Система анализа и мониторинга состояния ИБ DATAPK

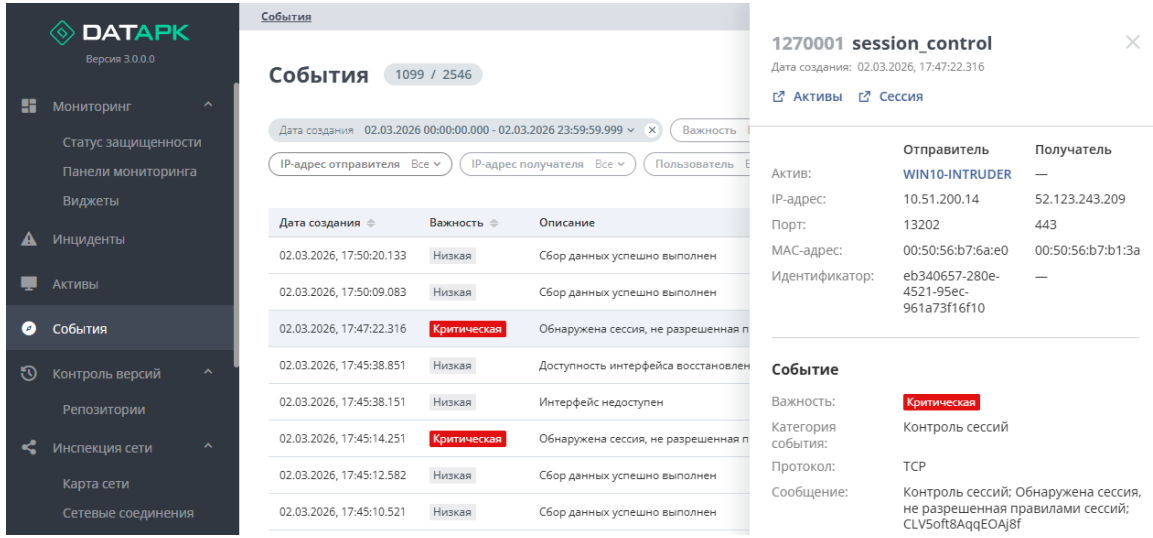
Тема 4. Настройка подсистемы мониторинга событий.

udv|group

События ИБ

Событие информационной безопасности (ИБ) – идентифицированное возникновение состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, или сбой средств контроля, или ранее неизвестную ситуацию, которая может быть значимой для безопасности

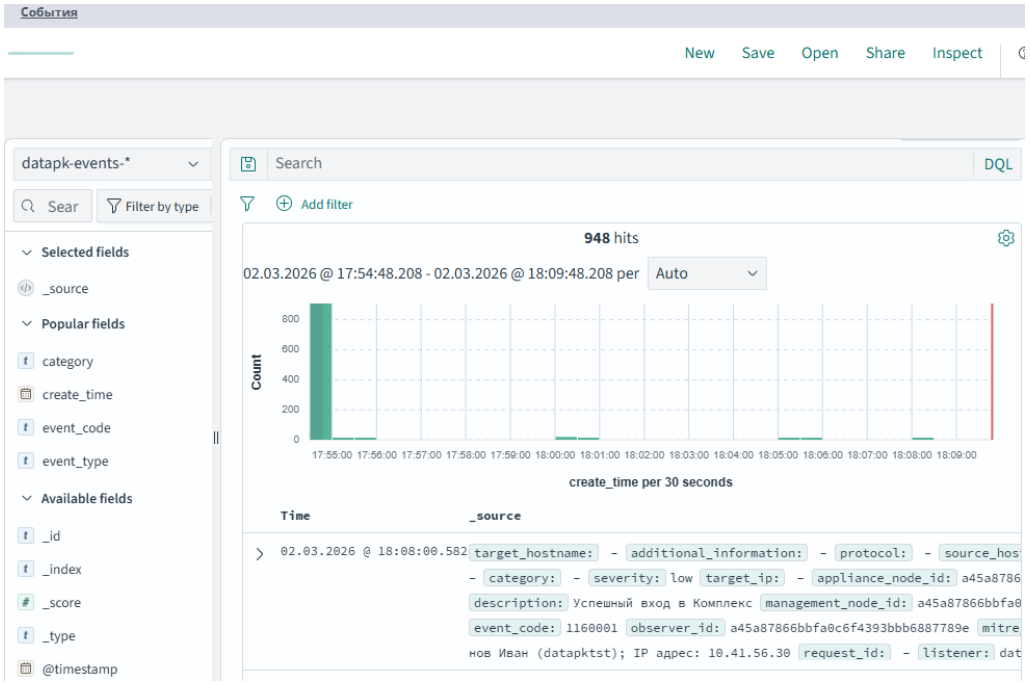
DATAPK регистрирует события и их атрибуты: дату и время обнаружения, данные о протоколе взаимодействия, адреса источника и получателя и другие. События отображаются на странице «События» в порядке их обнаружения от последних к более ранним. События формируются на уровне Management (данные о событиях предоставляет Sensor и в редких случаях сам Management).



События ИБ

DATAPK обрабатывает следующие виды событий:

1. **служебные события, зарегистрированные самим DATAPK** (действия пользователей, обнаружение и изменение ОЗ, обнаружение и изменение потоков и пр.) – модуль **Core** (и события, генерируемые другими модулями (iNTA, CM, VM,…));
2. **пассивный сбор событий** – прием событий от ОЗ по протоколам Syslog и SNMP trap – модуль **EEM**, надо создавать источник для приема, отправлять на соответствующий Sensor;
3. **сбор событий в режиме опроса** – события собираются сканерами сбора данных по протоколам: MSRPC, WinRM, SQL и ряду других – модуль **EEM** + **CM**.



События из пп. 2 и 3 можно посмотреть только в **экспертном режиме** при наличии модуля **EEM**. Так же только здесь события от модуля **ML for PLC**

События ИБ. Экспертный режим

С обычной страницей событий уже знакомились в предыдущих темах, здесь ее подробно не будем разбирать.

Возможность перехода в экспертный режим появляется **при установке модуля EEM** – это стек OpenSearch:

- **Logstash** для нормализации (**/etc/logstash** на уровне Management – Sensor просто доставляет события, нормализацию уже делает Management);
- **OpenSearch** для хранения событий (все внешние и сюда дублируются внутренние);
- **OpenSearch Dashboards** для визуализации событий

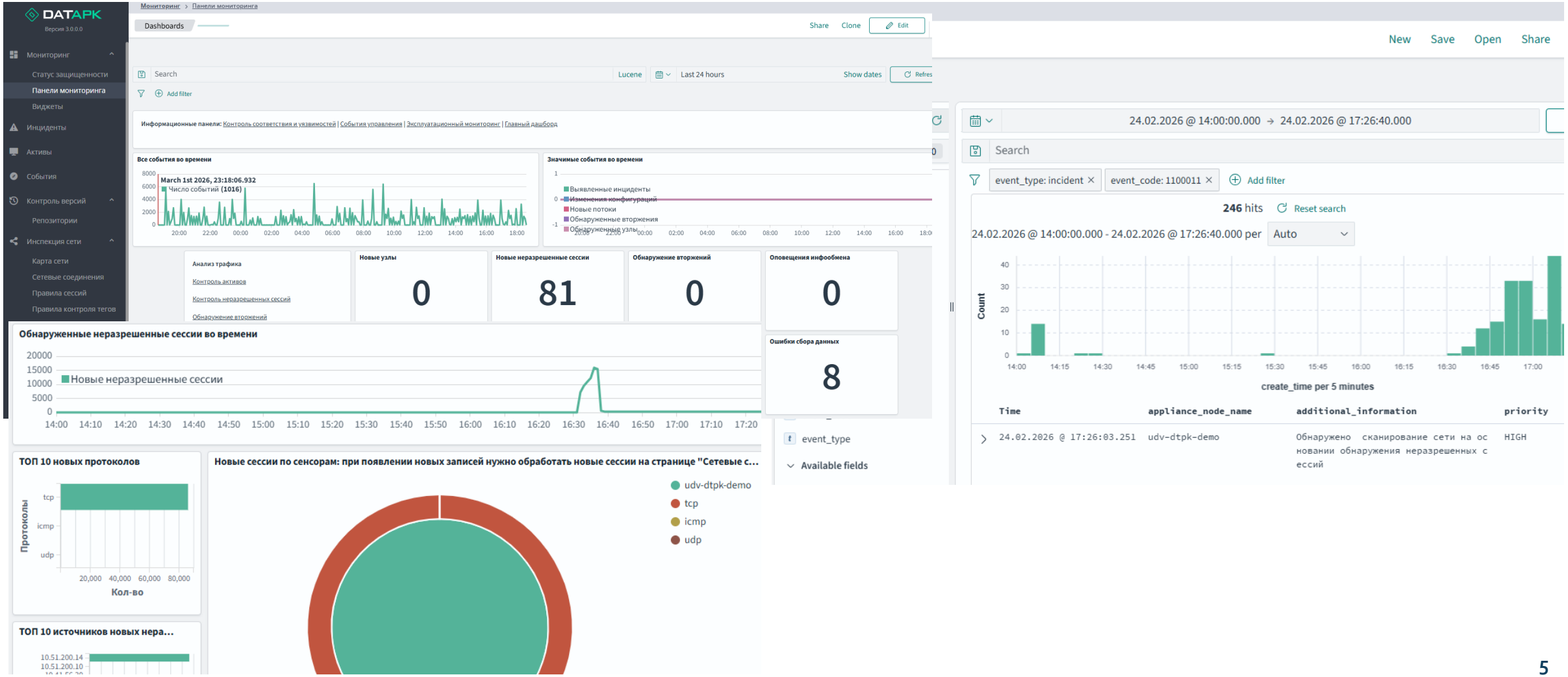
После установки EEM надо создать шаблон индекса (**datapk-events-***) с сортировкой по Create Time (рекомендуемое значение).

Так же производитель DATAPK позволяет типовые панели мониторинга, которые могут помочь с визуализацией (**обратить внимание на нюансы импорта** – при некорректном следовании инструкции часть дашбордов может импортироваться некорректно).

Можно создавать свои панели мониторинга (гибкий механизм). Реагировать надо на интересующие события (сделать нужные фильтры/панели при необходимости)

CyberLympha®

События ИБ. Экспертный режим



События ИБ. Источники

Источники настраиваются на странице Администрирование\Источники.

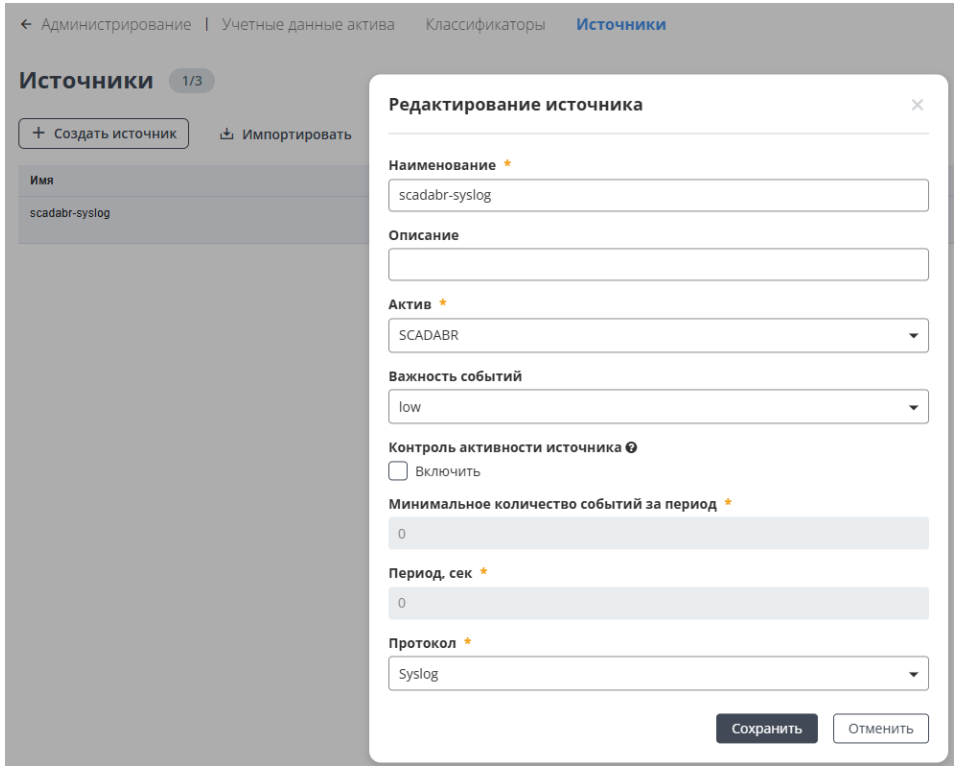
Необходимо задать наименование, выбрать актив, выбрать протокол.

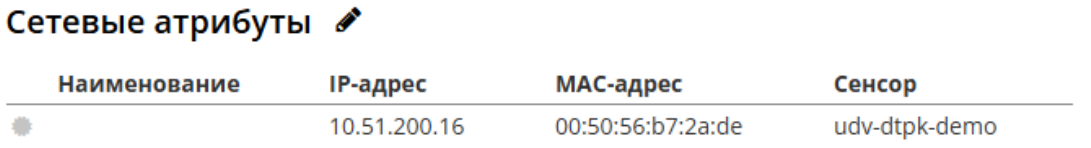
Так же опционально можно выбрать минимальное число событий за указанный период, и система будет оповещать, если от источника мало событий.

Протокол **Syslog** – прием Syslog с узла (3164 на 514 порт, 5424 на 515 порт), транспорт TCP или UDP

Протокол **SNMP** – прием SNMP-Trap v1 или v2 с указанным в источнике Community (на практике используется редко)

С актива события надо отправлять **на сенсор, который у его интерфейса сбора данных** (и соответственно обеспечить сетевые доступы)

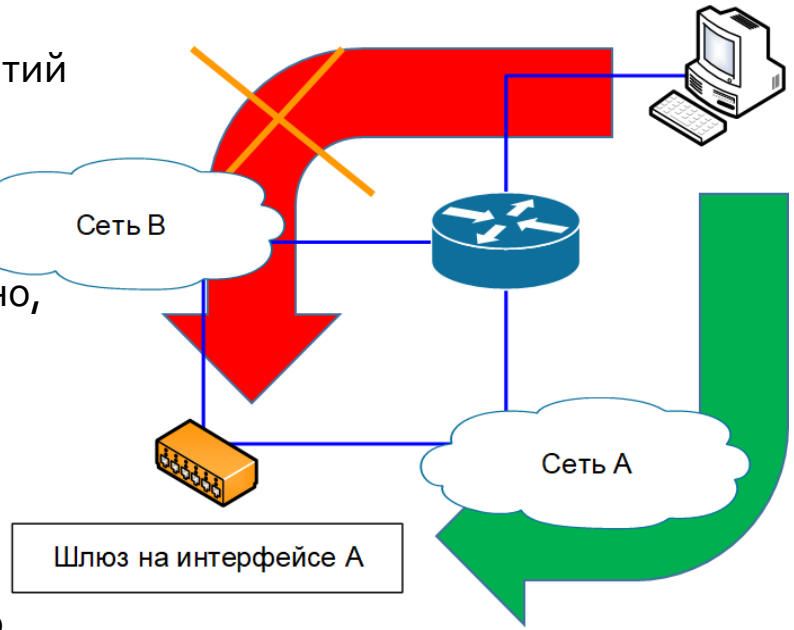




События ИБ. Диагностика

Довольно часто возникают нюансы с приемом внешних событий (такие события нужно смотреть только в экспертном режиме, выбрав нужное временно́е окно). Диагностировать нужно следующее:

- приходят ли события на нужный Sensor/нужный порт (проверить можно с помощью tcpdump)
  - если событий не видно в tcpdump – проверить сетевые доступы/генерацию событий на источнике
- если есть в tcpdump на сенсоре (и поступают на правильный порт, сформированы по правильному протоколу), то проверить:
  - есть ли обратный маршрут от приемного интерфейса сенсора до актива (особенно, когда у сенсора несколько интерфейсов)
  - есть ли связь Sensor-Management
  - создан ли источник событий на уровне Management
  - у актива интерфейс сбора данных с нужным IP-адресом (с которого приходят события) и привязан нужному сенсору
  - на активе правильное время и таймзона (события по умолчанию фильтруются по **create_time** (время создания события активом) – если время на активе сильно неправильное, в ожидаемое временное окно мы события не увидим)
  - посмотреть логи сервисов, обратиться в ТП с предоставлением артефактов выше



CyberLympha®

События ИБ. Отправка в SIEM

Довольно часто стоит задача отправки событий в смежные системы.

DATAPK умеет отправлять события по протоколу Syslog (транспорт TCP или UDP).

Если нет EEM – то через **manager.env** по Syslog 5424 (переменные **EVENT_SYSLOG_SEND** (true/false), **EVENT_SYSLOG_HOST** (адрес syslog-сервера), **EVENT_SYSLOG_PORT** (порт syslog-сервера), **EVENT_SYSLOG_PROTOCOL** (TCP или UDP), **EVENT_SYSLOG_SEVERITY** (INFORMMATIONAL – все внутренние события, CRITICAL – только критичные)).

Если есть EEM – через нормализацию Logstash (**/etc/logstash/pipeline**, по умолчанию файл **95-siem-output.conf**) – можно более тонко настроить транспорт; формат сообщения; фильтр, какие события отправлять; так же можно на разные адреса отправлять. **Рекомендуется отправлять по UDP, т.к. при длительной недоступности syslog-tcp-сервера пайплайн обработки событий (logstash, opensearch) может остановиться в DATAPK**

Инциденты

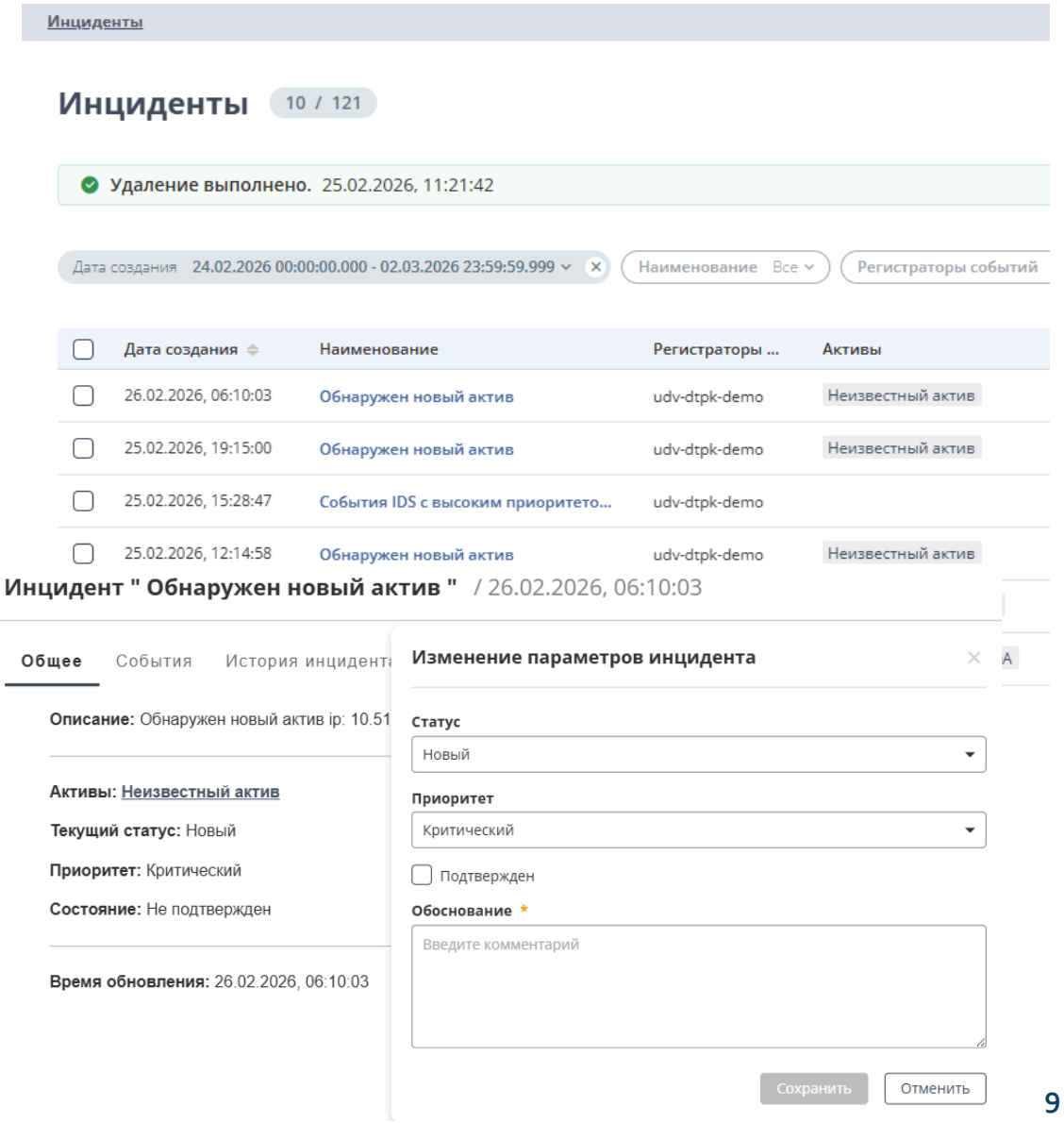
Инцидент – совокупность событий, попавших под определенное правило корреляции.

На инциденты необходимо **реагировать в первую очередь** (изучить связанные события, посмотреть другие события за указанный период, проверить конфигурации узлов). Если правило срабатывает слишком часто/ложно – отключить или переписать правило под конкретные задачи.

Инциденты можно брать в работу, закрывать, менять приоритет.

Из карточки инцидента можно перейти к связанным данным (активам, событиям).

Можно отправлять оповещения об инцидентах в смежные системы по SMTP или OPC UA (ну и по Syslog, как было рассмотрено ранее).



Корреляция

В DATAPK 2 коррелятора:

Внутренний:

- в составе модуля Core;
- 28 простых правил корреляции (перечислены в документации);
- ненужные правила можно отключить в файле **/usr/share/udv/event-correlator/exceptions_rules.json** (["0001","0004"]) и перезапустить сервис **udv-event-correlator**

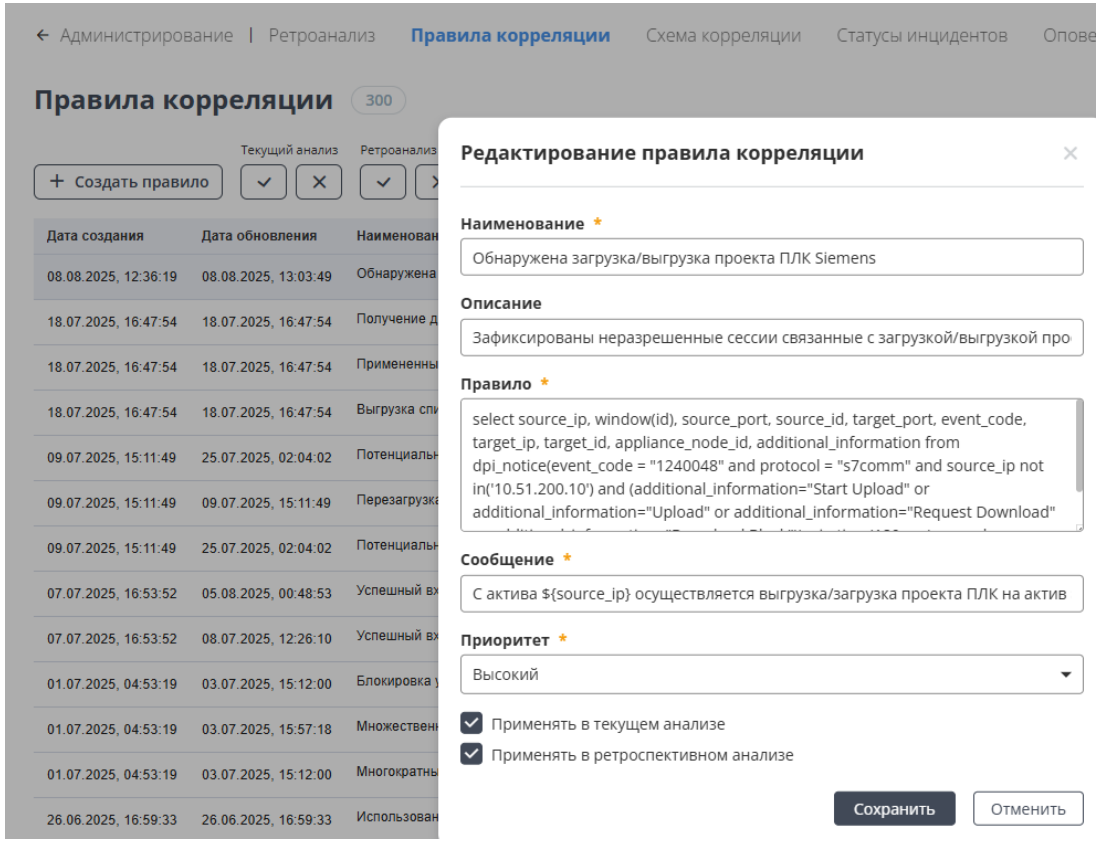
Полноценный на базе движка Esper:

- в составе модуля EEM (при добавлении EEM внутренний коррелятор деактивируется);
- гибкий синтаксис правил на языке EPL;
- правила не только под внутренние, но и под внешние события;
- написание и редактирование правил через web;
- импорт и экспорт правил и политики корреляции через web, производитель DATAPK поставляет обновления вместе с контентом (порядка 300 правил)

Коррелятор на базе Esper

- в составе модуля EEM;
- можно включать и выключать правила;
- можно редактировать правила (рекомендуется копировать правило и менять скопированное, оригинальное отключать);
- есть возможность ретроспективного анализа (старые события прогнать через выбранные правила корреляции)

- **Схема корреляции** – маппинг полей событий в поля коррелятора, правится производителем DATAPK (редко другими);
- **Правила корреляции** – непосредственно сами правила на языке EPL (уже чаще правятся конечными пользователями);
- **Политика корреляции** – правила + схема в одном файле (в таком виде поставляется производителем для удобства)



Вопросы?

udv|group