Журнал событий системы MITIGATOR

Формат записи syslog

Оглавление

Формат записи журнала событий в syslog 3
Пример записи события: 3
Пример записи события с расширенным набором полей: 3
Поля записи журнала событий 4
Типы событий 6
Расширение набора полей записи события 15

Формат записи журнала событий в syslog

Каждая запись журнала событий MITIGATOR состоит из префикса «BIFIT_Mitigator[]» и содержательной части, описывающей событие. Содержательная часть имеет формат JSON и включает три обязательных поля и ряд необязательных, состав которых зависит от типа события. Все возможные поля описаны в таблице «Поля записи журнала событий».

Для ряда событий предусмотрено расширение формата описания. Для таких событий в записи журнала будет присутствовать поле «custom», содержащее JSON объект со специфичным для события набором полей. Перечень таких типов событий и состав полей приведены в таблице «Расширение набора полей записи события».

Все типы событий системы MITIGATOR перечислены в таблице «Типы событий».

Пример записи события:

```
Apr 7 15:59:43 10.50.0.3 BIFIT_Mitigator[1]: {"created_at":"2023-04-07T12:59:43.738
089Z","type_id":"auth_login","type":"Logged in","user_id":1, "user_login":"admin",
"firstname":"System","surname":"Administrator","user_ip":"10.50.0.1","user_role":
"System administrator"}
```

Пример записи события с расширенным набором полей:

```
Apr  7 16:00:19 10.50.0.3 BIFIT_Mitigator[1]: {"created_at":"2023-04-07T13:00:19.63
0366Z","type_id":"config_change","type":"Countermeasure settings were changed",
"user_id":1,"user_login":"admin","firstname":"System","surname":"Administrator",
"user_ip":"10.50.0.1","user_role":"System administrator","policy_id":1,
"policy_name":"Default","element":"TCP Connection Rate Blocking","element_id":
"crb","handler":"Countermeasure settings","custom_type":"diff","custom":
{"averaging_period_calculation":{"new":"100","old":"1"},"block_ip":{"new":"true","o
ld":"false"},"block_time":{"new":"3000","old":"300"},"limit_crb":{"new":"10","old":
""}}}
```

Поля записи журнала событий

Поле	Тип	Назначение	Комментарии
instance_id	uint	Идентификатор экземпляра	
instance_name	string	Название экземпляра	
created_at	time	Время фиксации события	Время на сервере MITIGATOR по UTC. Обязательное поле.
type_id	string	Идентификатор типа события	Обязательное поле.
type	string	Название типа события	Обязательное поле.
user_id	uint	Идентификатор пользователя, совершившего действие	Информация о пользователе присутствует для событий, которые возникают в результате действий пользователя. Действия системы автодетектирования фиксируются с идентификатором пользователя «3».
user_login	string	Логин пользователя	
firstname	string	Имя пользователя	Для действий системы автодетектирования указывается значение «Autodetection».
surname	string	Фамилия пользователя	Для действий системы автодетектирования указывается значение «System».
user_ip	string	IP-адрес устройства, с которого выполнен вход	
user_role	string	Роль пользователя в системе	
user_group	string	Название группы пользователя	Присутствует только для групповых пользователей.
policy_id	uint	Идентификатор политики защиты	
policy_name	string	Название политики защиты	
is_ipv6	boolean	Признак IPv6 политики защиты	
element	string	Название контрмеры	
element_id	uint	Идентификатор контрмеры	
handler	string	Группа параметров	Указание на группу изменившихся параметров.

value	string	Новое значение параметра	Устаревшее поле. В следующих версиях поле будет упразднено. Изменившиеся значения параметров записываются в поле custom.
custom_type	string	Тип custom	Указывает тип **custom**. От типа зависит набор содержащихся в **custom** полей. Возможные значения **custom_type** перечислены в таблице “Расширение набора полей записи события“.
custom	string	Расширенная информация о событии	Содержит набор специфичных для типа события дополнительных полей, расширяющих описание события.

Значение типа time передаются в формате Internet Date/Time согласно RFC 3339 с точностью до микросекунды.

Пример: 2019-08-24T11:54:48.780948Z

Типы событий

Служебный идентификатор типа события	Название типа события
Политики защиты	
autodetect_off	Отключено автодетектирование
autodetect_on	Включено автодетектирование
automitigation_off	Автоматическое включение защиты запрещено
automitigation_on	Автоматическое включение защиты разрешено
policy_add	Создана политика защиты
policy_delete	Удалена политика защиты
policy_edit	Изменены параметры политики защиты
policy_rename	Название политики изменено
policy_on	Включена политика
policy_off	Отключена политика
policy_monitor_mode	Изменение тестового режима работы контрмеры
isn_settings	Изменены параметры синхронизации сессии
isn_servers	Установлены IP-адреса серверов с синхронизацией
policy_memory_save_enabled	Включен режим экономии памяти
policy_memory_save_disabled	Отключен режим экономии памяти
Управление политиками по syslog	
attack_on	Включена политика защиты по сигналу syslog
attack_off	Отключена политика защиты по сигналу syslog
attack_start	По syslog получен сигнал включения политики защиты
attack_stop	По syslog получен сигнал отключения политики защиты
syslog_create	Создан syslog сервер
syslog_update	Обновлены настройки syslog сервера
syslog_delete	Удален syslog сервер
syslog_on	Включен удаленный сислог
syslog_off	Выключен удаленный сислог
Правила маршрутизации	
rules_update_common	Обновлены групповые правила маршрутизации
rules_update_post	Обновлены Пост-правила маршрутизации
rules_update_pre	Обновлены Пред-правила маршрутизации
rules_autoupdate	Автоматически изменены правила маршрутизации
Лицензирование	
autodetect_license_threshold_crossed_up	Входящий трафик поднялся выше лицензионной полосы
autodetect_license_threshold_crossed_down	Входящий трафик опустился ниже лицензионной полосы
license_bandwidth_limit_expired	Время действия лицензионных лимитов закончилось
license_server_disconnected	Соединение с сервером лицензирования разорвано

license_server_connected	Соединение с сервером лицензирования установлено
license_token_update	Обновлен лицензионный ключ
license_set_limit	Лицензионная полоса изменена
license_upload_limit	Загружен лицензионный файл
license_server_failed	Произошла ошибка на стороне сервера лицензирования
license_tariff_expiring	Время действия тарифа подходит к концу
license_tariff_expired	Время действия тарифа истекло
support_expired	Время действия сервисного контракта истекло
license_token_delete	Удалён лицензионный ключ
license_change	Изменён режим лицензирования
license_dynamic_limit	Лицензионная полоса изменена динамически
Системные события	
mitigation_on	Включена система защиты
mitigation_off	Отключена система защиты
router_ext_on	Установлено соединение с внешним роутером
router_ext_off	Разорвано соединение с внешним роутером
router_int_on	Установлено соединение с внутренним роутером
router_int_off	Разорвано соединение с внутренним роутером
port_up	Включен сетевой порт
port_down	Отключен сетевой порт
backend_start	Запущен Backend
backend_stop	Остановлен Backend
click_start	Запущен MITIGATOR
click_stop	Обработчик пакетов остановлен
log_level_set	Изменён уровень логирования
waf_add	WAF добавлен
waf_edit	WAF изменён
waf_delete	WAF удалён
softstart_started	Применён «Мягкий старт»
softstart_aborted	«Мягкий старт» прерван пользователем
softstart_finished	Закончен «Мягкий старт»
dns_not_available	DNS-сервер недоступен
host_not_available	Ошибка разрешения доменного имени
resolver_settings_update	Изменены параметры опроса DNS-сервера
incident_on	Начало инцидента
incident_off	Завершение инцидента
incident_comment	Отредактирован комментарий инцидента
scan	Зафиксирован сброс трафика
multi_conflict	Возник конфликт лидерства экземпляров
accesslog_alert	Получено оповещение от анализатора логов

accesslog_rules	Изменены правила анализа логов
accesslog_switch_on	Включен анализатор логов
accesslog_switch_off	Отключен анализатор логов
isn_key_delete	Удален секретный ключ для ISN
isn_key_set	Установлен секретный ключ для ISN
new_iplists	Создан именованный список IP-адресов
put_iplists	Изменен именованный список IP-адресов
delete_iplists	Удален именованный список IP-адресов
not_available_iplists	Недоступен источник именованного списка IP-адресов
ip_list_update_error	Не удалось обновить именованный список IP-адресов
new_aclset	Создан именованный набор правил фильтрации
put_aclset	Изменен именованный набор правил фильтрации
rem_aclset	Удален именованный набор правил фильтрации
not_available_aclset	Недоступен источник именованных правил фильтрации
new_ja3lists	Создан именованный список JA3-отпечатков
put_ja3lists	Изменен именованный список JA3-отпечатков
delete_ja3lists	Удален именованный список JA3-отпечатков
not_available_ja3lists	Недоступен источник именованного списка JA3-отпечатков
cpu_profiling_start	Запущен сбор информации о работе процессора
cpu_profiling_stop	Остановлен сбор информации о работе процессора
heap_profiling_start	Запущен сбор информации о памяти
heap_profiling_stop	Остановлен сбор информации о памяти
Пользователи	
auth_login	Вошел в систему
failed_auth_login	Неудачная попытка входа в систему
auth_logout	Вышел из системы
group_create	Создана группа
group_update	Обновлена группа
group_delete	Удалена группа
user_create	Создана учетная запись пользователя
user_update	Изменена учетная запись пользователя
user_delete	Удалена учетная запись пользователя
group_user_create	Создана учетная запись группового пользователя
group_user_update	Изменена учетная запись группового пользователя
group_user_delete	Удалена учетная запись группового пользователя
role_create	Создана роль
role_delete	Удалена роль
role_update	Изменена роль
group_role_create	Создана групповая роль
group_role_delete	Удалена групповая роль

group_role_update	Изменена групповая роль
notification_update	Обновлена подписка на уведомления
policy_notification_update	Обновлена подписка на уведомления по политикам
group_prefix_change	Изменен префикс группы
BGP	
bgp_neighbor_add	Добавлен BGP-сосед
bgp_neighbor_update	Изменены параметры BGP-соседа
bgp_neighbor_delete	Удален BGP-сосед
bgp_config_change	Изменены параметры BGP-соединения
bgp_idle	Разорвано BGP-соединение
bgp_established	Установлено BGP-соединение
bgp_prefixes_add	Создан список сетей для анонса
bgp_prefixes_update	Обновлён список сетей для анонса
bgp_prefixes_delete	Удалён список сетей для анонса
bgp_flowspec_add	Создан список флоуспек-правил для анонса
bgp_flowspecs_update	Обновлен список FlowSpec-правил
bgp_flowspec_delete	Удалён список флоуспек-правил для анонса
bgp_community_add	Создан список коммьюнити для анонса
bgp_community_update	Обновлён список коммьюнити для анонса
bgp_community_delete	Удалён список коммьюнити для анонса
bgp_announce	Отправка BGP-анонса
bgp_announce_on	Включено анонсирование префиксов политики по BGP
bgp_announce_off	Выключено анонсирование префиксов политики по BGP
bgp_blackhole_rules_on	Включена blackhole-фильтрация префиксов политики по BGP
bgp_blackhole_rules_off	Выключена blackhole-фильтрация префиксов политики по BGP
bgp_blackhole_ips_on	Включена blackhole-фильтрация IP-адресов по BGP, полученных с коллектора
bgp_blackhole_ips_off	Выключена blackhole-фильтрация IP-адресов по BGP, полученных с коллектора
bgp_blackhole_hpd_on	Включена blackhole-фильтрация IP-адресов политики по BGP, полученных из HPD
bgp_blackhole_hpd_off	Выключена blackhole-фильтрация IP-адресов политики по BGP, полученных из HPD
bgp_policy_edit	Изменены параметры политики анонса
bgp_policy_settings_change	Изменены настройки BGP-анонсирования из политики
bgp_prefixlist_announced	Списки префиксов добавлены в анонс
bgp_prefixlist_withdrawed	Списки префиксов сняты с анонса
bgp_flowspeclist_withdrawed	Списки FlowSpec сняты с анонса
bgp_flowspeclist_announced	Списки FlowSpec добавлены в анонс

bgp_signaling_rules_on	Включена signaling-фильтрация префиксов политики по BGP
bgp_signaling_rules_off	Выключена signaling-фильтрация префиксов политики по BGP
bgp_signaling_ips_on	Включена signaling-фильтрация IP-адресов по BGP, полученных с коллектора
bgp_signaling_ips_off	Выключена signaling-фильтрация IP-адресов по BGP, полученных с коллектора
bgp_signaling_hpd_on	Включена signaling-фильтрация IP-адресов политики по BGP, полученных из HPD
bgp_signaling_hpd_off	Выключена signaling-фильтрация IP-адресов политики по BGP, полученных из HPD
flow_notification_on	Включено сбрасывание префиксов амплификации по BGP
flow_notification_off	Выключено сбрасывание префиксов амплификации по BGP
Настройка системы	
geolite2_update	Загружена база данных геолокации
geolite2_update_fail	Не удалось загрузить базу данных геолокации
mail_update	Обновлены настройки почтового сервера
deploy_set	Изменен способ интеграции в сеть
bypass_mode	Установлен режим работы bypass
vestochka_update	Обновлены настройки Весточки
deploy_mssp	Переключен выключатель GRE MSSP
logo_delete	Удален логотип
logo_update	Обновлен логотип
deploy_settings	Изменена схема деплоя
connreqtable_reset	Сброшена таблица отслеживаемых соединений и запросов для всех политик
telegram_update	Обновлены настройки Telegram
external_auth_settings	Параметры внешней аутентификации изменены
accesslog_config	Изменен адрес анализатора логов
background_update	Обновлен фон страницы входа
background_delete	Удален фон страницы входа
sflow_v4_switch_enable	Включена отправка sFlow IPv4
sflow_v4_switch_disable	Отключена отправка sFlow IPv4
sflow_v4_update	Изменены параметры sFlow IPv4
sflow_v6_switch_enable	Включена отправка sFlow IPv6
sflow_v6_switch_disable	Отключена отправка sFlow IPv6
sflow_v6_update	Изменены параметры sFlow IPv6
statistic_settings	Изменены параметры отправки статистики
syslog_notifications_update	Обновлены настройки уведомлений по Syslog
collector_new	Добавлен коллектор

collector_update	Обновлены настройки коллектора
collector_delete	Коллектор удален
exporters_update	Источники flow обновлены
forwards_update	Настройки проброса flow-пакетов обновлены
feed_token_update	Feed-токен обновлен
hwbypass_enabled	Включен аппаратный байпас
hwbypass_disabled	Отключен аппаратный байпас
hwbypass_wdt_enabled	Аппаратный байпас переведён в режим сторожевого таймера
ignored_policies_update	Исключенные политики защиты коллектора обновлены
Изменение настроек контрмер	
acl_write	Обновлены правила фильтрации
ipset_add	Добавлены значения в список IP-адресов
ipset_remove	Удалены значения из списка IP-адресов
ipset_reset	Сброшен список IP-адресов
ipset_update	Обновлен список IP-адресов
ipset_settings	Обновлены параметры прогрессивной блокировки
ipall_reset	Сброшена таблица аутентифицированных IP-адресов для всех политик
config_change	Изменены параметры контрмеры
geolite2_action	Задан тип действия над трафиком
geolite2_selections	Задан список стран
geolite2_change	Переопределены значения в базе данных геолокации
geolite2_delete_changes	Удалены переопределенные значения в базе данных геолокации
prefix_limiter_delete	Удалены значения
prefix_limiter_reset	Список ограничений очищен
prefix_limiter_set	Добавлены значения
prefix_limiter_updated	Обновлены значения
prefix_limiter_reset_drops	Сброшены счетчики
prefix_limiter_reset_drops_stats	Сброшена статистика
prefix_limiter_drops_trigger	Отослано уведомление
switch_on	Включена контрмера
switch_off	Отключена контрмера
autodetect_alert_down	Трафик опустился ниже порога
autodetect_alert_up	Трафик поднялся выше порога
autodetect_timing_policy_update	Обновлены тайминги автодетекта для политики
autodetect_timing_update	Обновлены тайминги автодетекта
autodetect_cm_update	Обновлены переменные
autodetect_cm_delete	Удалены переменные
autodetect_reset	Сброшены данные

tls_training_finished	Обучение окончено
tls_training_aborted	Обучение прервано пользователем
tls_training_failed	Обучение завершено с ошибкой
tls_training_started	Запущено обучение
tls_prot_database	Загружена база правил
pcap_start	Запущен захват пакетов
pcap_stop	Остановлен захват пакетов
pcap_failed	Захват пакетов завершен с ошибкой
packet_capture_send_email	Результаты захвата отправлены на email
packet_capture_send_telegram	Результаты захвата отправлены в telegram
pcap_send_failed	Отправка результатов захвата пакетов не удалась
pcap_send_succeeded	Результаты захвата пакетов отправлены
autopcap_start	Запущен автозахват пакетов
autopcap_stop	Остановлен автозахват пакетов
autopcap_failed	Автозахват пакетов завершен с ошибкой
autopcap_settings	Изменены настройки автозахвата пакетов
autopcap_send_failed	Отправка результатов автозахвата пакетов не удалась
autopcap_send_succeeded	Результаты автозахвата пакетов отправлены
learning_start	Запущено обучение
learning_reset	Сброшена статистика обучения
training_reset	Удалены результаты обучения
iptable_reset	Сброшена таблица аутентифицированных IP-адресов
conntable_reset	Сброшена таблица отслеживаемых соединений
reqtable_reset	Сброшена таблица отслеживаемых запросов
session_reset	Сброшена таблица сессий
add_by_tuple	Добавлен IP-адрес по параметрам пакета
bpf_program_upload	Программа загружена
bpf_program_delete	Программа удалена
table_add	Добавлено значение в таблицу
table_delete	Удалено значение из таблицы
table_reset	Очищена таблица
fingerprint_wl_add	Загружен белый список отпечатков
fingerprint_wl_delete	Удален белый список отпечатков
fingerprint_bl_add	Загружен черный список отпечатков
fingerprint_bl_delete	Удален черный список отпечатков
fingerprint_allow_add	Загружен список разрешенных отпечатков
fingerprint_allow_delete	Удален список разрешенных отпечатков
fingerprint_autoallow_delete	Автоматически собранный список разрешенных удален
fingerprint_autobl_delete	Автоматически собранный черный список удален
fingerprint_auto_delete	Удален список автоматически собранных отпечатков

fingerprint_collection_start	Запущен сбор отпечатков
fingerprint_collection_stop	Остановлен сбор отпечатков
fingerprint_collection_finished	Закончен сбор отпечатков
fingerprint_collection_attack	Запущен сбор выборки атаки
config_auto_change	Автоматически изменены настройки контрмеры
rts_start	Запущена генерация сигнатур
rts_stop	Остановлена генерация сигнатур
rts_reference_start	Запущен захват эталонного дампа
rts_reference_stop	Остановлен захват эталонного дампа
rts_reference_delete	Эталонный дамп удалён
rts_reference_add	Эталонный дамп добавлен
learning_on	Включено обучение
learning_off	Отключено обучение
scan_detected	Обнаружено сканирование
hpa_enabled	Адресная защита начата
learning_list_clear	Очищена таблица обучения
monitor_mode_on	Включен тестовый режим
monitor_mode_off	Отключен тестовый режим
accesslog_rules	Изменены правила анализа логов
hpd_added_detected	Добавлены адреса в список адресной защиты
hpd_removed_detected	Удалены адреса из списка адресной защиты
named_set_auto_change	Обновлены значения именованного набора в контрмере
named_set_auto_change_failed	Не удалось обновить значения именованного набора в контрмере
Облачная сигнализация «Тип 1»	
type1_objects_add	Добавлен объект мониторинга соседа
type1_objects_update	Обновлён объект мониторинга соседа
type1_objects_delete	Удалён объект мониторинга соседа
type1_neigbor_add	Создан новый сосед
type1_neigbor_update	Обновлён сосед
type1_neigbor_delete	Удалён сосед
type1_alert_on	Отправлен алерт
type1_alert_off	Снят алерт
type1_alert_off_recv	Alert остановлен в системе
Облачная сигнализация «Периметр»	
perimeter_switch_on	Включено подключение к Периметру
perimeter_switch_off	Отключено подключение к Периметру
perimeter_add	Создан новый объект Периметр
perimeter_update	Изменены настройки объекта Периметр
perimeter_delete	Удален объект Периметр

perimeter_wl	В Периметр передан белый список
perimeter_bl	В Периметр передан черный список
perimeter_mititgation_start	В Периметр отправлен запрос митигации
perimeter_mititgation_stop	В Периметр отправлен запрос остановки митигации
perimeter_mititgation_start_recv	Митигация запущена в Периметре
perimeter_mititgation_stop_recv	Митигация остановлена в Периметре
Управление сигнатурами регулярных выражений	
rex_aliases_delete	Удалены наборы правил
rex_aliases_update	Обновлены наборы правил
rex_reset	Сброшены настройки
rex_templates_delete	Удалены шаблоны
rex_templates_update	Обновлены шаблоны
rex_versions_update	Обновлены версии
Экземпляры	
leader_order_set	Задан порядок выбора экземпляра-лидера
instance_change	Настройки экземпляра изменены
click_out_of_sync	Рассинхронизация настроек клика
leader_giveup	Экземпляр прекратил лидировать

Расширение набора полей записи события

Наборы Custom-полей по типам.

Поле	Тип	Описание
accesslog_alert		
ips	string	IP-адреса
policy_description	string	Описание политики защиты
aclset_update		
aclset_id	uint	Идентификатор именованного набора правил фильтрации
aclset_name	string	Название именованного набора правил фильтрации
aclset_source	string	Источник именованного набора правил фильтрации
ip_version	string	Версия протокола IP
auth		
user_login_tag	string	Логин пользователя
user_ip_tag	string	IP-адрес пользователя
error	string	Ошибка
autodetect_alert_down		
autodetect_alert_created_at	time	Время события
autodetect_alert_alert	boolean	Понижение
autodetect_alert_flow	string	Параметр автодетектирования
autodetect_alert_threshold	float	Заданный порог срабатывания
autodetect_alert_value	float	Зафиксированное значение
autodetect_alert_up		
autodetect_alert_created_at	time	Время события
autodetect_alert_alert	boolean	Превышение
autodetect_alert_flow	string	Параметр автодетектирования
autodetect_alert_threshold	float	Заданный порог срабатывания
autodetect_alert_value	float	Зафиксированное значение
autodetect_meta		
policy_input_pps	float	Скорость трафика на входе в политику в пакетах в секунду
policy_input_bps	float	Скорость трафика на входе в политику в битах в секунду
policy_drop_pps	float	Скорость сбрасываемого в политике трафика в пакетах в секунду
policy_drop_bps	float	Скорость сбрасываемого в политике трафика в битах в секунду
policy_pass_pps	float	Скорость трафика, пропущенного на выход политики, в пакетах в секунду
policy_pass_bps	float	Скорость трафика, пропущенного на выход политики, в битах в секунду
bgp_flowspeclist		

bgp_neighbor_id	uint	Идентификатор BGP-соседа
bgp_neighbor_name	string	Название BGP-соседа
bgp_flowspeclist_name	string	Название списка flowspec
bgp_neighbor		
bgp_neighbor_id	uint	Идентификатор BGP-соседа
bgp_neighbor_name	string	Название BGP-соседа
bgp_neighbor_address	string	IP-адрес BGP-соседа
bgp_as	int	Номер автономной системы
bgp_prefixlist		
bgp_neighbor_id	uint	Идентификатор BGP-соседа
bgp_neighbor_name	string	Название BGP-соседа
bgp_prefixlist_name	string	Название списка префиксов
click_fail		
request	string	Запрос
method	string	HTTP method
error	string	Ошибка
deploy		
deploy_router_id	uint	Идентификатор роутера
deploy_mode	uint	Режим деплоя
vlan_ext	int	Внешний VLAN
vlan_int	int	Внутренний VLAN
diff		
name	string	Название измененного параметра
new	string	Новое значение параметра
old	string	Старое значение параметра
game_version		
game_version	uint	Версия протокола
geolite_asns_change		
new_as	string	Новый номер автономной системы
new_asn	string	Новое название автономной системы
prefixes	string	Префикс базы
geolite_countries_change		
new_country	string	Новая страна
prefix	string	Префикс базы
geolite_version_change		
version	string	Версия базы
updated_at	time	Дата и время обновления базы
error	string	Ошибка
hpd		
detected_ips	string	IP-адреса

detected_at	time	Дата и время активации HPD
incident_off		
incident_id	uint	ID инцидента
incident_started_at	time	Время начала
incident_finished_at	time	Время завершения
incident_duration	uint	Длительность
incident_countermeasures	string	Контрмеры
incident_max_input_pps	uint	Максимальная скорость входящего трафика в пакетах
incident_max_input_bps	uint	Максимальная скорость входящего трафика в байтах
incident_max_drop_pps	uint	Максимальная скорость сброшенного трафика в пакетах
incident_max_drop_bps	uint	Максимальная скорость сброшенного трафика в байтах
incident_max_pass_pps	uint	Максимальная скорость прошедшего трафика в пакетах
incident_max_pass_bps	uint	Максимальная скорость прошедшего трафика в байтах
incident_type	string	Тип инцидента
incident_on		
incident_id	uint	ID инцидента
incident_started_at	time	Время начала
incident_max_input_pps	uint	Максимальная скорость входящего трафика в пакетах
incident_max_input_bps	uint	Максимальная скорость входящего трафика в байтах
incident_max_drop_pps	uint	Максимальная скорость сброшенного трафика в пакетах
incident_max_drop_bps	uint	Максимальная скорость сброшенного трафика в байтах
incident_max_pass_pps	uint	Максимальная скорость прошедшего трафика в пакетах
incident_max_pass_bps	uint	Максимальная скорость прошедшего трафика в байтах
incident_rules	-	Правила маршрутизации на политику защиты
type_id	uint	Тип правила
policy_id	uint	Идентификатор политики
is_default	boolean	Признак политики по умолчанию
number	uint	Номер правила
dst_prefix	string	Префикс получателя
src_prefix	string	Префикс отправителя
protocol	string	Протокол

dst_port	string	Порт получателя
src_port	string	Порт отправителя
iplist_update		
iplist_id	uint	Идентификатор именованного списка префиксов
iplist_name	string	Название именованного списка префиксов
iplist_type	string	Источник именованного списка префиксов
ip_version	string	Версия протокола IP
ja3list_update		
ja3list_id	uint	Идентификатор именованного списка JA3-отпечатков
ja3list_name	string	Название именованного списка JA3-отпечатков
ja3list_type	string	Источник именованного списка JA3-отпечатков
packetCapture_send		
policy_id_tag	uint	Идентификатор политики
policy_name_tag	string	Название политики
user_id_tag	uint	Идентификатор пользователя
user_tag	string	Имя пользователя
files	array[string,]	Список фалов захвата с указанием размера каждого.
settings_tag	-	Настройки захвата
size_tag	int	Размер файла
acl_tag	string	Фильтр ACL
rex_tag	string	Фильтр REX
ja3_tag	string	Фильтр JA3
in_tag	boolean	На входе
out_tag	boolean	На выходе
back_tag	boolean	Обратный
drop_tag	boolean	Сброшенный
merge_tag	boolean	Объединять с нескольких экземпляров
instances_tag	string	Идентификатор экземпляра
telegram_ids	string	Идентификаторы Telegram
email	string	Email
fileservers	string	Адреса серверов
perimeter_settings		
perimeter_id	uint	Идентификатор Периметра
perimeter_name	string	Название Периметра
policy_monitor_mode		
policy_id	uint	Идентификатор настроек
monitor_mode	int	Тестовый режим работы контрмеры
port		
ports	string	Порты

resolver		
hosts	string	IP-адреса
rts_settings		
rts_settings_id	uint	Идентификатор настроек RTS
rts_settings_apply	boolean	Применить полученные правила
scanners		
scanner_ip	string	IP-адрес сканера
scanner_first_time	time	Время первого сканирования с IP-адреса
scanner_last_time	time	Время последнего сканирования с IP-адреса
instance_id	string	Идентификатор экземпляра системы
instance_name	string	Название экземпляра системы
as_number	string	Номер автономной системы, к которой относится IP-адрес сканера
as_name	string	Имя автономной системы, к которой относится IP-адрес сканера
country	string	Страна, к которой относится IP-адрес сканера
city	string	Город, к которому относится IP-адрес сканера
softstart		
learning_period	uint	Длительность режима «Мягкий старт»