие уровни: • Очень низкий: события, сформировавшие срабатывание правила аналитики, представляют очень низкий уровень угрозы, и администратор может не предпринимать никаких действий. • Низкий: события, сформировавшие срабатывание правила аналитики, представляют низкий уровень угрозы, и администратор может не предпринимать никаких действий. • Средний: необходимо обратить внимание на события, попавшие под срабатывание правила аналитики. • Высокий: события, требующие исследования и принятия мер. • Очень высокий: события, требующие исследования и срочного принятия мер.

Наименование	Описание
Приоритет	Показывает приоритет, установленный для срабатывания правила аналитики: • Низкий: срабатывания данных правил обладают низким приоритетом реагирования. • Нормальный: на срабатывания данных правил необходимо обратить внимание и, возможно, предпринять меры. • Важный: на срабатывания данных правил необходимо обратить внимание и предпринять меры. • Критический: срабатывания данных правил требуют незамедлительного реагирования. При срабатывании правила установленный приоритет будет указывать на важность срабатывания правила аналитики.
Категория	Отображает категорию, к которой относится срабатывание. По умолчанию для выбора доступны следующие категории: • Security: правила данной категории определяют инциденты, приводящие к ухудшению безопасности информационных систем. • Availability: правила данной категории определяют инциденты, которые приводят к ухудшению доступности информационных систем. • Performance: правила данной категории определяют инциденты, которые приводят к ухудшению производительности информационных систем. Дополнительные категории срабатываний могут быть созданы во вкладке Настройки в разделе Библиотеки → Категории срабатываний.
Часовой пояс	Указывает на часовой пояс, по времени которого будут работать правила аналитики, т.к. сервер может собирать данные с источников, находящихся в различных часовых поясах.

Во вкладке **Условия** необходимо указать условие/условия срабатывания правила. Если условий несколько, то они связаны между собой логическим «И» и выполняются сверху вниз. Т.е. правило сработает только в том случае, если будут выполнены все условия. Условие можно создать нажатием кнопки **Добавить**. Далее необходимо указать следующие параметры.

Наименование	Описание
Название	Отображает название условия правила аналитики.
Описание	Описывает условие правила аналитики. Данное поле необязательно для заполнения.
Ограничить время выполнения условия	Включить/отключить ограничение времени выполнения условия. При включении ограничения времени правило аналитики сработает, только в том случае, когда за указанный отрезок времени условие выполнится заданное количество раз.
Время выполнения условия	Указывает на отрезок времени, за который условие должно выполниться заданное количество раз, чтобы произошло срабатывание правила аналитики. Время указывается в секундах. Указание времени выполнения условия доступно при включённом чекбоксе Ограничить время выполнения условия.
Использовать запрос остановки	Включить/отключить использование запроса остановки в правиле аналитики.
Запрос остановки	SQL-подобный поисковый запрос остановки выполняется вместе с запросом условия. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы (задаётся аналогично запросу фильтра). Если при выполнении анализа найдётся хотя бы одна запись, соответствующая заданному запросу остановки, до того, как будет найдено заданное количество событий, соответствующих условию правила аналитики, то правило аналитики не сработает, а счётчик количества записей, найденных до выполнения запроса остановки, будет обнулён.

Наименование	Описание
Запрос фильтра	Отображает SQL-подобный поисковый запрос условия, который пишется по базе журналов. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы. Синтаксис написания запроса можно посмотреть в разделе Поиск и фильтрация данных. Запрос также может быть написан с использованием синтаксиса Google/RE2 в операторе MATCH. Например. Поисковый запрос: <pre>source = 'wmi log' and logFile = 'Microsoft-Windows-Sysmon/Operational' and logEventId = 1 and data MATCH 'ParentCommandLine:(.*)cmd.exe' and data ~ 'CertReq -Post -config'.</pre> Данный запрос производит поиск в журнале событий конечных устройств, который берёт данные из журнала Microsoft-Windows-Sysmon/Operational. При нахождении события, которое соответствует созданию нового процесса, запускается поиск родительского процесса (т.е. процесса, который вызвал создание нового процесса) и поиск вызова команды certreq с параметрами. Часть запроса с оператором MATCH позволяет определить, что certreq запустили из cmd (командной строки). Таким образом определяется то, что у текущего процесса родительским был cmd.exe. Подробнее о синтаксисе Google/RE2 в операторе MATCH: https://github.com/google/re2/wiki/Syntax.
Группировать по	Отображает список параметров, по которым могут быть сгруппированы правила в результате срабатывания. Поля будут отображены при просмотре карточки срабатывания. О параметрах, по которым возможна группировка, читайте в разделе Поиск. При указании категорий для группировки правило аналитики сработает только в том случае, если условие выполнится именно для выбранной категории заданное количество раз, указанное в поле параметра Повторений шаблона.
Повторений шаблона	Показывает количество выполнений условия, необходимое для срабатывания правила. Данный параметр может быть использован вместе с параметром Ограничить время выполнения условия или без него.
Запустить сейчас	Производит запуск анализа событий за определённый период времени (работа в историческом режиме). Далее необходимо задать временной диапазон. Если чекбокс Указать диапазон времени не активен, то анализ по созданному правилу аналитики проводится по всей базе событий за всё время. После завершения анализа, нажав кнопку Показать срабатывания в окне Запуск правила аналитики, можно перейти в журнал срабатываний и просмотреть информацию о срабатывании этого правила. Также правило можно запустить без записи в журнал срабатываний, т.е. для проверки работоспособности правила или просмотра количества срабатываний. Для этого необходимо включить чекбокс Тестовый запуск.

Во вкладке **Действия реагирования** могут быть добавлены действия, которые будут выполнены автоматически при срабатывании правила аналитики. Действия реагирования могут быть созданы нажатием кнопки **Создать и добавить новый объект** или добавлены из списка существующих действий. Подробнее о действиях реагирования и их настройке читайте в разделе [Действия реагирования](#).

Чтобы запустить правило в режиме реального времени необходимо нажать кнопку **Включить**. Кнопка **Отключить** завершает выполнение выбранного правила аналитики.

Созданные правила можно редактировать, удалять и копировать. Кнопка **Показать срабатывания** отобразит журнал с краткой информацией о всех срабатываниях выбранного правила. Также можно настроить отображение списка правил: отображать все правила, только включённые/выключенные правила.

Для правил аналитики также доступны функции экспорта и импорта. Импорт правил производится в бинарном формате или формате YAML. Экспортировать правила можно только в бинарном формате; экспортируются выделенные правила или все созданные, если правила не были выбраны.

При настройке условий правил аналитики возможно производить группировку событий по параметрам, представленным в записях журналов LogAn, NGFW и конечных устройств. Список параметров, по которым возможна группировка событий, смотрите в таблице раздела [Поиск](#).

Пример настройки правила аналитики

Version: 7.0.1

Product: LogAn

Documentation: ☒

В качестве примера рассмотрим настройку правила аналитики, направленную на поиск попыток брутфорса.

Брутфорс (Brute force) - метод взлома учётных записей путём подбора паролей к ним. Суть подхода заключается в последовательном автоматизированном переборе всех возможных комбинаций символов с целью определения правильной.

После задания общих настроек, таких как название правила, описание, уровень угрозы, приоритет, категория срабатывания и часовой пояс, были заданы несколько условий.

- **source = 'endpoint events log' AND logEventId = 4625 AND data MATCH 'Failure Reason:(\s*)Unknown user name or bad password.'**

В соответствии с условием производится поиск в журнале событий конечных устройств по идентификатору события 4625. Данный идентификатор события соответствует неудачной попытке авторизации учётной записи. Часть условия с оператором MATCH позволяет определить причину отказа в авторизации: неправильный логин или пароль.

Подробнее о событии 4625 читайте в соответствующей документации: <https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/event-4625>.

- **source = 'endpoint events log' AND logEventId = 4672**

В соответствии с условием производится поиск в журнале событий конечных устройств по идентификатору события 4672. Данный идентификатор события соответствует успешной авторизации с назначением специальных привилегий текущему сеансу.

Подробнее о событии 4672 читайте в соответствующей документации: <https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/event-4672>.

- **source = 'endpoint events log' AND logEventId = 4624**

В соответствии с условием производится поиск в журнале событий конечных устройств по идентификатору события 4624. Данный идентификатор события соответствует успешному входу пользователя в систему.

Подробнее о событии 4624 читайте в соответствующей документации: <https://docs.microsoft.com/ru-ru/windows/security/threat-protection/auditing/event-4624>.

Поиск

Version: 7.0.1
Product: LogAn
Documentation: ☒

Во вкладке **Поиск** отражён список всех событий журналов подключённых сенсоров и событий журналов LogAn. С использованием строки поиска можно производить поиск нужных событий. Строка поиска использует SQL-подобный поисковый запрос. Для формирования запроса используются названия полей, значения полей, ключевые слова и операторы. Синтаксис написания запроса можно просмотреть в разделе [Поиск и фильтрация данных](#). Запрос также может быть написан с использованием синтаксиса Google/RE2 в операторе MATCH.

С использованием кнопки **Добавить правило**, можно добавить новое правило аналитики, в котором в качестве запроса фильтра будет указан введённый поисковый запрос. Подробнее о правилах аналитики смотрите в разделе [Аналитика](#).

Также, нажатием кнопки **Добавить условие**, по введённому поисковому запросу можно сформировать условие и добавить его в созданное ранее правило аналитики. При добавлении необходимо указать правило аналитики и имя условия.

Выбранное событие можно добавить в инцидент нажатием кнопки **Добавить в инцидент**. Подробнее об инцидентах читайте в главе [Настройки инцидентов](#).

Существует 2 режима представления данных о событиях: табличный вид и текстовый вид. Для перехода в выбранный режим используются кнопки **Переключить в текстовый вид** или **Переключить в табличный вид**.

Во вкладке **Поиск** можно увидеть следующую информацию о событиях.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Узел	node	Показано имя узла устройства NGFW или LogAn.
Время	date	Указано время события или срабатывания правила аналитики. Отображается в часовом поясе, настроенном на LogAn.
Время первого события	triggeredAlertFirstEventDate	Для журнала срабатываний: отображено время первого события, попавшего под срабатывание правила аналитики.
Время последнего события	triggeredAlertLastEventDate	Для журнала срабатываний: отображено время последнего события, попавшего под срабатывание правила аналитики.
Источник	source	Показан журнал, в который записано событие: журналы LogAn, NGFW, конечных устройств, срабатываний.
Важность	severity	Отражена категория события журналов событий NGFW, LogAn: Информационные: как правило, не требуют внимания администратора. Предупреждение: предупреждают о возможных проблемах. Ошибка: сообщают об ошибках. Критические: сообщают о серьёзных ошибках, которые могут повлиять на функциональность.
Компонент	component	Отражён компонент, в котором произошло событие (например: обновления, настройки, консольная авторизация, аналитика и т.п.). Относится к записям журнала событий NGFW и LogAn.
Тип события	event	Отображён тип события из журнала событий NGFW, LogAn (например: проверка, скачивание, установка обновлений, успешная/неуспешная авторизация, поиск параметров и т.п.).
Пользователь	user	Показано имя пользователя, с учётной записи которого был совершён вход в систему NGFW, LogAn, конечного устройства. Относится к записям журналов событий NGFW, LogAn и конечных устройств, веб доступа, трафика, COB, срабатываний.
Модуль	module	Указан модуль, в котором произошло событие (например: Web console, Core, VPN сервер и т.п.). Относится к записям журнала событий NGFW, LogAn.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Учёт изменений	changeTracker	Указан тип изменений (журнал событий LogAn, NGFW). Возможные типы изменений пользователь может задать самостоятельно.
Данные	data	Представлена подробная информация о событии. Относится к записям журналов событий конечных устройств и Syslog.
Информация	details	Представлена подробная информация о событии из журнала событий LogAn и NGFW.
Правило	rule	Отображено название правила аналитики, межсетевого экрана, контентной фильтрации, АСУ ТП или COB.
Действие	action	Отображено действие, настроенное в правилах межсетевого экрана, контентной фильтрации, АСУ ТП или COB: • Разрешить (allow/pass/allow_webaccess): действие, настроенное в правилах межсетевого экрана, COB или контентной фильтрации. • Безопасный поиск ('safe browsing'). • Captive-портал ('captive portal'). • Предупредить (warning): действие, настроенное в правилах контентной фильтрации. • Уведомление (alert): относится к DoS защите на зоне. • NAT (nat). • DNAT (dnat). • Порт-форвардинг ('port forwarding'). • Policy-based routing ('policy based routing'). • Network mapping ('network mapping'). • Запретить (deny/drop/deny_webaccess): действие, настроенное в правилах межсетевого экрана, COB или контентной фильтрации. • Расшифровать (decrypt): действие, настроенное в правилах инспектирования. • Журналировать (log): действие, настроенное в правилах COB. • Пропускать (pass): действие, настроенное в правилах АСУ ТП. • Блокировать (drop): действие, настроенное в правилах АСУ ТП.
Приложение	application	Название приложения. Относится к записям журнала трафика, COB, Syslog, журналов правил и приложений конечных устройств.
Сетевой протокол	networkProtocol	Показан транспортный протокол подключения, использующийся для доступа к ресурсу. Относится к записям журналов трафика, COB, журнала правил конечных устройств.
Протокол прикладного уровня	httpProtocol	Указана версия HTTP протокола. Относится к записям журнала веб-доступа.
Категории сайтов	urlCategory	Отображены категории, к которым относится сайт. Относится к записям журнала веб-доступа и журнала правил конечных устройств.
Причины		Отображены причины из журнала веб-доступа (например: причина блокировки).

Наименование в базе данных	Наименование в поисковом запросе	Описание
HTTP метод	httpMethod	Отображен метод HTTP (основная операция над ресурсом). • OPTIONS: используется для определения возможностей веб-сервера или параметров соединения для конкретного ресурса. • GET: используется для запроса содержимого указанного ресурса. • HEAD: аналогичен методу GET, за исключением того, что в ответе сервера отсутствует тело. • POST: применяется для передачи пользовательских данных заданному ресурсу. • PUT: используется для загрузки содержимого запроса на указанный в запросе URI. • PATCH: аналогично PUT, но применяется только к фрагменту ресурса. • DELETE: удаляет указанный ресурс. • TRACE: возвращает полученный запрос так, что клиент может увидеть, какую информацию промежуточные серверы добавляют или изменяют в запросе. • CONNECT: преобразует соединение запроса в прозрачный TCP/IP-туннель. Относится к записям журнала веб-доступа.
Код ответа HTTP	statusCode	Отображён код состояния, являющийся частью первой строки ответа от сервера при запросах по протоколу HTTP. Относится к записям журнала веб-доступа.
Тип контента	mime	Показан тип контента. Является записью журнала веб-доступа и журнала правил конечных устройств.
URL	url	Показан URL-адрес ресурса, к которому было выполнено обращение. Относится к записям журнала веб-доступа.
Реферер	referer	Отображён URL-адрес предыдущей страницы (если есть). Относится к записям журнала веб-доступа.
Операционная система	operatingSystem	Отображён тип операционной системы устройства пользователя. Относится к записям журнала веб-доступа и COB.
User-agent	userAgent	Указан Useragent пользовательского браузера. Относится к записям журнала веб-доступа.
Сигнатуры	signature	Отображено имя сработавшей сигнатуры системы обнаружения вторжений (COB). Является параметром журнала COB.
Зона источника	zoneSource	Указана зона источника. Относится к записям журналов веб-доступа, трафика, АСУ ТП, COB.
IP источника	ipSource	Показан IP-адрес источника трафика. Относится к записям журналов веб-доступа, трафика, АСУ ТП, COB, журнала правил конечных устройств.
Порт источника	portSource	Отображён номер порта источника, через который осуществляется подключение. Относится к записям журналов веб-доступа, трафика, COB, журнала правил конечных устройств.
MAC источника	macSource	Показан MAC-адрес источника. Относится к записям журналов трафика и COB.
Зона назначения	zoneDest	Отображена зона назначения. Относится к записям журналов веб-доступа, трафика, COB, журнала правил конечных устройств.
IP назначения	ipDest	Показан IP-адрес назначения трафика. Относится к записям журналов веб-доступа, трафика, АСУ ТП, COB, журнала правил конечных устройств.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Порт назначения	portDest	Указан номер порта назначения, используемый транспортным протоколом. Относится к записям журналов веб-доступа, трафика, АСУ ТП, COB, журнала правил конечных устройств.
MAC назначения	macDest	Показан MAC-адрес назначения. Относится к записям журналов трафика и COB.
NAT адрес источника	natIpSource	Отображён NAT IP-адрес источника (если настроены правила NAT). Относится к записям журнала трафика.
NAT порт источника	natPortSource	Отображён NAT порт источника (если настроены правила NAT). Относится к записям журнала трафика.
NAT адрес назначения	natIpDest	Отображён NAT IP-адрес назначения (если настроены правила NAT). Относится к записям журнала трафика.
NAT порт назначения	natPortDest	Отображён NAT порт назначения (если настроены правила NAT). Относится к записям журнала трафика.
Байт отправлено/получено	bytesSent/bytesRecv	Отображён отправленный/полученный объём информации. Относится к записям журналов трафика и веб-доступа.
Пакетов отправлено/получено	packetSent/packetRecv	Показано количество отправленных/полученных пакетов. Относится к записям журналов трафика и веб-доступа.
Конечное устройство/сенсор	sensor	Отображено имя конечного устройства/сенсора. Относится к записям журнала событий конечных устройств.
Счётчик	counter	Название счётчика, добавленного в WMI и SNMP сенсор. Относится к записям журнала событий конечных устройств.
Объект SNMP	snmpObject	Указан идентификатор SNMP объекта (SNMP OID). Относится к записям журнала событий конечных устройств.
Тип SNMP объекта	snmpObjectType	Указан тип SNMP объекта. Относится к записям журнала событий конечных устройств.
Статус	status	Отображён результат выполнения WMI или SNMP запроса (OK или Error). Относится к записям журнала событий конечных устройств.
Ошибка	error	Показана ошибка WMI или SNMP, возникшая в результате выполнения запроса. Относится к записям журнала событий конечных устройств.
Протокол АСУТП	scadaProtocol	Указан протокол SCADA (Supervisory Control And Data Acquisition — диспетчерское управление и сбор данных). • IEC 104 (ГОСТ Р МЭК 60870-5-104). • Modbus. • DNP3 (Distributed Network Protocol). • MMS (Manufacturing Message Specification). • OPC UA (Open Platform Communications Unified Architecture). Относится к записям журнала АСУ ТП.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Уровень лога	logLevel	Указан тип события: • Audit Success (успешный аудит): событие журнала безопасности, которое происходит при успешном обращении к аудируемым ресурсам. • Audit Failure (неуспешный аудит): событие журнала безопасности, которое происходит при неуспешном обращении к аудируемым ресурсам. • Error (ошибка): событие указывает на существенные проблемы, которые могут стать причиной потери функциональности или данных. • Information (сведения): информационные события, которые, как правило, не требуют внимания администратора. • Warning (предупреждение): события указывают на проблемы, которые не требуют немедленного исправления, однако могут привести к ошибкам в будущем. Относится к записям журнала событий конечных устройств.
Источник журнала событий	logEventSource	Отображено название программного обеспечения, которое сформировало запись события в журнал. Относится к записям журнала событий конечных устройств.
Категория лога	logCategory	Указана категория лога, необходимая для упорядочивания событий. Данные берутся из Windows EventLog. Каждый источник может определять свои идентификаторы категорий. Относится к записям журнала событий конечных устройств.
Категория задачи	taskCategory	Показана категория задачи. Является записью журнала событий конечных устройств.
Имя компьютера	computerName	Представлено полное имя конечного устройства. Относится к записям журналов событий конечных устройств, Syslog.
Код события лога	logEventCode	Отображён код события лога, соответствующий определённому событию. Является записью журнала событий конечных устройств.
Идентификатор события лога	logEventId	Показан идентификатор события лога, который определяет первичный идентификатор события. Относится к записям журнала событий конечных устройств.
Тип события лога	logEventType	Отображён тип события лога. Он представлен параметрами, каждый из которых соответствует уровню лога: • 1 — уровень лога: error. • 2 — уровень лога: warning. • 3 — уровень лога: information. • 4 — уровень лога: audit success. • 5 — уровень лога: audit failure. Относится к записям журнала событий конечных устройств.
Строка вставки	insertionString	Отображены данные блока eventData события Windows. Относится к записям журнала событий конечных устройств.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Файл журнала лога	logFile	Показана информация из журнала событий конечных устройств, т.е. информация о важных программных и аппаратных событиях. Типы журналов: • Application (файл журнала приложений): для событий приложений и служб. • Security (файл журнала безопасности): для событий системы аудита. • System (файл системного журнала): для событий драйверов устройств. • CustomLog: журнал содержит события, регистрируемые приложениями, которые создают пользовательский журнал. Использование пользовательского журнала позволяет приложению управлять размером журнала или присоединять списки управления доступом в целях безопасности, не затрагивая другие приложения. Относится к записям журнала событий конечных устройств.
Команда	scadaCommand	Отображена команда управления АСУ ТП (например: чтение или запись). Относится к записям журнала АСУ ТП.
Адрес регистра	scadaAddress	Представлен адрес регистра, с которым необходимо провести операцию (запись или чтение). Относится к записям журнала АСУ ТП.
Номер ASDU	scadaAsdu	Показан адрес ASDU (COA — Common Object Address). Параметр относится к протоколу IEC-104. Относится к записям журнала АСУ ТП.
Идентификатор устройства	scadaDevice	Указан уникальный номер устройства, содержащийся в базе данных OPC-сервера. Параметр относится к протоколу OPC UA. Относится к записям журнала АСУ ТП.
Имя переменной	scadaVarname	Отображено имя переменной. Параметр, в основном, используется для обмена данными в режиме реального времени. Параметр относится к протоколу MMS. Относится к записям журнала АСУ ТП.
Хэш	hash	Показан хэш приложения. Является параметром журнала приложений конечных устройств.
Объект	facility	Отображена категория события. Относится к записям журнала Syslog. Возможны следующие значения: • Сообщения ядра. • Сообщения пользовательские. • Почтовая система. • Системный сервис. • Безопасность/авторизация. • Сообщения syslog. • Система печати LPR. • Система сетевых новостей. • Подсистема UUCP. • Сервис времени. • Безопасность/аутентификация. • FTP сервис. • Система NTP. • Аудит. • Тревога. • Сервис времени 2. • Local 0 — Local7.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Критичность	syslogSeverity	Указана критичность событий журнала Syslog. • Экстренная: критическое состояние, которое сказывается на работоспособности системы. • Тревога: состояние, требующее незамедлительного вмешательства. • Критическая: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. • Ошибки: несрочные сбои в системе. • Предупреждения: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. • Уведомительная: события, которые относятся к необычному поведению системы, но не являются ошибками. • Информативная: информационные уведомления. • Отладочная: информация, полезная разработчикам для отладки приложений.
Идентификатор процесса	processId	Указан идентификатор процесса. Относится к записям журнала Syslog.

Администратор может выбрать для показа только те столбцы, которые ему необходимы. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

Действия реагирования

Product: LogAn
Version: 7.0.1
Documentation: ☒

Действия реагирования позволяют определить методы реагирования при срабатывании правил аналитики информационной безопасности. LogAn позволяет гибко настраивать правила, используя переменные, относящиеся к категориям срабатывания правил аналитики.

Переменные для уведомлений и команд

ПримечаниеПоле чувствительно к регистру букв. Название переменных необходимо вводить прописными буквами в фигурных скобках (как представлено в таблице).
ПримечаниеИспользование переменных в командах и уведомлениях возможно в случае, если они были выбраны в разделе Аналитика → Правила аналитики → Условия для группировки событий.

Наименование	Описание
{ANALYTICS_RULE_NAME}	Название правила аналитики.
{ANALYTICS_RULE_DESCRIPTION}	Описание правила аналитики.
{NAME}	Название определённого срабатывания.
{TIME}	Время срабатывания правила аналитики.
{TRIGGERED_ALERTS_NUMBER}	Количество срабатываний.
{FIRST_TRIGGERED_ALERT_TIME}	Время первого срабатывания.
{LAST_TRIGGERED_ALERT_TIME}	Время последнего срабатывания.
{TRIGGERED_ALERTS_NAMES}	Список названий срабатываний, если используется группировка.
{FIRST_EVENT_TIME}	Время первого события, попавшего под срабатывание правила аналитики.
{LAST_EVENT_TIME}	Время последнего события, попавшего под срабатывания правила аналитики.
{THREAT_LEVEL}	Указанный уровень угрозы.
{CATEGORY}	Категория, к которой относится срабатывание.
{PRIORITY}	Приоритет срабатывания правила аналитики.
{ADMINISTRATOR_NAME}	Имя администратора, которым было создано правило аналитики.
{USER_NAME}	Имя пользователя.
{SOURCE_ZONE}	Зона источника.
{DESTINATION_ZONE}	Зона назначения.
{SOURCE_COUNTRY}	Страна источника.
{DESTINATION_COUNTRY}	Страна назначения.

Наименование	Описание
{SOURCE_IP}	IP-адрес источника.
{SOURCE_PORT}	Порт источника.
{DESTINATION_IP}	IP-адрес назначения.
{DESTINATION_PORT}	Порт назначения.
{SOURCE_ZONE_ALL}	Зоны источников всех событий, сформировавших срабатывание.
{DESTINATION_ZONE_ALL}	Зоны назначения всех событий, сформировавших срабатывание.
{SOURCE_COUNTRY_ALL}	Страны источников всех событий, сформировавших срабатывание.
{DESTINATION_COUNTRY_ALL}	Страны назначения всех событий, сформировавших срабатывание.
{SOURCE_IP_ALL}	IP-адреса источников всех событий, сформировавших срабатывание.
{SOURCE_PORT_ALL}	Порты источников всех событий, сформировавших срабатывание.
{DESTINATION_IP_ALL}	IP-адреса назначения всех событий, сформировавших срабатывание.
{DESTINATION_PORT_ALL}	Порты назначения всех событий, сформировавших срабатывание.

Действия могут быть созданы во вкладке **Аналитика → Действия реагирования** . При добавлении действия необходимо указать следующие параметры.

Наименование	Описание
Включено	Включает/отключает правило реагирования.
Название	Отображает название правила реагирования.
Описание	Описывает правила реагирования. Данное поле необязательно для заполнения.
Действие	Показывает действие, выбранное для исполнения в случае срабатывания правила аналитики. Действие реагирования выполнится, если оно указано в свойствах правила аналитики. Для выбора доступны следующие виды реагирования: • Отправить email: отправка письма на выбранные почтовые адреса. Настройка действия Отправить email будет рассмотрена далее в разделе Действие типа отправить email. • Отправить сообщение: отправка сообщения на указанные номера телефонов. Настройка действия Отправить сообщение будет рассмотрена далее в разделе Действие типа отправить сообщение. • Webhook: получение уведомления о срабатывании правила на веб-странице, адрес которой был указан при настройке действия. Настройка действия Webhook будет рассмотрена далее в разделе Действие типа webhook. • Создать инцидент: автоматическое создание инцидента в результате срабатывания правил аналитики. О настройке действия Создать инцидент читайте в разделе Настройки инцидентов. • Послать команду на коннектор — отправка команды на выбранный коннектор. Настройка действия Послать команду на коннектор будет рассмотрена далее в разделе Действие типа послать команду на коннектор. • Послать команду на эндпоинт — отправка команды на конечное устройство с установленным ПО UserGate Client. Подробнее читайте в раздел Действие типа послать команду на эндпоинт.

Наименование	Описание
Записывать в журнал правил	Включает/отключает журналирование данных о срабатывании действия реагирования. Данные записываются в журнал событий Log Analyzer, который можно просмотреть во вкладке Журналы и отчёты → Журналы Log Analyzer → Журнал событий .
Группировать похожие срабатывания	Для удобства при настройке действий реагирования возможно использование функции группировки срабатываний. Группировка возможна по следующим параметрам: • Никогда. • За период времени. При настройке группировки срабатываний правила аналитики за период времени действие реагирования выполнится, если в течение указанного времени произошло хотя бы одно срабатывание. • По количеству срабатываний. При настройке группировки по количеству срабатываний правила аналитики действие реагирования выполнится только после указанного количества срабатываний.
Период группировки	Отображает период группировки в минутах. Задание параметра возможно только при выборе группировки похожих срабатываний за период времени.
Количество срабатываний	Отображает заданное количество срабатываний. Задание параметра возможно только при выборе группировки похожих срабатываний по количеству срабатываний.

Созданные действия реагирования можно редактировать, удалять, копировать, включать, отключать. Также в списке действий реагирования можно отображать все действия, только включённые или только выключенные.

Действие типа отправить email

Если в качестве действия реагирования была выбрана отправка email, то в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
Профиль оповещения	Профиль оповещения SMTP, который будет использован для отправки email. Подробнее о настройке профилей SMTP читайте в главе Профили оповещений .
От	Имя отправителя письма.
Тема	Тема письма.
Почтовые адреса	Список почтовых адресов получателей. Получатели должны быть добавлены в списки в разделе Настройки → Библиотеки → Почтовые адреса . О добавлении почтовых адресов читайте в разделе Почтовые адреса .
Шаблон	Шаблон письма уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд .

Действие типа отправить сообщение

Если в качестве действия реагирования была выбрана отправка сообщения, то в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
Профиль оповещения	Профиль оповещения SMPP, который будет использован для отправки сообщения. Подробнее о настройке профилей SMPP читайте в главе Профили оповещений .
От	Имя отправителя письма.

Наименование	Описание
Номера телефонов	Список номеров телефонов получателей. Получатели должны быть добавлены в списки в разделе Настройки → Библиотеки → Номера телефонов . О добавлении телефонных номеров читайте в разделе Номера телефонов .
Шаблон	Шаблон сообщения с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд .

Действие типа webhook

Для настройки webhook в свойствах правила реагирования необходимо указать следующие параметры.

Наименование	Описание
URL	Адрес веб-сайта, на котором будут отображаться оповещения о срабатывании правила.
Шаблон	Шаблон уведомления с возможностью передачи значений различных переменных, относящихся к срабатыванию. Подробнее читайте в разделе Шаблон уведомлений и Переменные для уведомлений и команд .

Для тестирования webhook можно воспользоваться сервисом <https://webhook.site>. Для этого необходимо перейти на сайт [Webhook.site](#) и скопировать сгенерированную ссылку. Далее её необходимо указать в свойствах правила реагирования в поле **URL** во вкладке **Действия**.

Действие типа послать команду на коннектор

В качестве одного из действий реагирования может быть настроена отправка команды на коннектор.

Если в качестве действия реагирования настроена передача команды для исполнения на коннекторе, то необходимо указать следующие параметры:

Наименование	Описание
Коннекторы	Выбор устройств, на которые необходимо отправить команду в случае срабатывания правила аналитики. Коннектор должен быть заранее добавлен и настроен в разделе Сенсоры --> Коннекторы вкладки Настройки веб-интерфейса управления LogAp (для более подробной информации обратитесь к разделу Коннекторы). Важно! Могут выбраны только коннекторы с одинаковой группой команд.
Команда	Определение команды, которая будет передана на коннектор для выполнения; представлены команды группы, указанной для выбранных коннекторов. В случае наличия в команде переменных, будут отображены дополнительные поля для указания их значений. Подробнее о командах читайте в разделе Команды .

Действие типа послать команду на эндпоинт

В качестве одного из действий реагирования может быть настроена отправка команды на конечное устройство с установленным ПО UserGate Client. Доступны следующие команды:

- **Отключить от сети** — блокировка доступа к сети Интернет.
- **Завершить процесс** — завершение указанного в запросе фильтра процесса.

Шаблон уведомлений

Во вкладке **Шаблон** необходимо указать текст уведомления. Можно передавать не только фиксированный текст, но и данные, относящиеся к срабатыванию или его записям в журнале.

Чтобы передать данные, относящиеся к срабатыванию, необходимо в поле во вкладке **Шаблон** ввести название одного из параметров, представленных в таблице. Например, если ввести **{ANALYTICS_RULE_NAME}**, то в тексте уведомления, настроенном как отправка email, SMS или webhook, будет отражено название правила аналитики, которое сработало. Если заполнить шаблон при настройке действия **Создать инцидент**, то текст будет отображён в описании инцидента.

Срабатывания

Version: 7.0.1
Product: LogAn
Documentation: ☒

Во вкладке **Срабатывания** показан список срабатываний правил аналитики и отображена краткая информация о них. Срабатывание — это набор событий, объединенных правилом аналитики.

Можно увидеть следующую информацию о срабатываниях.

Наименование	Описание
Узел	Показан уникальный код, соответствующий устройству.
Время	Указаны дата и время срабатывания правила аналитики.
ID	Отображен идентификатор срабатывания.
Время первого события	Показано время первого события, попавшего под срабатывание правила аналитики.
Время последнего события	Показано время последнего события, попавшего под срабатывание правила аналитики.
Количество событий	Показано количество событий, попавших под срабатывание правила аналитики.
Правило	Отображено название правила аналитики, которое сработало.
Категория	Отображена категория, к которой относится срабатывание. По умолчанию для выбора доступны следующие категории: • Security: правила данной категории определяют инциденты, приводящие к ухудшению безопасности информационных систем. • Availability: правила данной категории определяют инциденты, которые приводят к ухудшению доступности информационных систем. • Performance: правила данной категории определяют инциденты, которые приводят к ухудшению производительности информационных систем. Дополнительные категории срабатываний правил аналитики могут быть созданы во вкладке Настройки в разделе Библиотеки → Категории срабатываний.
Приоритет	Показан приоритет срабатывания, указанный при настройке правила аналитики: • Низкий: данные правила обладают низким приоритетом реагирования. • Нормальный: на данные правила необходимо обратить внимание и, возможно, предпринять меры. • Важный: на данные правила необходимо обратить внимание и предпринять меры. • Критический: данные правила требуют незамедлительного реагирования. Установленный приоритет указывает на важность срабатывания.
Пользователь	Указано имя пользователя.
Сигнатуры	Отображено имя сработавшей сигнатуры COB.
Зона источника	Отображена зона, из которой происходит подключение.
IP источника	Показан IP-адрес источника.

Наименование	Описание
Порт источника	Указан порт источника.
Зона назначения	Отображена зона назначения.
IP назначения	Показан IP-адрес назначения.
Порт назначения	Указан порт назначения.

Администратор может выбрать для показа только те столбцы, которые ему необходимы. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

Доступны два режима поиска: простой и расширенный. Простой режим использует графический интерфейс, расширенный поиск предназначен для формирования более сложных фильтров поиска с использованием специального языка запросов, о синтаксисе которого написано в разделе [Поиск и фильтрация данных](#).

Нажатием кнопки **Сохранить как** можно сохранить настроенный фильтр. Список сохранённых фильтров поиска можно просмотреть, нажав на кнопку **Популярные фильтры**.

Чтобы посмотреть карточку срабатывания (краткую информацию о выбранном срабатывании), необходимо нажать кнопку **Показать**.

Нажатие кнопки **Показать подробно** произведёт перевод на вкладку Подробности срабатывания, где отображена подробная информации о выбранном срабатывании. О вкладке **Подробности срабатывания** читайте в соответствующей главе [Подробности срабатывания](#).

Выбранное срабатывание правила аналитики можно добавить в инцидент нажатием одноимённой кнопки **Добавить в инцидент**.

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

Подробности срабатывания

Version: 7.0.1
 Product: LogAn
 Documentation: ☒

На данной вкладке отображена подробная информация о срабатывании правила аналитики и отображаются все события, попавшие в данное срабатывание.

Данные могут быть представлены в табличном или текстовом виде. Переключение между режимами осуществляется нажатием кнопок **Переключить в текстовый вид** или **Переключить в табличный вид**, находящихся внизу экрана.

Представлена следующая информация о срабатывании.

Наименование	Описание
Срабатывание	Показан идентификатор срабатывания.
Время	Указано время срабатывания правила аналитики. Отображается в часовом поясе, настроенном на LogAn.
Приоритет	Отображён установленный при настройке приоритет срабатывания. Низкий: данные правила обладают низким приоритетом реагирования. Нормальный: на данные правила необходимо обратить внимание и, возможно, предпринять меры. Важный: на данные правила необходимо обратить внимание и предпринять меры. Критический: данные правила требуют незамедлительного реагирования.
Правило	Показано название правила аналитики, которое сработало.
Поиск инцидента	Нажатие данной кнопки производит поиск инцидента, в котором используется данное срабатывание.
Список событий	Показаны события, которые попали в данное срабатывание.

Нажатие кнопки **Показать срабатывания** произведёт перевод на вкладку **Срабатывания**, где будет отображён список срабатываний выбранного правила аналитики.

Процессы конечных устройств

Version: 7.0.1

Product: LogAn

Documentation: ☒

Во вкладке **Процессы конечных устройств** отображён список процессов устройств с установленным ПО UserGate Client. Она позволяет отследить цепочку вызова процессов, а также разобраться в параметрах запуска и просмотреть полезную информацию о файле. Вкладка представлена двумя панелями: **Лог процессов** и **Процесс**.

На панели **Лог процессов** отображён список процессов конечных устройств (процессы запущенных приложений, фоновые процессы, процессы Windows), передающих информацию на UserGate Log Analyzer. Для просмотра доступна следующая информация:

- дата и время запуска;
- название конечного устройства;
- приложение;
- идентификатор процесса.

Для удобства записи могут быть отфильтрованы по различным критериям, например таким, как диапазон дат, название приложения, идентификатор процесса и т.п. Фильтрация также возможна с использованием расширенного поиска для формирования сложных фильтров; в режиме расширенного поиска используется специальный язык запросов, синтаксис которого рассмотрен далее в разделе [Поиск и фильтрация данных](#).

Администратор может выбрать только те столбцы для показа, которые ему необходимы. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

Выделив процесс можно просмотреть дерево процесса и подробную информацию о нём. Дерево процесса и подробная информация будут отображены на панели **Процесс**.

Инциденты

Общие сведения

Documentation: ☒

Version: 7.0.1

Product: LogAn

Раздел **Инциденты** предоставляет функционал встроенной в LogAn системы IRP — платформы управления процессами реагирования на инциденты информационной безопасности. Инцидентом считается событие или набор событий информационной безопасности, которые подлежат расследованию. LogAn позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании (подробнее читайте разделе [Настройки инцидентов](#)).

IRP система плотно интегрирована с системой SIEM, функционал которой представлен разделом [Аналитика](#). Раздел **Аналитика** позволяет задать создание инцидента в качестве действия реагирования, тем самым автоматизируя процесс создания инцидентов информационной безопасности (подробнее о настройке действий реагирования читайте в разделе [Действия реагирования](#)).

Также, помимо автоматического создания, инциденты могут быть созданы вручную инженером информационной безопасности (подробнее читайте в разделе [Создание инцидентов безопасности](#)).

Настройки инцидентов

Version: 7.0.1
Product: LogAn
Documentation: ☒

Процесс расследования инцидента проходит в несколько этапов, на каждом из которых инциденту присваивается определенный статус или **Состояние**, например, **Открыт → Сбор данных → В работе → Закрыт**. Переход между состояниями возможен по определенным правилам, определяемыми администратором, например, нельзя перейти из состояния **Открыт** сразу в состояние **Закрыт**. Возможные переходы между состояниями инцидентов описываются в **Схеме инцидентов**.

По окончании расследования каждому инциденту присваивается **Решение**, например, ложная атака, подтвержденная атака, выполнено и т.п.

Тип инцидента выбирается на этапе создания инцидента и определяет назначение инцидента. Например, типом инцидента может быть Инцидент безопасности, Задача и т.п.

Схема инцидента связывает воедино состояния, возможные переходы между состояниями, решения и типы инцидентов, формируя процесс расследования инцидента информационной безопасности.

UserGate LogAn позволяет настроить процесс расследования инцидентов индивидуально под нужды конкретной компании. После первоначальной установки решения создается схема расследования по умолчанию с названием **Incident**. Администратор системы может изменить существующую схему или создать свою собственную схему. Можно создать несколько схем расследования инцидентов, но использоваться может только одна схема, которая является активной.

Чтобы создать свою собственную схему расследования инцидентов необходимо выполнить следующие действия:

Наименование	Описание
Шаг 1. Создайте необходимые решения инцидентов	В разделе Настройки инцидентов → Решения инцидентов нажмите добавить, укажите название и описание создаваемого решения и нажмите кнопку Сохранить .
Шаг 2. Создайте типы инцидентов	В разделе Настройки инцидентов → Типы инцидентов нажмите добавить, укажите название и описание создаваемого типа и нажмите кнопку Сохранить .
Шаг 3. Создайте состояния инцидентов	В разделе Настройки инцидентов → Состояния инцидентов нажмите добавить, укажите название, описание и группу создаваемого состояния. Группа состояние определяет положение данного состояние в схеме состояний. Возможно 3 варианта: • Открыто — данная группа назначается состояниям инцидентов, по которым еще не начата работа или она приостановлена. Как правило, это начальные состояния инцидентов, например Создан. Все состояния данной группы помечаются синим цветом в веб-консоли. • В работе — данная группа назначается состояниям инцидентов, по которым ведется, но еще не завершена работа. Это промежуточные состояния инцидентов, например, В работе, Расследование. Все состояния данной группы помечаются желтым цветом в веб-консоли. • Закрыто — данная группа назначается состояниям инцидентов, по которым завершена работа. Это конечные состояния инцидентов, например, Завершено, Закрыто. При переходе в состояние этой группы необходимо обязательно указать решение инцидента, например, Ложная атака, Подтвержденная атака, Выполнено. Все состояния данной группы помечаются зеленым цветом в веб-консоли. После определения всех полей нажмите кнопку Сохранить.

Наименование	Описание
Шаг 4. Создайте схему инцидентов	В разделе Настройки инцидентов → Схемы инцидентов нажмите добавить и укажите следующие параметры: • Сделать активной — делает данную схему активной. Только одна схема может быть активной, если была активна другая схема, то данное действие сделает ее не активной, и все новые и существующие инциденты перейдут на работу по новой схеме. • Схема — название схемы. • Префикс — префикс, который будет использован при назначении идентификаторов создаваемым инцидентам. Идентификатор будет иметь вид Префикс — порядковый номер, например INC-99. • Описание — необязательное описание данной схемы. • Состояния рабочего процесса — описывает все состояния, которые может принимать инцидент в своем жизненном цикле. Добавьте сюда все состояния инцидентов, созданные на предыдущем шаге. • Начальное состояние — указывает начальное состояние, которое принимает инцидент при его создании. • Переходы — необходимо указать все возможные переходы между состояниями и дать им названия. Например, создать переход под названием Взять в работу для перехода из состояния Открыто в состояние В работе. Перевод инцидента между состояниями возможен только для тех состояний, между которыми определены переходы. • Решения инцидентов — указывает список возможных решений инцидентов. Решение является обязательным при завершении работы по расследованию тикета, то есть при переводе его в состояние, относящееся к группе закрыто. Выберите все необходимые решения, которые были созданы ранее. • Типы инцидентов — укажите типы инцидентов, которые могут быть использованы в этой схеме.
Шаг 5. Активируйте схему инцидентов	После создания схемы инцидентов ее необходимо активировать. Для этого активируйте чекбокс Сделать активной в настройках схемы инцидентов.

Дашборд по инцидентам

Version: 7.0.1
Product: LogAn
Documentation: ☒

В данной вкладке можно просмотреть текущее состояние инцидентов информационной безопасности, созданных на LogAn. Отчеты представлены в виде виджетов, которые могут быть настроены администратором системы в соответствии с его требованиями. Виджеты можно добавлять, удалять, изменять расположение и размер на странице Дашборд.

Некоторые виджеты позволяют настроить отображение, указать фильтрацию данных и настроить прочие параметры. Для настройки виджета необходимо кликнуть по символу шестеренки в правом верхнем углу. Не все параметры, перечисленные ниже, доступны для каждого типа виджетов.

Наименование	Описание
Название	Название виджета, которое будет отображено в Дашборд.
Диаграмма	Тип представления данных: • Число. • Вертикальная гистограмма. • Таблица.
Запрос фильтра	SQL-подобная строка запроса, позволяющая ограничить объем информации, используемой при построении виджета.
Описание	Описание виджета.
Количество записей	Максимальное количество записей для отображения.

Журнал инцидентов

Product: LogAn
Version: 7.0.1
Documentation: ☒

Во вкладке **Журнал инцидентов** представлен список созданных инцидентов информационной безопасности. В таблице отражена следующая информация об инцидентах.

Наименование в базе данных	Наименование в поисковом запросе	Описание
Создан	date	Дата и время создания инцидента.
Изменён	updateDate	Дата и время последнего изменения.
Индекс	incidentPrefix	Префикс инцидента (INC-N, где N — порядковый номер инцидента; нумерация начинается с 0).
Имя	incidentName	Название инцидента.
Правило	rule	Название правила аналитики, в результате срабатывания которого автоматически был создан инцидент, т.е. при настройке правила аналитики было задано действие реагирования Создать инцидент .
Статус	status	Статус инцидента. Существует 3 группы состояний, которые определяют положение данного состояние в схеме состояний: • Открыто — данная группа назначается состояниям инцидентов, по которым еще не начата работа или она приостановлена. Как правило, это начальные состояния инцидентов, например Создан. Все состояния данной группы помечаются синим цветом в веб-консоли. • В работе — данная группа назначается состояниям инцидентов, по которым ведется, но еще не завершена работа. Это промежуточные состояния инцидентов, например, В работе, Расследование. Все состояния данной группы помечаются желтым цветом в веб-консоли. • Закрыто — данная группа назначается состояниям инцидентов, по которым завершена работа. Это конечные состояния инцидентов, например, Завершено, Закрыто. При переходе в состояние этой группы необходимо обязательно указать решение инцидента, например, Ложная атака, Подтвержденная атака, Выполнено. Все состояния данной группы помечаются зеленым цветом в веб-консоли. По умолчанию в UserGate создана схема Incident, которая содержит переходы между всеми состояниями. Схемы инцидентов можно добавить в разделе Настройки → Настройка инцидентов → Схема инцидентов. Дополнительные состояния инцидентов можно задать во вкладке Настройки → Настройка инцидентов → Состояния инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Решение	resolution	Решение инцидента. По умолчанию созданы: • False positive: ложная атака. • True positive: подтверждённая атака. • Duplicate: проблема повторяет другую проблему. • Won't do: задача не выполняма. • Done: проблема решена. Дополнительные решения инцидентов можно создать во вкладке Настройки → Настройка инцидентов → Решения инцидентов. Подробнее читайте в разделе Настройки инцидентов.
Тип	type	Тип инцидента. По умолчанию доступны 2 типа: инцидент безопасности и задача. Дополнительно типы инцидентов можно создать в разделе Настройки → Настройка инцидентов → Типы инцидентов . Подробнее читайте в разделе Настройки инцидентов .

Наименование в базе данных	Наименование в поисковом запросе	Описание
Приоритет	priority	Приоритет инцидента: • Низкий. • Нормальный. • Важный. • Критический.
Инициатор	reporter	Имя администратора, который создал инцидент.
Последнее изменение	lastChangeBy	Имя администратора, который внёс последнее изменение.
Назначен	assignee	Имя администратора, назначенного на инцидент.
Активность		Количество комментариев, срабатываний правил аналитики и журналов событий, добавленных в инцидент.

Администратор может выбрать для показа только те столбцы, которые ему необходимы. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

Возможно производить фильтрацию инцидентов по параметрам, представленным в таблице. Фильтрация доступна в двух режимах: простой и расширенный (подробнее о синтаксисе расширенного поиска читайте в разделе [Поиск и фильтрация данных](#)).

Настроенные фильтры можно сохранять, нажав кнопку **Сохранить как**. Сохранённые фильтры можно просмотреть с использованием кнопки **Популярные фильтры**.

Нажатием кнопки **Экспортировать в CSV** администратор может скачать отфильтрованный список инцидентов в csv-файл для дальнейшего анализа.

Создание инцидентов безопасности

Version: 7.0.1
Product: LogAn
Documentation: ☒

Во вкладке **Журнал инцидентов** также можно создавать инциденты информационной безопасности. Для создания и работы с инцидентами информационной безопасности пользователь должен обладать определёнными ролевыми разрешениями (подробнее читайте в разделе [Роли и ролевые разрешения пользователей](#)).

Инциденты создаются нажатием кнопки **Создать инцидент**. Далее необходимо указать следующие параметры.

Наименование	Описание
Имя	Указать название инцидента информационной безопасности.
Тип	Указать тип инцидента. По умолчанию созданы 2 типа инцидентов: инцидент безопасности и задача. Дополнительно типы инцидентов могут быть созданы в разделе Настройки → Настройка инцидентов → Типы инцидентов . Подробнее читайте в разделе Настройки инцидентов .
Приоритет	Назначить приоритет - Низкий. - Нормальный. - Важный. - Критический.
Назначен	Назначить ответственного на инцидент.
Наблюдатели	Указать список сотрудников для наблюдения за инцидентом. При любых изменениях инцидента они будут получать уведомление.
Вложения	Прикрепить файлы, относящиеся к инциденту.
Описание	Ввести описание инцидента.

Подробнее инцидента

Version: 7.0.1
 Product: LogAn
 Documentation: ☒

Выбор инцидента и нажатие кнопки **Показать** произведет перевод на новую вкладку (название вкладки формируется из индекса и заданного имени инцидента), где будет отображена подробная информация о выбранном инциденте. На данной вкладке также можно редактировать (кнопка **Редактировать**) и комментировать (кнопка **Комментировать**) инцидент, изменять ответственного за инцидент (кнопка **Назначить**), и статус рабочего процесса (кнопка **Рабочий процесс**). Помимо информации об инциденте, отображённой во вкладке **Журнал инцидентов** (подробнее читайте в разделе [Журнал инцидентов](#)), можно увидеть следующую информацию.

В разделе **Срабатывания** отражена информация о срабатываниях правил аналитики, добавленных в инцидент. Подробнее читайте в разделе [Срабатывания](#). Добавить срабатывания в инцидент можно нажатием кнопки **Добавить срабатывания**. Далее необходимо выбрать срабатывания, которые необходимо добавить в инцидент. Чтобы просмотреть подробности срабатывания выделите нужное срабатывание правила аналитики и нажмите кнопку **Показать подробно**. Также можно просмотреть краткую информацию о срабатывании нажав на кнопку **Показать**. Нажатием на кнопку **Удалить из инцидента** можно удалить запись о срабатывании правила аналитики из инцидента. Список срабатываний правил аналитики, добавленный в инциденты, можно скачать в csv-файл для дальнейшего анализа нажатием кнопки **Экспортировать в CSV**.

В разделе **Журналы** отображена подробная информация о событиях всех журналов (подробнее о записях журналов читайте в разделе [Поиск](#)). Чтобы добавить события в инцидент нажмите **Добавить в инцидент** и выберите события для добавления. Нажатие кнопки **Удалить из инцидента** позволяет удалить ненужные события.

В разделе **Улики** отображены записи о наблюдениях за объектами, указанными при настройке. Улики необходимы для упрощения анализа инцидента информационной безопасности, принятия верного решения и уменьшения затраченного на инцидент времени. Для получения информации используются ресурсы для обогащения (подробнее читайте в разделе [Внешние сервисы обогащений](#)). Подробную информацию, предоставленную сервисом, можно увидеть в настройках обогащения, нажав на обогащение.

Улики можно создать нажатием кнопки **Добавить**. Далее необходимо указать параметры, которые будут отражены в таблице раздела.

Наименование	Описание
Тип улики	Возможен выбор одного из следующих типов улик: Автономная система: система IP-сетей и маршрутизаторов, находящихся под единым управлением. Домен: имя сайта в Интернете. Файл: файл, о котором необходимо собрать информацию. Имя файла: название файла, о котором необходимо собрать информацию. FQDN: полное доменное имя. Хэш: хэш какого-либо файла, например, добавленного в инцидент. Имя хоста: метка устройства, подключённого к компьютерной сети и используемая для идентификации устройства. IP: уникальный адрес, идентифицирующий устройство в компьютерной сети. Почта: адрес электронной почты. Тема письма: часть письма, указанная в поле subject. Реестр: ключ реестра Microsoft Windows — каталог, в котором хранятся настройки и параметры операционной системы. Путь URI: последовательность символов, идентифицирующая абстрактный или физический ресурс. URL: индивидуальный адрес ресурса в сети Интернет. Агент пользователя: буквенно-цифровая строка, идентифицирующая программу, которая отправляет запрос на сервер и одновременно запрашивает доступ к web-сайту. Другое.
Значение	Необходимо указать объект, с которым будет производиться работа: IP-адрес, домен, и т.п.

Наименование	Описание
Тип атаки	Для указания доступны следующие типы атаки: • Ботнет — сеть заражённых компьютеров, удалённо управляемых преступниками. • Фишинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. • Вредоносное ПО — любое программное обеспечение, которое пытается заразить компьютер или мобильное устройство. • DDoS — способ заблокировать работу сайта путем подачи большого количества запросов, превышающих пропускную способность сети. • Угон трафика — злоумышленное перенаправление трафика. • Сетевое сканирование — сканирование узлов сети для определения уязвимостей. • Брутфорс — метод взлома учётных записей путём подбора паролей к ним. • Компроментация — факт несанкционированного доступа к защищенной информации, а также подозрение осуществления такого доступа. • Спам — массовая рассылка с использованием специальных программ, коммерческой, политической и иной рекламы или иного вида сообщений людям, не выразившим желания их получать. • Другое.
TLP	Отобрана маркировка конфиденциальной информации (Traffic Light Protocol). Возможны следующие маркировки: • RED: информация является крайне конфиденциальной. • AMBER: информацией можно поделиться в рамках своей организации, при условии, что этой информацией нужно поделиться. • GREEN: информация может быть широко распространена в пределах определённого сообщества. • WHITE: информация в свободном распространении, но не нарушает авторские права.
Индикатор компроментации?	Чекбокс необходимо отметить, если объект является потенциальным индикатором компроментации.
Сервисы	Отображён список сервисов, которые используются для получения дополнительной информации об объектах наблюдения. Список сервисов отображается автоматически после выбора типа улики. Список сервисов доступен в разделе Настройки → Библиотеки → Внешние сервисы обогащений . Подробнее читайте в разделе Внешние сервисы обогащений .
Обновлено	Показаны дата и время последнего обновления сервиса.

С использованием соответствующих кнопок **Редактировать** и **Удалить** улики можно редактировать или удалять.

В разделе **Активность** можно просмотреть комментарии по инциденту и историю внесения изменений (добавление наблюдателей, изменение статуса рабочего процесса и т.д.).

С использованием кнопки **Создать отчёт** можно создать отчёт об инциденте:

- **Incident report:** пользовательский отчёт, который может быть создан на английском или русском языках в формате PDF или HTML. При создании отчёта возможно использование шаблонов, список которых доступен в разделе **Журналы и отчёты → Отчёты инцидентов → Правила отчётов инцидентов**.
- **GOSSOPKA report:** для создание отчёта используется шаблон **Форма для ГОССОПКА**, который соответствует требованиям к отчётам ГОССОПКА. Отчёт можно просто скачать (кнопка **Создать файл**) или сразу сформировать в требуемом формате и отправить в систему личных кабинетов ГОССОПКА (кнопка **Послать через сеть**). Для автоматической отправки отчёта пользователю необходимо предоставить учётную запись для входа в личный кабинет на сайте ГОССОПКА и защищённый канал передачи. Подробнее читайте в разделе [Передача отчётов об инцидентах информационной безопасности в ГосСОПКА](#).

Передача отчётов об инцидентах информационной безопасности в ГосСОПКА

Version: 7.0.1
Product: LogAn
Documentation: ☒

ГосСОПКА — Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Целью создания ГосСОПКА является защита критической информационной инфраструктуры (КИИ), владельцы объектов которой должны подключиться к ГосСОПКА. Также к ГосСОПКА можно подключиться и на добровольной основе для обеспечения более высокого уровня информационной безопасности и улучшения методов выявления и реагирования на инциденты.

В LogAn реализована возможность передачи отчётов о компьютерных атаках, инцидентах и уязвимостях в стандартизированном формате через личный кабинет ГосСОПКА.

Для отправки отчётов необходимо:

- 1. Самостоятельно подключиться к системе личных кабинетов ГосСОПКА.

Подключение необходимо для взаимодействия и автоматизации обмена информацией о зафиксированных инцидентах информационной безопасности и методах их предотвращения с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак.

- 2. Добавить криптографический шлюз для организации межсетевого взаимодействия с сетью НКЦКИ (Национальный координационный центр по компьютерным инцидентам; главный центр ГосСОПКА).

Для самостоятельного подключения к ГосСОПКА используются аппаратно-программные комплексы компаний Инфотекс (ViPNet), Код безопасности (Континент), С-Терра (С-Терра Шлюз).

Примечание Не указывайте криптографический шлюз в качестве шлюза по умолчанию.

- 3. Добавить DNS-серверы для определения адреса системы личных кабинетов ГосСОПКА.

Для определения адреса системы личных кабинетов ГосСОПКА необходимо добавить серверы с адресами 10.0.100.49 и 10.0.100.50.

Примечание В список системных DNS-серверов можно добавить не более трёх серверов. Серверы ГосСОПКА не могут быть использованы для преобразования доменных имён в сети Интернет.

- 4. Настроить статический маршрут в сеть ГосСОПКА для обеспечения доступности DNS-серверов, указанных в пункте 3.

Для обеспечения доступности серверов ГосСОПКА необходимо добавить статический маршрут с адресом назначения: 10.0.100.0/24. Подробнее о настройке маршрутов читайте в разделе [Маршруты](#).

- 5. Настроить подключение к личному кабинету ГосСОПКА с LogAn для возможности отправки отчёта.

В LogAn по умолчанию создан коннектор **Gossopka**, предназначенный для взаимодействия с ГосСОПКА.

Для настройки коннектора перейдите во вкладку **Настройки** в раздел **Сенсоры → Коннектор**. Используйте коннектор **Gossopka**, созданный в LogAn по умолчанию; необходимо указать: FQDN личного кабинета, вместо указанного по умолчанию (значение по умолчанию отображает формат, в котором должно быть указано значение поля), логин/пароль и ключ API, который добавляется в поле HTTP заголовки.

- 6. Настроить шаблон отчёта.

По умолчанию создан шаблон **Форма для ГОССОПКА**, соответствующий требованиям ГосСОПКА к отчётам. Заполните поля формы; данная форма будет использоваться при формировании отчёта.

Наименование	Описание
Организация	Название организации.
Категория	Категория уведомления: - уведомление о компьютерном инциденте; - уведомление о компьютерной атаке; - уведомление о наличии уязвимости.

Наименование	Описание
Тип события ИБ	Тип события информационной безопасности: • вовлечение контролируемого ресурса в инфраструктуру ВПО; • замедление работы ресурса в результате DDoS-атаки; • заражение ВПО; • захват сетевого трафика; • использование контролируемого ресурса для фишинга; • компрометация учётной записи; • несанкционированное изменение информации; • несанкционированное разглашение информации; • публикация на ресурсе запрещённой законодательством РФ информации; • рассылка спам-сообщений с контролируемого ресурса; • успешная эксплуатация уязвимости.
Статус реагирования на инцидент	Статус реагирования на инцидент: • меры приняты; • проводятся мероприятия по реагированию; • возобновлены мероприятия по реагированию.
Необходимость привлечения сил ГосСОПКА	Отметьте флаг в случае необходимости привлечения сил ГосСОПКА.
Краткое описание события ИБ	Описание события информационной безопасности.
Сведения о средстве или способе выявления инцидента	Информация о способе и устройстве/ПО, посредством которого был выявлен инцидент.
Дата и время выявления инцидента	Дата и время выявления инцидента заполняются автоматически.
Дата и время завершения инцидента	Дата и время завершения инцидента заполняются автоматически.
Ограничительный маркер TLP	Маркировка конфиденциальной информации (Traffic Light Protocol). Возможны следующие маркировки: • RED: информация является крайне конфиденциальной; • AMBER: информацией можно поделиться в рамках своей организации, при условии, что этой информацией нужно поделиться; • GREEN: информация может быть широко распространена в пределах определённого сообщества; • WHITE: информация в свободном распространении, но не нарушает авторские права.
Влияние на доступность	Потенциальное влияние на доступность информационных ресурсов: • отсутствует; • низкое; • высокое.
Влияние на целостность	Потенциальное влияние на целостность ресурсов информационной системы: • отсутствует; • низкое; • высокое.

Наименование	Описание
Влияние на конфиденциальность	Потенциальное влияние на конфиденциальность (ограничение доступа к информационным ресурсам, разрешения доступа к системе только авторизованным пользователям, предотвращение раскрытия информации неуполномоченным лицам): • отсутствует; • низкое; • высокое.
Краткое описание иной формы последствий компьютерного инцидента	Описание последствий инцидента, кроме тех, что были указаны ранее.
Наименование контролируемого ресурса, на котором был выявлен компьютерный инцидент	Наименование контролируемого информационного ресурса объекта КИИ, на котором выявлен компьютерный инцидент, компьютерная атака или уязвимость.
Информация о категорировании ОКИИ	Присвоенная объекту КИИ категория значимости: • Информационный ресурс не является объектом КИИ; • Объект КИИ без категории значимости (объект признан незначимым); • Объект КИИ третьей категории значимости (самая низкая); • Объект КИИ второй категории значимости; • Объект КИИ первой категории значимости (самая высокая).
Сфера функционирования субъекта	Сфера функционирования объекта КИИ (например, банковская сфера, здравоохранение и т.п.).
Наличие подключения к сети Интернет	Наличие подключения к сети Интернет: • Да; • Нет.
Страна/регион	Код в соответствии с ISO-3166-2 .
Населенный пункт или геокоординаты	Название населённого пункта или его географические координаты. Географические координаты указываются в формате: <i>широта</i> — С.Ш, <i>долгота</i> - В.Д.

7. Сформировать и отправить отчёт об инциденте информационной безопасности.

Формирование отчёта доступно во вкладке с подробностями об инциденте нажатием кнопки **Создать отчёт → GOSSOPKA report**. Для отправки отчёта необходимо указать коннектор, настроенный ранее и нажать **Послать через сеть**.

Далее нужно заполнить необходимые поля формы (большинство поле заполнено в соответствии с шаблоном **Форма для ГОССОПКА**) и нажать **ОК**. В случае успешного соединения сервер UserGate Log Analyzer отправит отчёт на коннектор (в систему личных кабинетов ГосСОПКА).

Запись об отправке отчёта будет отображена в журнале событий LogAn.

Техническая поддержка

Documentation: ☒

Product: LogAn, SIEM

Version: 6.1.9, 7.0.1, 7.1.0

Раздел технической поддержки на сайте компании <https://www.usergate.com/ru/support> содержит дополнительную информацию по настройке LogAn. Кроме этого, здесь же вы можете оставить заявку на решение вашей проблемы.

Требования к сетевому окружению

Documentation: ☒
Product: LogAn
Version: 7.0.1

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
Веб-консоль	TCP	8010	Входящий (к веб-консоли LogAn)	Доступ к веб-интерфейсу управления устройством.
CLI по SSH	TCP	2200	Входящий (к CLI по SSH)	Доступ к интерфейсу командной строки (CLI) UserGate по протоколу SSH.
XML-RPC	TCP	4041	Входящий (к UserGate по API)	Управление устройством UserGate по API.
Удалённый помощник	TCP	22	Исходящий (до серверов технической поддержки)	Удалённый доступ к серверу технической поддержки. Доступ к серверам: 93.91.171.46; 178.154.221.222; - ra.entensys.com.
NTP	UDP	123	Исходящий (до сервера точного времени)	Синхронизация времени.
DNS	UDP	53	Исходящий (до DNS-серверов)	Сервис получения информации (IP-адрес) о доменах.
Регистрация сервера UserGate	TCP	443	Исходящий (до сервера регистрации)	Доступ до сервера регистрации продуктов UserGate reg2.usergate.com.
Обновление ПО и библиотек	TCP	443	Исходящий (до серверов обновления)	Обновление программного обеспечения и элементов библиотек: доступ до сервера updates.usergate.com.
Связь с UGMC	TCP	9712	Исходящий (от LogAn к UGMC)	Первоначальная установка связи и обмен ключами шифрования с сервером UGMC.
		2022	Исходящий (от LogAn к UGMC)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
Сервис LogAn	TCP	9713	Исходящий (от LogAn к NGFW)	Первоначальная установка связи и обмен ключами шифрования с сервером NGFW.
		2023	Исходящий (от LogAn к NGFW)	Построение SSH-туннеля для обмена данными с помощью полученных ключей.
	TCP	22699 (приём данных от NGFW 6.x.x), 22711 (приём данных от NGFW 7.x.x, использующих SSL)	Входящий (от NGFW к LogAn)	Сервис сбора журналов LogAn.
SNMP	UDP	161	Входящий (до LogAn)	Доступ к серверу UserGate по протоколу SNMP.

Сервис	Протокол	Порт	Исходящий/Входящий	Функция
Сборщик логов	TCP/UDP	514	Входящий (до LogAn)	Сервис сбора информации с удалённых устройств по протоколу Syslog.
SMTP	TCP	25	Исходящий (до почтового сервера)	Отправка уведомлений на электронную почту.
DHCP	UDP	67, 68	Исходящий (запрос на получение адреса от UserGate на сервер DHCP)	Сервис службы DHCP.
LDAP	TCP	389, 636	Исходящий (на LDAP-коннектор)	Выполнение запросов LDAP (389 - для LDAP и 636 - для LDAP over SSL).
RADIUS	UDP	1812	Исходящий (на сервер аутентификации RADIUS)	Аутентификация пользователей по протоколу RADIUS.
TACACS+	TCP	49	Исходящий (на сервер аутентификации TACACS+)	Аутентификация пользователей по протоколу TACACS+.
FTP (экспорт журналов)	TCP	21	Исходящий (до сервера FTP)	Экспорт журналов на сервер FTP.
SSH (экспорт журналов)	TCP	22	Исходящий (до сервера SSH)	Экспорт журналов на сервер SSH.
Syslog (экспорт журналов)	TCP/UDP	514	Исходящий (до сервера Syslog)	Экспорт журналов на сервер Syslog.

Documentation: ☒
Product: LogAn
Version: 7.0.1

Формат журнала событий

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	events
	Origin	Модуль, в котором произошло событие.	admin_console
	Severity	Важность события.	Может принимать значения: 1 — информационные; 4 — предупреждения; 7 — ошибки; 10 — критичные.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	suser	Имя пользователя.	Admin
	cat	Компонент, в котором произошло событие.	console_auth
	act	Тип события.	login_successful
	src	IPv4-адрес источника.	192.168.117.254
	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
	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.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	captive
	reason	Причина, по которой было создано событие, например, причина блокировки сайта.	{"id":39,"name":"Social Networking","threat_level":3}
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Default Allow
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	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)
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs4Label	Поле используется для индикации зоны 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)
	cs6Label	Поле указывает было ли содержимое расшифровано.	Decrypted
	cs6	Расшифровано или нет.	true, false
	app	Протокол прикладного уровня и его версия.	HTTP/1.1
	requestMethod	Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET
	request	В случае HTTP-запроса поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
	requestContext	URL источника запроса (реферер HTTP).	https://www.google.com/
	requestClientApplication	Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
	cn3Label	Поле указывает исходный ответ сервера.	Response
	cn3	Код ответа HTTP.	302
	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
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	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

Формат журнала трафика

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	traffic
	Rule Type	Тип правила, срабатывание которого вызвало событие.	firewall
	Threat Level	Уровень угрозы приложения.	Может принимать значения от 1 (если приложения нет) до 10 (указанный уровень угрозы, умноженный на 2).
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
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	cs2Label	Поле используется для индикации зоны источника.	Source Zone
	cs2	Название зоны источника.	Trusted
	cs3Label	Поле используется для указания страны источника.	Source Country
	cs3	Название страны источника.	RU (отображается двухбуквенный код страны)

Тип поля	Название поля	Описание	Пример значения
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	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)
	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)
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40
	cn1Label	Поле используется для указания количества переданных пакетов в направлении источник — назначение.	Packets sent
	cn1	Количество переданных пакетов в направлении источник — назначение.	3
	cn2Label	Поле используется для указания количества пакетов, переданных в направлении назначение — источник.	Packets received
	cn2	Количество пакетов, переданных в направлении назначение — источник.	1

Формат журнала COB

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0

Тип поля	Название поля	Описание	Пример значения
	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 от 2 до 10 (указанный уровень угрозы, умноженный на 2).
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
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	IDPS Rule Example
	msg	Уровень угрозы сигнатуры и её название.	[2] BlackSun
	app	Протокол прикладного уровня.	HTTP
	proto	Используемый протокол 4-го уровня.	TCP или UDP
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	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)
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	cs4Label	Поле используется для индикации зоны назначения.	Destination Zone

Тип поля	Название поля	Описание	Пример значения
	cs4	Название зоны назначения.	Untrusted
	cs5Label	Поле используется для указания страны назначения.	Destination Country
	cs5	Название страны назначения.	RU (отображается двухбуквенный код страны)
	in	Количество переданных входящих байтов; данные передаются в направлении источник — назначение.	231
	out	Количество переданных исходящих байтов; данные передаются в направлении назначение — источник.	40

Формат журнала АСУ ТП

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Название журнала.	scada
	Name	Тип источника.	log
	PDU Severity	Критичность АСУ ТП.	Может принимать значения: 1 — очень низкий. 2 — низкий. 3 — средний. 4 — высокий. 5 — очень высокий.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	Scada Rule Example

Тип поля	Название поля	Описание	Пример значения
	src	IPv4 источника трафика.	10.10.10.10
	spt	Порт источника.	Может принимать значения от 0 до 65535.
	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)
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	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)
	app	Протокол прикладного уровня.	Modbus
	cs6Label	Поле указывает на информацию об устройстве.	PDU Details
	cs6	Информация об устройстве в формате JSON.	{"protocol": "modbus", "pdu_severity": 0, "pdu_func": "3", "pdu_address": 0, "mb_value": 0, "mb_quantity": 0, "mb_payload": "AAIAAA==", "mb_message": "response", "mb_addr": 0}

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

Тип поля	Название поля	Описание	Пример значения
	Threat Level	Уровень угрозы приложения.	Может принимать значения от 1 (если приложения нет) до 10 (указанный уровень угрозы, умноженный на 2).
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
	act	Действие, принятое устройством в соответствии с настроенными политиками.	accept
	app	Протокол прикладного уровня.	SSH или SFTP
	suser	Имя пользователя.	user_example (Unknown, если пользователь неизвестен)
	cs1Label	Поле используется для указания срабатывания правила.	Rule
	cs1	Название правила, срабатывание которого вызвало событие.	SSH inspection rule
	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
	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)
	dst	IPv4 адрес назначения трафика.	194.226.127.130
	dpt	Порт назначения.	Может принимать значения от 0 до 65535.
	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

Тип поля	Название поля	Описание	Пример значения
	cs6	Команда, передаваемая по SSH, в формате JSON.	whoami

Documentation: ☒
Product: LogAn
Version: 6.1.9, 7.0.1

Описание журнала событий

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

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
url_categories	id	Идентификатор категории, к которой относится URL.	39
	threat_level	Уровень угрозы категории URL.	Может принимать значения: 1 — очень низкий; 2 — низкий; 3 — средний; 4 — высокий; 5 — очень высокий.
	name	Название категории, к которой относится URL.	Social Networking
bytes_sent		Количество байтов, переданных в направлении источник — назначение.	52
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica

Название поля			Описание	Пример значения
packets_recv			Количество байтов, переданных в направлении назначение — источник.	5
request_method			Метод, используемый для доступа к URL-адресу (POST, GET и т.п.).	GET
url			Поле содержит URL-адрес запрашиваемого ресурса с указанием используемого протокола.	http://www.secure.com
packets_sent			Количество пакетов, переданных в направлении источник — назначение.	2
action			Действие, принятое устройством в соответствии с настроенными политиками.	block
media_type			Тип контента.	application/json
host			Имя хоста.	www.google.com
session			Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
app_protocol			Протокол прикладного уровня и его версия.	HTTP/1.1
status_code			Код ответа HTTP.	302
bytes_recv			Количество пакетов, переданных в направлении назначение — источник.	100
http_referer			URL источника запроса (реферер HTTP).	https://www.google.com/
decrypted			Поле указывает было ли содержимое расшифровано.	true, false
reasons			Причина, по которой было создано событие, например, причина блокировки сайта.	"url_cats":[{"id":39,"name":"Social Networking","threat_level":3}]
useragent			Useragent пользовательского браузера.	Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:96.0) Gecko/20100101 Firefox/96.0
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника.	Trusted
	country		Страна источника трафика.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted

Название поля			Описание	Пример значения
	country		Страна назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения.	192.168.174.134
	port		Порт назначения.	Может принимать значения от 0 до 65535.
rule	guid		Уникальный идентификатор правила, срабатывание которого вызвало создание события.	f93da24d-74f9-4f8c-9e9b-8e6d02346fb4
	name		Название правила.	Default allow
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 трафика

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
bytes_sent		Количество байтов, переданных в направлении источник — назначение.	100
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
packets_recv		Количество пакетов, переданных в направлении назначение — источник.	1
proto		Используемый протокол 4-го уровня.	TCP или UDP
packets_sent		Количество пакетов, переданных в направлении источник — назначение.	1
action		Действие, принятое устройством в соответствии с настроенными политиками.	accept
session		Идентификатор сессии.	a7a3cd49-8232-4f1a-962a-3659af89e96f (если System: 00000000-0000-0000-0000-000000000000)
bytes_recv		Количество байтов, переданных в направлении назначение — источник.	6
signatures	id	Идентификатор сработавшей сигнатуры.	999999

Название поля		Описание	Пример значения
	threat_level	Уровень угрозы сработавшей сигнатуры.	Может принимать значения: 1 — очень низкий; 2 — низкий; 3 — средний; 4 — высокий; 5 — очень высокий.
	name	Название сработавшей сигнатуры.	BlackSun Test
application	id	Идентификатор приложения.	195
	threat_level	Уровень угрозы приложения.	Может принимать значения: 1 — очень низкий; 2 — низкий; 3 — средний; 4 — высокий; 5 — очень высокий.
	name	Название приложения.	Youtube
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.
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
nat	source	ip	Адрес источника после переназначения (если настроены правила NAT).
		port	Порт источника после переназначения (если настроены правила NAT).
	destination	ip	Адрес назначения после переназначения (если настроены правила NAT).

Название поля			Описание	Пример значения
		port	Порт источника после переназначения (если настроены правила NAT).	Может принимать значения от 0 до 65535 (если NAT не настроен, то: "nat":null)
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	type		Тип правила.	firewall
	name		Название правила, срабатывание которого вызвало событие.	Allow trusted to untrusted
user	guid		Уникальный идентификатор пользователя. Если пользователь типа 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.	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)
packets_sent		Количество пакетов, переданных в направлении источник — назначение.	1
packets_recv		Количество пакетов, переданных в направлении назначение — источник.	1
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
proto		Используемый протокол 4-го уровня.	TCP или UDP
bytes_sent		Количество байтов, переданных в направлении источник — назначение.	100
bytes_recv		Количество байтов, переданных в направлении назначение — источник.	6
action		Действие, принятое устройством в соответствии с настроенными политиками.	accept
application	id	Идентификатор приложения.	195

Название поля		Описание	Пример значения
	threat_level	Уровень угрозы приложения.	Может принимать значения: 1 — очень низкий; 2 — низкий; 3 — средний; 4 — высокий; 5 — очень высокий.
	name	Название приложения.	Youtube
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.
		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
signatures	id	Идентификатор сработавшей сигнатуры.	999999
	threat_level	Уровень угрозы сработавшей сигнатуры.	Может принимать значения: 1 — очень низкий; 2 — низкий; 3 — средний; 4 — высокий; 5 — очень высокий.
	name	Название сработавшей сигнатуры.	BlackSun Test
source	zone	guid	Уникальный идентификатор зоны источника трафика.
		name	Название зоны источника трафика.
	country	Название страны источника.	RU (отображается двухбуквенный код страны)
	ip	IPv4-адрес источника трафика.	10.10.10.10
	port	Порт источника.	Может принимать значения от 0 до 65535.
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.
		name	Название зоны назначения трафика.

Название поля		Описание	Пример значения
	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.

Описание журнала АСУ ТП

Название поля		Описание	Пример значения
timestamp		Время получения события в формате: yyyy-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
pdu_severity		Критичность АСУ ТП.	1
pdu_func		Код функции (говорит ведомому устройству, какие данные или выполнение какого действия требует от него ведущее устройство).	12
pdu_address		Адрес регистра, с которым необходимо провести операцию.	3154
node		Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
details	pdu_varname	Имя переменной. Параметр, в основном, используется для обмена данными в режиме реального времени. Параметр относится к протоколу MMS.	VAR
	pdu_device	Адрес устройства, используемый в протоколах MMS и OPCUA.	DEV
	mb_write_quantity	Количество значений для записи (команда Read Write Register).	998
	mb_write_addr	Начальный адрес регистра для записи (команда Read Write Register).	776
	mb_value	Записываемое значение (для команд Write Single Coil, Write Single Register).	322
	mb_unit_id	Адрес устройства.	186
	mb_read_quantity	Количество значений для чтения (команда Read Write Register).	658
	mb_read_addr	Начальный адрес регистра для чтения (команда Read Write Register).	122
	mb_quantity	Количество значений для чтения.	875
	mb_payload	Значения регистров (для команд Read Coil, Read Holding Registers, Read Input Registers, Read/Write Multiple registers, Write Multiple Coil).	75be5ecdс24f9883
	mb_or_mask	Значение маски OR команды Mask Write Register.	1024
	mb_message	Сообщение Modbus.	exception
	mb_exception_code	Код ошибки. Актуален для типа сообщения error_response.	255
	mb_and_mask	Значение маски AND команды Mask Write Register.	121

Название поля			Описание	Пример значения
	mb_addr		Адрес регистра.	3154
	iec104_msgtype		Тип запроса.	request, response, error_response
	iec104_ioa		Адрес объекта информации, который позволяет однозначно идентифицировать приёмной стороной тип события.	23
	iec104_cot		Причина передачи протокольного блока данных прикладного уровня (Application Protocol Data Unit, APDU).	6
	iec104_asdu		Адрес ASDU (COA — Common Object Address). Параметр относится к протоколу IEC-104.	123
app_protocol			Протокол прикладного уровня.	Modbus
action			Действие, принятое устройством в соответствии с настроенными политиками.	pass
source	zone	guid	Уникальный идентификатор зоны источника трафика.	d0038912-0d8a-4583-a525-e63950b1da47
		name	Название зоны источника трафика.	Trusted
	country		Название страны источника.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес источника трафика.	10.10.10.10
	port		Порт источника.	Может принимать значения от 0 до 65535.
destination	zone	guid	Уникальный идентификатор зоны назначения трафика.	3c0b1253-f069-4060-903b-5fec4f465db0
		name	Название зоны назначения трафика.	Untrusted
	country		Название страны назначения.	RU (отображается двухбуквенный код страны)
	ip		IPv4-адрес назначения трафика.	104.19.197.151
	port		Порт назначения	Может принимать значения от 0 до 65535.
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	SCADA Sample Rule

Описание журнала инспектирования SSH

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

Название поля			Описание	Пример значения
node			Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	utmcore@ersthetatica
command			Команда, передаваемая по SSH.	whoami
app_threat			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
app_id			Идентификатор приложения.	195
action			Действие, принятое устройством в соответствии с настроенными политиками.	block
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
	port		Порт назначения	Может принимать значения от 0 до 65535.
rule	guid		Уникальный идентификатор правила, срабатывание которого создало событие.	59e38e06-533a-4771-9664-031c3e8b2e1f
	name		Название правила, срабатывание которого вызвало событие.	SSH Rule Example
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.	919878b2-e882-49ed-3331-8ec72c3c79cb
		name	Название группы, в которой состоит пользователь.	Default Group

