

Система анализа и мониторинга состояния ИБ DATARK

Тема 2. Настройка подсистемы инвентаризации.

Понятие контролируемой сети

Контролируемая сеть – совокупность IPv4-подсетей, которые контролирует UDV DATAPK.

Внешняя сеть – понятие, противоположное домашней сети. Это совокупность IPv4 сетей, которые не попадают в домашнюю сеть.

Контролируемая сеть влияет на:

- обнаружение новых объектов защиты;
- обнаружение новых потоков IPv4;
- отображение результатов сканирования сети



Обсуждение

На DATAPK заданы следующие контролируемые сети:

- 192.168.1.0/24
- 192.168.23.1/32
- 10.0.0.0/24

Будут ли автоматически обнаружены следующие объекты защиты:

- 10.0.0.1
- 10.0.1.1
- 192.168.23.1
- 192.168.1.123
- 172.16.1.1

Будут ли зафиксированы следующие потоки:

- tcp: источник 10.0.0.1, получатель 192.168.23.12
- udp: источник 192.168.2.1, получатель 10.0.0.21
- tcp: источник 192.168.23.1, получатель 8.8.8.8
- tcp: источник 192.168.32.1, получатель 8.8.8.8



Понятие актива

Актив (Объект защиты (ОЗ)) – сетевой узел, подлежащий защите от потенциальных угроз и неправомерных действий, например, несанкционированного доступа и изменения данных третьими лицами.

Актив обычно состоит из одного или нескольких сетевых интерфейсов

Сетевой интерфейс – уникальная связка IP+MAC+Sensor



Атрибуты актива

- Наименование (обычно hostname, например WIN2008-SCADA)
- Описание (более детальное объяснение, например Сервер SCADA)
- Производитель (обычно определяется автоматически по первым октетам MAC-адреса)
- Тип (АРМ, ПЛК, ... У автоматически обнаруженных устройств он неизвестный)
- АСУ ТП (принадлежность узла АСУ ТП, справочник АСУ ТП ведется в системе, узлу можно назначить только 1 АСУ ТП)
- Группа (пользовательский справочник, удобно использовать при сборе данных, активу можно назначить только 1 группу)
- Дата создания (когда узел был обнаружен и создан в сети)
- Последнее появление (когда узел последний раз был виден в сети)

 WIN2008-SCADA

Описание актива 

Наименование: WIN2008-SCADA

Описание: Сервер SCADA

Производитель: VMware

Тип: Сервер

Группа: SCADA

АСУ ТП: Демонстрационная АСУ ТП

Дата создания: 28.07.2025, 19:03:09

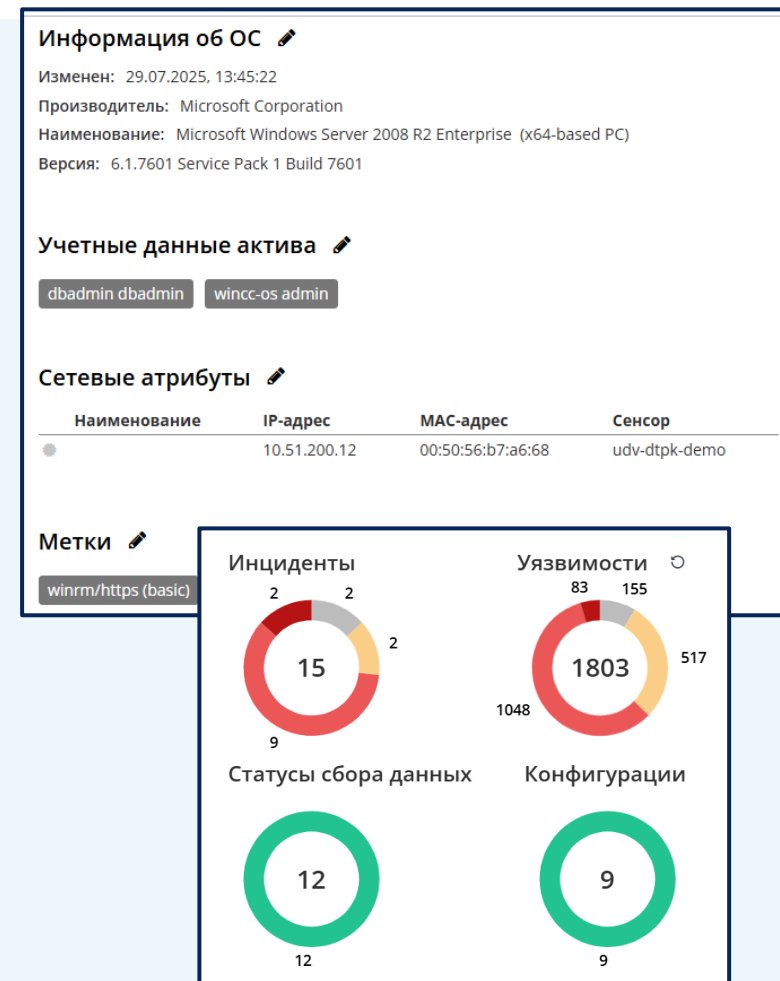
Последнее появление: 24.02.2026, 14:07:59

IP-адрес интерфейса сбора данных: 10.51.200.12

MAC-адрес интерфейса сбора данных: 00:50:56:b7:a6:68

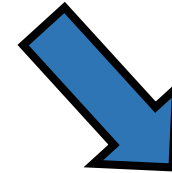
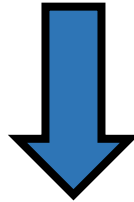
Атрибуты актива

- Информация об ОС (собранная с помощью сканеров или заданная вручную информация об ОС/версии прошивки, рекомендуется собирать с помощью сканеров)
- Учетные данные актива (как подключаться к активу для сбора данных)
- Метки (произвольные классификаторы, можно много меток на 1 узел)
- Сетевые атрибуты – информация о сетевых интерфейсах узла (IP, MAC, принадлежность сенсору). У узла м.б. более 1 интерфейса (но всегда 1 основной интерфейс – по нему осуществляется опрос актива указанным в этом интерфейсе сенсором)
- Источники – созданные сущности для приема Syslog или SNMP-trap с узла
- Конфигурации (собранные конфигурации, статус их эталонности)
- Уязвимости (информация о найденных уязвимостях по версии ОС и перечню ПО)
- Перечень ПО (собранный специальными сканерами список установленного ПО)



Виды пользовательских классификаторов

Пользовательские классификаторы (справочники)



АСУ ТП

Группы

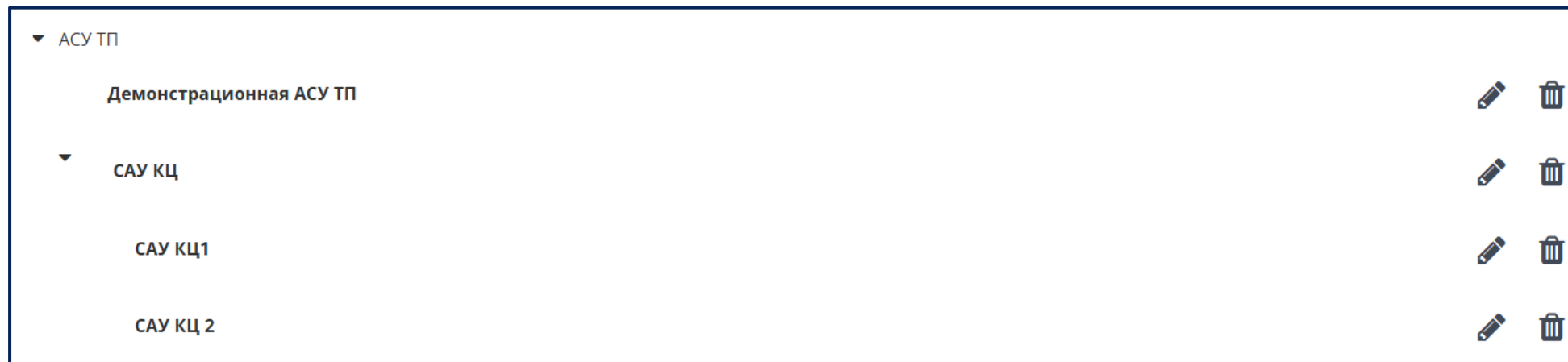
Метки

АСУ ТП

АСУ ТП – позволяет определить принадлежность актива конкретной АСУ ТП. Активу м.б. назначена не более одной АСУ ТП

Атрибуты АСУ ТП

- Наименование – обязательный атрибут, название конкретной АСУ ТП.
- Описание – опциональное поле для ввода расширенного описания АСУ ТП
- Родительская АСУ ТП – поле для выбора родительской (вышестоящей по иерархии АСУ ТП)

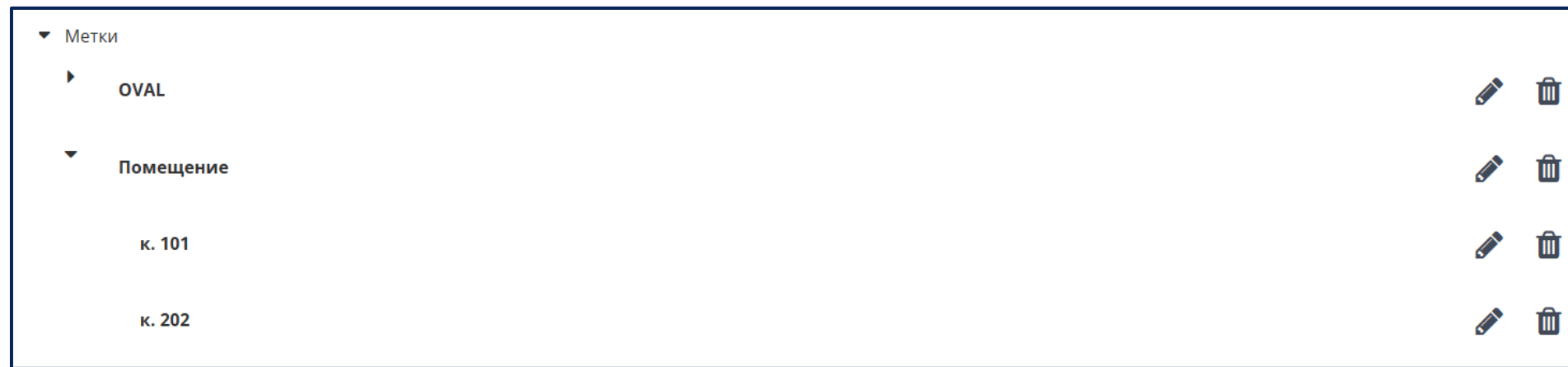


Метки

Метки – справочник для добавления произвольных иерархических атрибутов к объектам защиты. Можно сгруппировать ОЗ по произвольному признаку, например, местоположение (номер помещения), режимам работы (непрерывный, сменный) и пр.

Атрибуты меток:

- Наименование – обязательный атрибут, название конкретной группы.
- Родительская метка – поле для выбора родительской (вышестоящей по иерархии) группы.

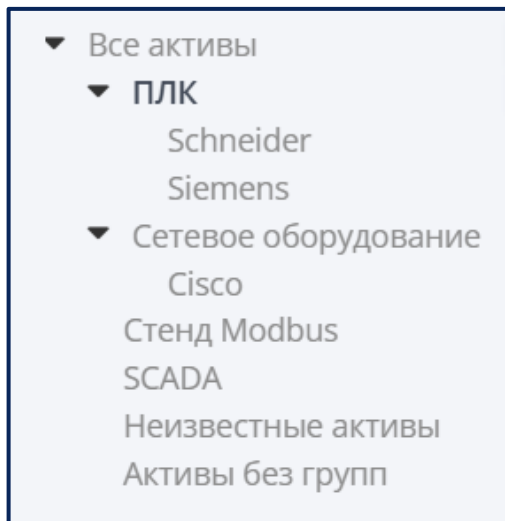


Группы

Группы – атрибут для объединения схожих узлов. Полезен для задач сбора данных (группового назначения задач сбора). Узлу м.б. добавлена не более одной группы. Довольно часто группы нижнего уровня делают по семейству ОС/вендору оборудования

Атрибуты групп:

- Наименование – обязательный атрибут, название конкретной группы.
- Вышестоящая группа – поле для выбора родительской (вышестоящей по иерархии) группы.



Фильтры страницы активов

Фильтровать активы можно по:

- Типам
- Производителям
- Наименованию/описанию
- IP-адресам, подсетям, MAC адресам
- Статусу проблемности (совокупный статус ошибок сбора данных и наличию неэталонных конфигураций)
- АСУ ТП, группам, меткам
- Сенсору (какому сенсору принадлежит основной интерфейс данного актива)

В первую очередь надо смотреть на:

- *неизвестные активы;*
- *проблемные активы*

При пусконаладке так же нужно обращать внимание на активы без групп

Критерий появления нового актива

Критерий автоматического обнаружения неизвестного актива – на слушающем интерфейсе сенсора зафиксирован поток данных с уникальной связкой IPv4 + MAC. IPv4 адрес при этом принадлежит домашней сети, заданной на этом сенсоре.

Впоследствии этот актив надо инвентаризовать или добавить этот интерфейс существующему активу.

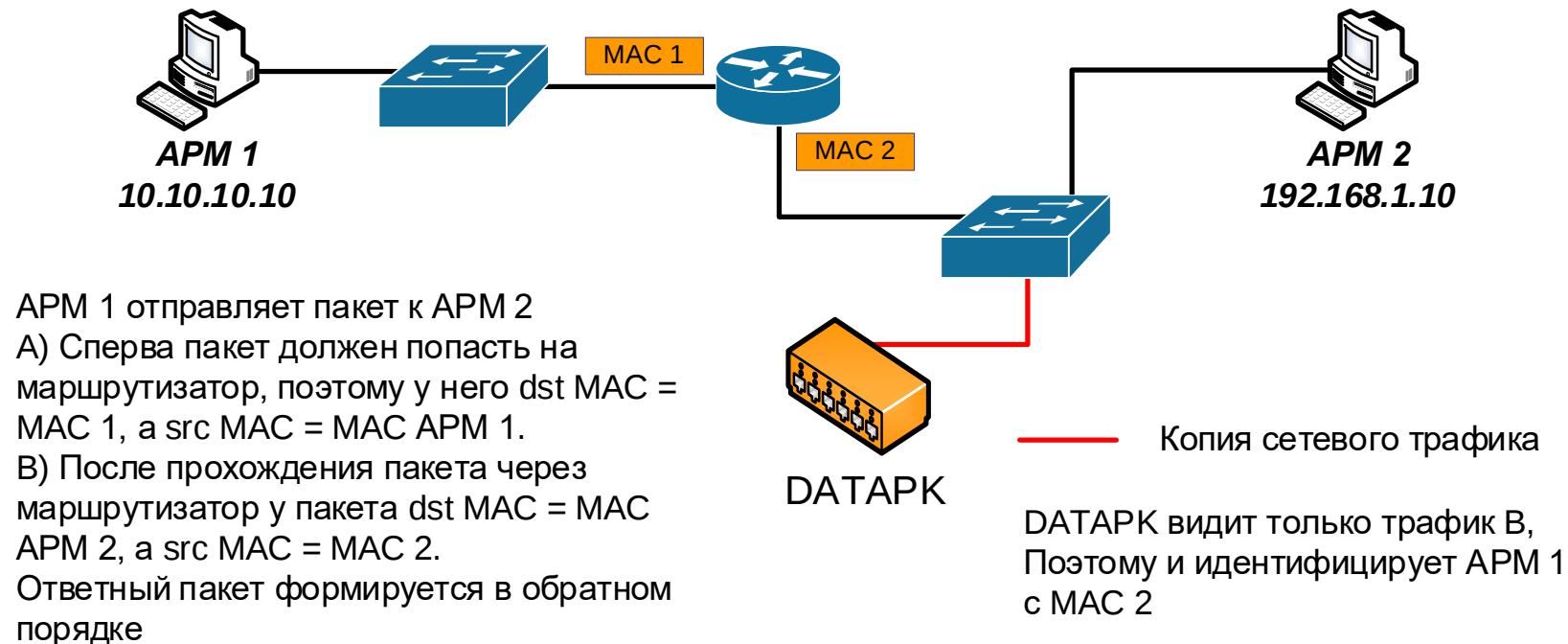
Если несколько сенсоров видят один и тот же интерфейс, то на уровне Management можно в актив добавить несколько таких интерфейсов

Появление нового актива практически всегда требует внимания оператора, поскольку зачастую это может свидетельствовать о начале сетевой атаки. Если узел известен – оператор инвентаризует его. Если нет – применяются меры по локализации данного узла вплоть до отключения его от сети



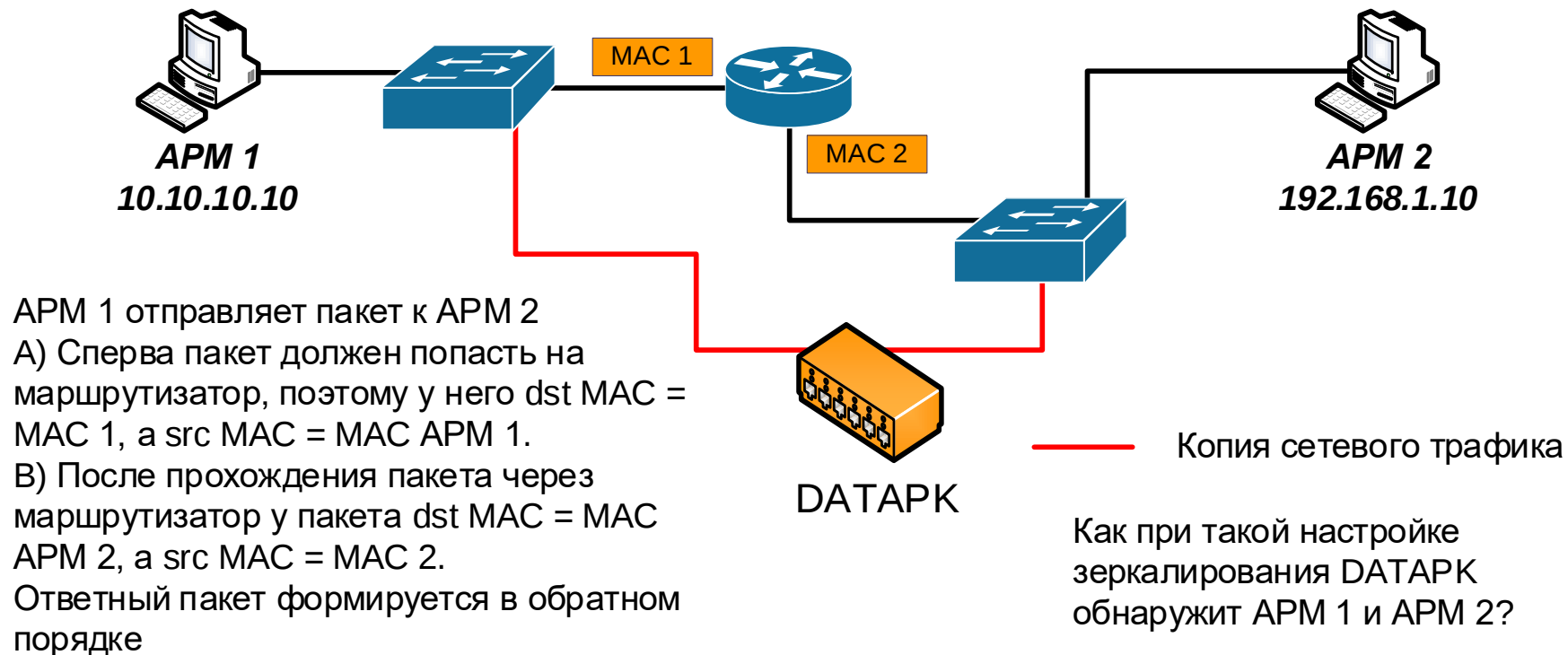
Нетиповые сценарии обнаружения активов

Кейс 1. Обнаружен неизвестный актив с чужим MAC-адресом, либо несколько ОЗ с одинаковым MAC-адресом.



Нетиповые сценарии обнаружения активов

Кейс 2. Обнаружены неизвестные ОЗ. У обоих ОЗ одинаковые IP-адреса, но у одного из них MAC-адрес маршрутизирующего устройства.



Нетиповые сценарии обнаружения активов

Кейс 3. DATAPK не видит актив.

Причина: Трафик от данного узла не попадает на слушающий интерфейс DATAPK Sensor либо актив не попадает в контролируемую сеть.

Объяснение: Если сенсор DATAPK не видит трафик от интересующего актива, то узел не будет обнаружен. Также не будет обнаружен актив, не попадающий в домашнюю сеть. Также не всегда можно обеспечить 100% зеркалирование сетевого трафика.

Подход к настройке: Проверить доступность актива по сети, настройки зеркалирования сетевого трафика, настройки домашней сети. Вероятно, стоит завести актив вручную либо запустить сканирование сети.

Нетиповые сценарии обнаружения активов

Кейс 4. DATAPK видит лишние объекты защиты

Причина: Совокупность настроек зеркалирования и контролируемой сети. Трафик от данных узлов попадает на слушающие интерфейсы сенсора.

Объяснение: Критерий появления нового актива.

Подход к настройке: Убедиться в принадлежности актива защищаемым АСУ ТП.
Инвентаризировать узлы защищаемых АСУ ТП. При необходимости привлечь инженеров Заказчика.

Пересмотреть настройки контролируемой сети, настройки зеркалирования. После этого – удалить лишние активы.

Если настройками сети нельзя разделить АСУ ТП и смежную/корпоративную систему, то допустимо по согласованию с Заказчиком создать специальный актив и добавить ему обнаруженные интерфейсы из смежной системы.

Нетиповые сценарии обнаружения активов

Кейс 5. Заведен актив с 2 интерфейсами. Появились еще 2 узла с IP адресом первого интерфейса, но MAC второго интерфейса; с IP адресом второго интерфейса, но MAC первого интерфейса

Причина: Если DATAPK видит уникальную связку IPv4+MAC в трафике, то это приводит к обнаружению нового ОЗ, включая ситуацию, описанную выше.

192.168.126.19	255.255.255.255	ff:ff:ff:ff:ff:ff,00:01:03:34:4f:52
192.168.126.19	255.255.255.255	ff:ff:ff:ff:ff:ff,00:01:03:34:4f:52
192.168.126.19	255.255.255.255	ff:ff:ff:ff:ff:ff,00:10:22:ff:0e:67
192.168.126.19	255.255.255.255	ff:ff:ff:ff:ff:ff,00:10:22:ff:0e:67

Объяснение: Если DATAPK видит уникальную связку IPv4+MAC в трафике, то это приводит к обнаружению нового актива, включая ситуацию, описанную выше.

Подход к настройке: Завести перекрестные интерфейсы нужному активу на этапе обучения системы в случае их обнаружения. Удобно через функцию привязки неизвестного интерфейса известному узлу

☐ Выберите сетевой атрибут ▲

10.51.200.14 00:50:56:b7:...

Выберите сенсор ▼

☒ Выбрать сетевой атрибут неизвестного актива

Автоматизированная привязка интерфейсов с MAC-адресом маршрутизирующего устройства к известному ОЗ

Для автоматизации привязки интерфейсов с MAC-адресом маршрутизирующего устройства к существующим активам в DATAPK реализован следующий алгоритм.

- Обнаружен новый узел с IP-адресом существующего актива (в т.ч. неизвестного).
- MAC-адрес этого узла совпадает с MAC-адресом одного из интерфейсов коммутатора, маршрутизатора, или сетевого средства защиты, уже заведенного в DATAPK.
- Тогда интерфейс добавляется существующему активу с пометкой `with_router_mac` и формированием соответствующего события.

Повышение точности работы алгоритма

Для повышения точности работы алгоритма нужно придерживаться следующей последовательности на начальном этапе ПНР:

- Инвентаризировать маршрутизирующие устройства (завести их в DATAPK)
- Через некоторое время удалить неизвестные активы, у которых производитель совпадает с производителем АСО. Этот шаг помогает избавиться от узлов с MAC маршрутизирующего устройства, которые были обнаружены раньше, чем актив со своим MAC-адресом
- После этого неизвестные интерфейсы с MAC-адресом маршрутизирующего устройства привяжутся к уже обнаруженным ОЗ со своим MAC

Сканирование

Легковесное iстр-сканирование, предназначено для поиска активов в защищаемой сети (не всегда есть возможность увидеть все активы из трафика / не всегда в поставке модуль iNTA).

Сканировать можно диапазон не более 255 адресов.

Актив создастся при условии, что его IP-адрес попадает в контролируемую сеть

Довольно часто сканирование в сетях АСУ ТП запрещено. Применять данный алгоритм только после согласования с Заказчиком

udv-dtpk-demo ✎

Описание:

Автоматически добавленный сенсор.

Эксплуатирующая организация:

ООО "СайберЛимфа"

Место установки:

Демонстрационный стенд

✓  Обновлено 24.02.2026, 14:03:09

Статус синхронизации настроек:

Активен

Статус получения данных:

Активен

Статус передачи данных:

Активен

✓ **Сканирование сети**

Начальный адрес *

192.168.243.10

Конечный адрес *

192.168.243.20

Запустить

Сбросить

Сканирование

При сканировании DATAPK определяет:

- наименование ОЗ (hostname) путем обращения к DNS-серверу
- IPv4, MAC адрес ОЗ, расположенных в той же подсети (широковещательном домене), что и DATAPK
- IPv4 -адрес (без MAC) у ОЗ, расположенных в другой подсети (широковещательном домене) – в случае обнаружения такого ОЗ у него не заполняется поле MAC-адрес

Автоматизированный сбор интерфейсов с АСО

- Сканер snmp, собирающий интерфейсы
- В окне просмотра конфигурации появляется кнопка «Создать сетевые атрибуты»
- После работы сканера на нужном сетевом оборудовании нужно удалить неизвестные активы
- Можно не использовать сканер, а добавлять интерфейсы вручную нужному коммутатору, маршрутизатору, сетевому средству защиты

Конфигурации актива cisco

(Эталонная) создана: 24.02.2026, 15:09:54; статус присвоен: 24.02.2026, 15:09:54; собрана: 24.02.2026, 15:... ×

Принять за эталонную 

Создать сетевые атрибуты

Просмотр Сравнение

№	Индекс	Описание	Тип	Максимальн...	Физический...	Статус	IP-адрес
1	1	GigabitEthernet1	ethernetCsmacd	1500	00:50:56:b7:17:7f	up	10.51.200.11

☐	Наименование сканера	Описание	Тип
☐	Раздел Interface (snmp2c)	Сканер для сбора параметр...	Конфигурации
☐	Раздел Interface (snmp3)	Сканер для сбора параметр...	Конфигурации

Результаты сканирования

По результатам детального сканирования сети появляется событие «Сканирование сети успешно завершено». Так же появляются новые активы при их обнаружении (и активы попадают в контролируемую сеть)

1220002 home_net

Дата создания: 24.02.2026, 14:02:11.895

Событие

Важность:

Низкая

Категория события:

—

Протокол:

—

Сообщение:

Сканирование сети успешно завершено; Диапазон сканирования: 192.168.243.10 - 192.168.243.20

Действие:

—

Дополнительная информация:

Диапазон сканирования: 192.168.243.10 - 192.168.243.20

Обоснование:

—

Идентификатор события:

00a90a95-6b39-4bb4-9850-f8a6d647e93d

Источник события:

datapk_sensor

☐		Неизвестный актив	Неизвестный ...
☐		Неизвестный актив	Неизвестный ...
☐		Неизвестный актив	Неизвестный ...
☐		Неизвестный актив	Неизвестный ...
☐		Неизвестный актив	Неизвестный ...

Поиск подключенного актива на АСО

Довольно часто в условиях эксплуатации DATAPK требуется идентифицировать, к какому коммутатору подключен узел. Особенно актуально для проведения расследований при появлении новых активов.

DATAPK предоставляет IPv4 и MAC-адрес узла, время первого и последнего появления узла в сети. Если узел активен (доступен), то можно попытаться найти, к какому коммутатору и в какой порт подключено устройство.

Для этого нужно на коммутаторе просмотреть ARP-таблицу с фильтром по интересующему IP, а также таблицу MAC-адресов с фильтром по интересующему MAC.

Команды для коммутаторов Cisco:

- **show arp | incl <IP-адрес узла>** – покажет ARP-таблицу коммутатора, с фильтром по IP-адресу
- **show mac address-table | incl <MAC-адрес или фрагмент>** – покажет таблицу MAC-адресов коммутатора с фильтром по MAC.

```
SW01-DTPK-LAB#show arp | inc 10.23.250.21
Internet 10.23.250.21      0    4c02.890c.7a4d  ARPA   Vlan5
SW01-DTPK-LAB#show mac address-table | incl 7a4d
      5      4c02.890c.7a4d      DYNAMIC      Gi0/1
```

Общая архитектура работы с трафиком

Механизмы анализа трафика (iNTA) обеспечивают:

- определение текущего состава активов защищаемых АСУ ТП;
- выявление изменений в составе активов;
- ведение каталога активов;
- идентификация сетевых соединений между активами;
- выявление изменений в сетевом взаимодействии между объектами защиты АСУ ТП;
- выявление известных сетевых атак на объекты защиты АСУ ПТК сигнатурным методом;
- контроль управляющих команд (Start, Stop, ...);
- контроль параметров техпроцесса (Modbus, OPC UA, Emerson DeltaV);
- извлечение файлов из трафика;
- запись сетевого трафика

Общая архитектура анализа трафика (iNTA)

Уровень Sensor:

- выявление сетевых соединений и интерфейсов, передаваемых файлов;
- глубокий разбор протоколов, выявление команд, извлечение файлов;
- запись трафика;
- выявление известных сетевых атак сигнатурным методом

Уровень Management:

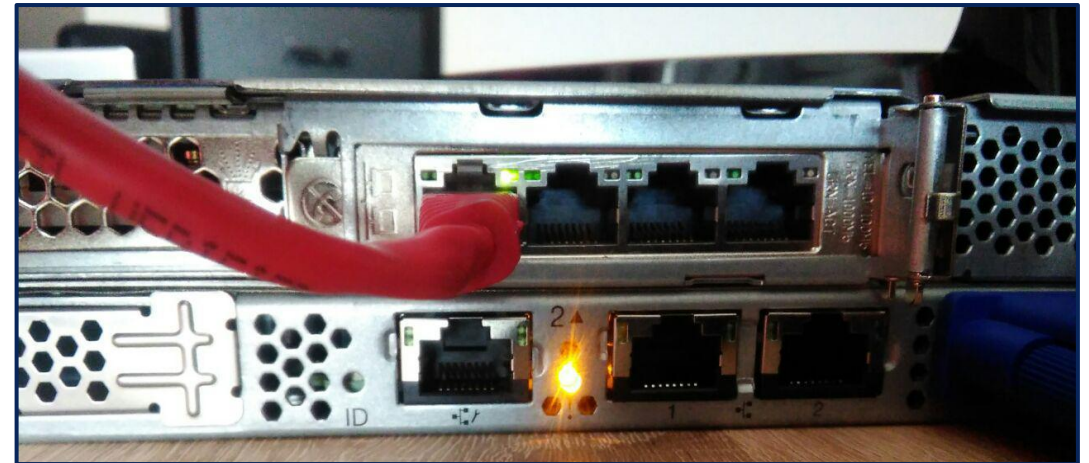
- инвентаризация активов (новые активы);
- отображение сетевых соединений (в т.ч. на карте);
- ведение правил сетевых сессий, сигнатур обнаружения вторжений, правил контроля тегов;
- формирование и отображение событий безопасности по трафику

Настройки Sensor для работы с трафиком

Обязательная переменная, которая задается в `/usr/share/udv/datapk/sensor.env`:

LISTENING_INTERFACES=ens224

- один интерфейс узловой ОС DATAPK, с которого слушается трафик. Если интерфейсов несколько – их надо сперва объединить в Bond (тип Broadcast) средствами ОС
- все интерфейсы д.б. в UP (программно)
- желательно, но не обязательно – в неразборчивом режиме (promisc mode)



Выявление сетевых соединений

Сетевое соединение – уникальная комбинация источника, получателя, портов, протокола транспортного уровня, протоколов более высоких уровней (при наличии).

Фиксируется каждое сетевое соединение. Разрешенность определяется по наличию/отсутствию правила сессии под него. Если соединение появилось в режиме обучения, оно имеет статус «Не определен» и под него создается правило автоматически.

- фиксируются потоки с транспортом TCP, UDP, ICMP и IPv4 адресацией (другие в настоящее время не фиксируются);
- фиксируются потоки при условии, что хотя бы один ip адрес принадлежит контролируемой сети;
- поток «привязывается» к активу на основании адресной информации (mac или ipv4+mac) по возможности;
- в правилах сессий учитывается только серверный порт;
- правила сессий создаются только по IP/подсетям и до уровня транспортного протокола (L4)

Служба обнаружения вторжений	☒
Регистрация событий техпроцесса	☒
Автоматическое создание правил сессий	☒

Служба обнаружения вторжений	☐
Регистрация событий техпроцесса	☐
Автоматическое создание правил сессий	☐

Выявление сетевых соединений

Обновлена 16.02.2026 15:56:01.011 - 16.02.2026 16:16:01.011

Активность Все

IP-адрес отправителя Все

Порт отправителя Все

IP-адрес получателя Все

Протоколы Все

Статус Все

UID сессии Cjg67m1ubZ6SoEQ3D2

Очистить

Обновлена	UID сессии	Длитель...	Отправите...	IP-адрес о...	Порт отпр...	Получатель	IP-адрес п...	Порт полу...
16.02.2026, 16:07:25	Cjg67m1u...	2 мин 11 с	Historian	10.51.200.15	56802	WIN2008-SC...	10.51.200.12	5986

Правила сессий 1 / 813

Создать правило

Дата создания Все

Наименование Все

Сенсоры udv-dtpk-demo

IP-адреса отправителей 10.51.200.15

IP-адреса получателей 10.51.200.12

Порты получателей 5986

Транспортные протоколы TCP

Очистить

Дата создания	Наименование	Сенсоры	IP-адреса отправит...	IP-адреса получате...	Порты по
29.08.2025, 16:19:01	Автоматически созданно...	udv-dtpk-demo	10.51.200.15	10.51.200.12	5986

Сессия (UID) Cjg67m1ubZ6SoEQ3D2

Неактивная

Правила сессий

	Отправитель	Получатель
Наименование:	Historian	WIN2008-SCADA
IP-адрес:	10.51.200.15	10.51.200.12
MAC-адрес:	00:50:56:b7:a0:42	00:50:56:b7:a6:68
Порт:	56802	5986
Пакетов:	32	36
Всего, байт:	19143	32319
Сеть:	Контролируемая	Контролируемая

Обновлена:

16.02.2026, 16:07:25

Обнаружена:

16.02.2026, 16:05:08

Длительность:

2 мин 11 с 553 мс

Сенсор:

udv-dtpk-demo

Состояние:

RSTR: Соединение установлено, но получатель перестал быть доступным (отправлен TCP-флаг RST)

Статус:

Разрешена

Транспортный протокол:

TCP

Создать файл PCAP

Создать правило

События о сессиях

События формируются о новых неразрешенных сессиях в боевом режиме работы.

События о такой сессии (без учета source_port) формируются не чаще 1 раза в сутки

Тип события: **"session_control"**

На стр. сетевых соединений показываются все обнаруженные сессии

В случае появления такого события надо проанализировать взаимодействие, при необходимости посмотреть детальную информацию/рсар-файл. Если взаимодействие легитимное – создать правило сессий (или дополнить существующее)

1270001 session_control

Дата создания: 24.02.2026, 14:39:19.922

[Активы](#) [Сессия](#)

	Отправитель	Получатель
Актив:	—	udv-dtpk-demo
IP-адрес:	10.41.56.30	10.51.200.10
Порт:	3031	22
MAC-адрес:	00:50:56:b7:b1:3a	00:50:56:b7:83:17
Идентификатор:	—	3025669d-a3e0-4d72-ae58-1cdd20219b9a

Событие

Важность:

Критическая

Категория события:

Контроль сессий

Протокол:

TCP

Сообщение:

Контроль сессий; Обнаружена сессия, не разрешенная правилами сессий; CKGuFO1xMihft63qM5

Действие:

Detected

Дополнительная информация:

—

Обоснование:

—

Идентификатор события:

5af17b7e-851f-4cab-8400-57208205af25

Источник события:

datapk_sensor

Доступность активов

- переменная **ASSETS_INACTIVITY_TIMEOUT** в **/usr/share/udv/datapk/manager.env**
- принимает значение в секундах (≥ 600)
- актив доступен – в заданный **ASSETS_INACTIVITY_TIMEOUT** есть пакеты от какого либо интерфейса данного ОЗ
- Тип события: **"host_interface_status_changed"**

В первую очередь надо реагировать, когда узел недоступен длительное время (видно в карточке актива, поле «Последнее появление»). 10 минут для ряда оборудования – это слишком мало (есть устройства, которые раз в сутки или реже генерируют трафик)

DATAPK не предназначен для детальной проверки доступности активов – для этого больше подходят SCADA и системы IT-мониторинга. В ряде инсталляций данные события отключают

1020002 host_interface_status_changed
✕

Дата создания: 24.02.2026, 15:14:47.037

[Активы](#)

	Отправитель	Получатель
Актив:	—	cisco
IP-адрес:	—	10.51.200.11
Порт:	—	—
MAC-адрес:	—	00:50:56:b7:17:7f
Идентификатор:	—	60deee48-f125-423e-b6bd-f4d523e95bba

Событие

Важность:	Низкая
Категория события:	—
Протокол:	—
Сообщение:	[10.51.200.11 - 00:50:56:b7:17:7f]: Интерфейс недоступен (Актив: cisco)
Действие:	—

Работа с картами

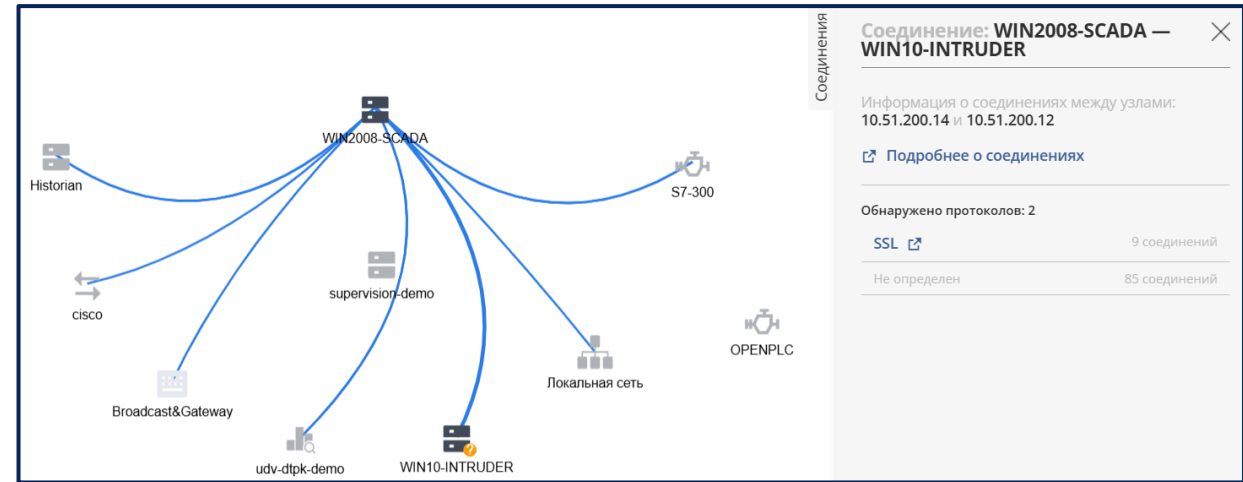
На карте отображаются сетевые соединения за выбранный временной интервал (не более недели). Есть гибкие фильтры. Можно формировать свои представления.

Есть служебные сущности:

Локальная сеть – взаимодействия со смежными локальными сетями в соответствии с RFC (192.168.0.0, 10.0.0.0 и пр.)

Глобальная сеть – взаимодействие с публичными адресами (иногда эти адреса используются внутри контура организации)

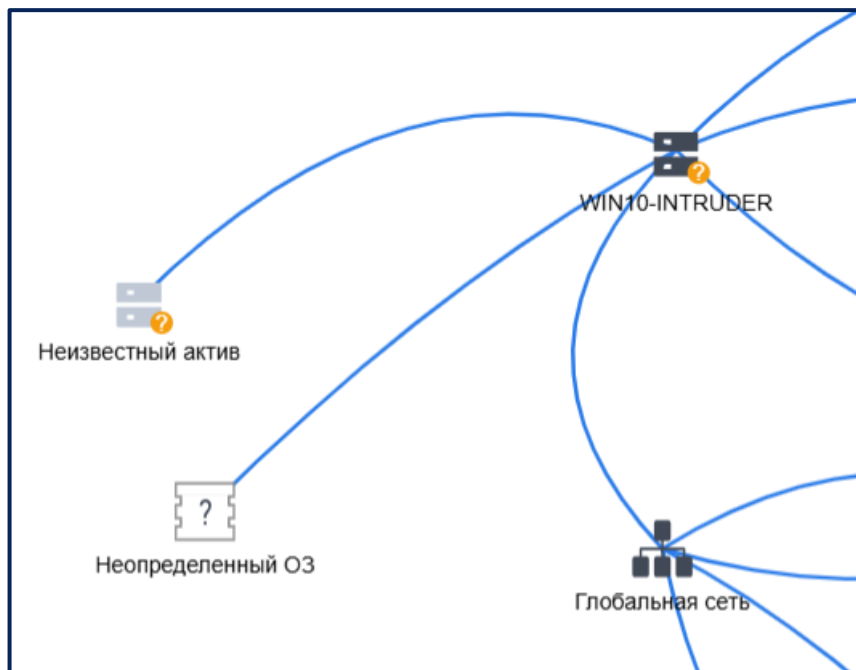
Неопределенный ОЗ – актив, в чью сторону есть сетевые пакеты, но ответных взаимодействий нет (иногда это Broadcast/Multicast-адреса, иногда отправка событий в смежные системы по UDP)



Реагировать в первую очередь надо на:

- *неизвестные активы*
- *взаимодействие с глобальной сетью;*
- *взаимодействие со смежными системами;*
- *неопределенные активы (их можно инвентаризовать вручную при необходимости)*

Работа с картами



Дата обновления

21.02.2026

×

📅

00:00:00

24.02.2026

×

📅

23:59:59

Установить текущие сутки

Наименование / Описание активов

Введите текст

IP-адреса активов

×

10.51.200.0/24

×

▼

Типы активов

Выберите типы ▼

MAC-адреса отправителей

Введите MAC-адреса ▼

☒ Использовать условие "И"

MAC-адреса получателей

Введите MAC-адреса ▼

Применить

Сбросить

Обсуждение

Задание для обсуждения:

DATAPK зафиксировал следующее сетевое соединение:

Источник: 10.51.200.10, 00:50:56:b7:83:17

Порт источника: 51716

Получатель: 10.51.200.13, 00:50:56:b7:5d:fc

Порт получателя: 102

Транспортный протокол: TCP

Протоколы: COTP_TPKT, S7comm

Попадет ли сетевое соединение под следующие правила сессий и почему:

- получатель 10.51.200.0/24, транспортный протокол TCP;
- источник 10.51.200.10, порт получателя 102, транспортный протокол UDP;
- источник 10.51.200.10, получатель 10.51.200.13, порт получателя 102;
- источник 10.51.200.0/24, получатель 10.51.200.0/24, порт получателя 102.

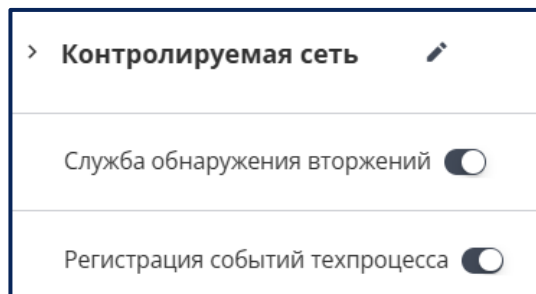
	Отправитель	Получатель
Наименование:	udv-dtpk-demo	S7-300
IP-адрес:	10.51.200.10	10.51.200.13
MAC-адрес:	00:50:56:b7:83:17	00:50:56:b7:5d:fc
Порт:	51716	102
Пакетов:	8	6
Всего, байт:	412	614
Сеть:	Контролируемая	Контролируемая
Обновлена:	24.02.2026, 16:04:35	
Обнаружена:	24.02.2026, 16:04:30	
Длительность:	23 мс	
Сенсор:	udv-dtpk-demo	
Состояние:	SF: Соединение штатно установлено и завершено	
Статус:	Разрешена	
Транспортный протокол:	TCP	
Протоколы:	COTP_TPKT, S7COMM	

Команды техпроцесса

DATAPK умеет фиксировать критичные команды техпроцесса.

Тип события: **"dpi_notice"**

Регистрация событий техпроцесса включается в настройках сенсора



Перечень критичных функций расположен в файле **/usr/share/udv/zeek-wrapper/configs/ics-function.dat** на уровне Sensor

Реагировать надо в первую очередь на события с нетиповых адресов (не относящихся к инженерным станциям), а так же на события в нетиповое время. Некоторые из критичных функций могут вполне легитимно использоваться в защищаемой АСУТП. При необходимости надо выполнить настройку.

1240048 dpi_notice
✕

Дата создания: 24.02.2026, 16:17:18.919

[Активы](#)
[Сессия](#)

	Отправитель	Получатель
Актив:	udv-dtpk-demo	S7-300
IP-адрес:	10.51.200.10	10.51.200.13
Порт:	41622	102
MAC-адрес:	00:50:56:b7:83:17	00:50:56:b7:5d:fc
Идентификатор:	3025669d-a3e0-4d72-ae58-1cdd20219b9a	b2fa025b-c65e-43c0-acca-d1b45eb3cdc0

Событие

Важность: **Критическая**

Категория события: Контроль тех. процесса

Протокол: S7COMM

Сообщение: Контроль тех. процесса; Обнаружено использование функции ПЛК, критичной для технического процесса

Действие: Detected

Дополнительная информация: Upload

Правила контроля тегов

DATAPK умеет разбирать теги Modbus, OPC UA, Emerson DeltaV.

При необходимости контроля критичных параметров техпроцесса можно создавать правила контроля тегов для указанных протоколов.

В правиле указывается IP-адрес ПЛК, адрес регистра и разрешенное значение (диапазон значений). При выходе значения за пределы формируется событие. Так же событие формируется, когда значение возвращается в нормальный диапазон

Тип события: **"tag_control"**

Поскольку правила контроля тегов настраиваются вручную, на события об отклонениях надо реагировать первоначально. Если выясняется, что сработка ложная, корректировать правило.

Переполнение бака

Активно

Сенсор: datapk-demo

IP-адрес ПЛК: 192.168.0.3

Тег: Уровень воды

Описание: —

Дата создания: 20.06.2025, 12:12:49

Дата обновления: 20.02.2026, 10:43:52

Автор: UDV Demo (datapk)

Критерии правила

Адрес: Регистры ввода: 2

Тип данных: int16

Условие: Меньше

Значение: 1500

16 /

2.2026

я Вс

968

793 Критическая Значение тега нормализовалось

514 Критическая Значение тега не соответствует критериям правила

092 Критическая Значение тега не соответствует критериям правила

138 Критическая Значение тега нормализовалось

989 Критическая Значение тега нормализовалось

734 Критическая Значение тега не соответствует критериям правила

382 Критическая Значение тега не соответствует критериям правила

764 Критическая Активировано правило контроля тегов

377 Критическая Активировано правило контроля тегов

1260001 tag_control

Дата создания: 20.02.2026, 11:06:05.514

[Сессия](#) [Правило контроля тегов](#)

Актив: —

IP-адрес: 192.168.0.4

Порт: 46078

MAC-адрес: 00:0c:29:ee:33:a2

Идентификатор: —

Отправитель: —

Получатель: 192.168.0.3 502 00:0c:29:0d:e7:b2

Событие

Важность: Критическая

Категория события: Контроль тегов

Протокол: MODBUS

Сообщение: Сенсор: datapk-demo, IP-адрес отправителя: 192.168.0.4, IP-адрес получателя: 192.168.0.3, MAC-адрес отправителя: 00:0c:29:ee:33:a2, MAC-...

Действие: Detected

Дополнительная информация: Значение тега "Уровень воды" = 1504

Детектирование атак

Модуль iNTA умеет фиксировать сетевые атаки собственными механизмами (на базе плагинов Zeek).

Тип события: **"dpi_notice"** или **"ml_notice"**

Регистрация событий включается в блоке «Управление регистрацией трафика». По умолчанию включено все.

Белый список задается в **/usr/share/udv/zeek-wrapper/configs/general.dat** на уровне Sensor

Подобные события в большинстве случаев свидетельствуют о явной атаке. Поэтому на них необходимо приоритетно реагировать (идентифицировать источник, получателей, понять, легитимный ли протокол взаимодействия, посмотреть информацию о сетевых соединениях). Иногда сработки ложные (использование устаревших протоколов, взаимодействия внутри домена) – в этом случае надо тюнить файл исключений

1240032 dpi_notice

Дата создания: 24.02.2026, 16:38:48.167

[Активы](#) [Сессия](#)

	Отправитель	Получатель
Актив:	Сервер для тес...	Тестовый узел
IP-адрес:	192.168.134.21	192.168.134.20
Порт:	51906	445
MAC-адрес:	00:0c:29:26:7d:58	00:0c:29:97:35:8f
Идентификатор:	41695f3c-3c48-4110-a8d4-31c01b5a5953	38231e32-0e43-44b3-8e17-38a6427a8ddc

Событие

Важность:

Критическая

Категория события:

Перемещение внутри периметра

Протокол:

SMB

Сообщение:

Перемещение внутри периметра; Обнаружена техника атаки T1210: Эксплуатация удаленных служб; Ck5Hj311PrgMQrc6ih;...

[Показать полностью](#)

Действие:

—

Дополнительная информация:

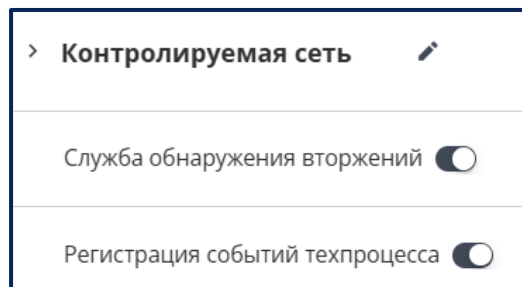
DoublePulsar

Обнаружение вторжений (Suricata)

В модуль iNTA так же входит классический механизм IDS на базе Suricata. Правила поставляются производителем DATAPK. При необходимости можно импортировать (или написать) свои

Тип события: **"ids_event"**

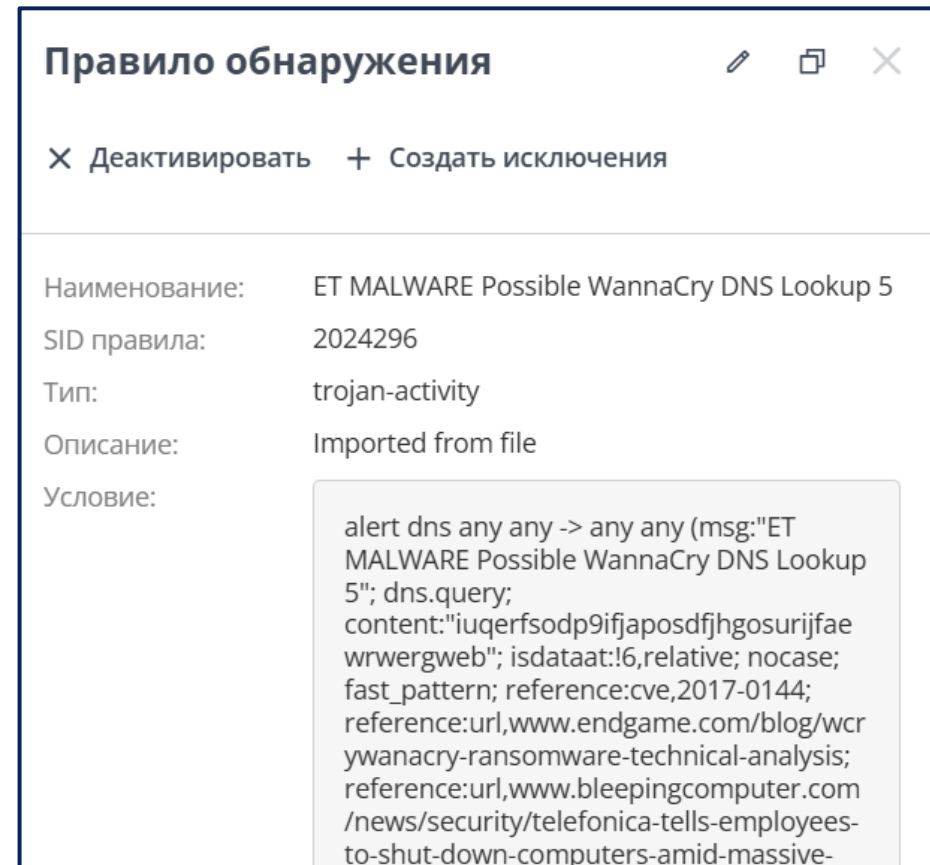
Служба обнаружения вторжений включается в настройках сенсора



Правила импортируются и редактируются на уровне Management. После внесения изменений правила необходимо синхронизировать.

Можно отключать ненужные правила, можно создавать исключения (отключать правила на определенных сенсорах).

Базовые правило не рекомендуется менять – лучше их отключать и создавать новые на их базе в пользовательском диапазоне SID (94000000-94999999) во избежание потерь при обновлении сигнатур



Обнаружение вторжений (Suricata)

События

События 4 / 58

Дата создания 01.07.2025 00:00:00.000 x
Важность Все v
Описание EXPLOIT Possible ETERNALBLUE v

IP-адрес получателя Все v
+
Очистить

Дата создания	Важность	Описание
24.02.2026, 16:38:48.000	Критическая	EXPLOIT Possible ETERNALBLUE SMB Exploit Attempt Stage 1/2 - Tree Connect
24.02.2026, 16:38:48.000	Критическая	EXPLOIT Possible ETERNALBLUE SMB Exploit Attempt Stage 2/2 - Trans2 SUCCE
24.02.2026, 16:38:48.000	Критическая	ET EXPLOIT Possible ETERNALBLUE MS17-010 Echo Response
24.02.2026, 16:38:48.000	Критическая	ET EXPLOIT Possible ETERNALBLUE MS17-010 Heap Spray

1280009 ids_event x

Дата создания: 24.02.2026, 16:38:48.000

Активы
Сессия
Правила обнаружения

	Отправитель	Получатель
Актив:	Сервер для тес...	Тестовый узел
IP-адрес:	192.168.134.21	192.168.134.20
Порт:	51906	445
MAC-адрес:	00:0c:29:26:7d:58	00:0c:29:97:35:8f
Идентификатор:	41695f3c-3c48-4110-a8d4-31c01b5a5953	38231e32-0e43-44b3-8e17-38a6427a8ddc

Событие

Важность: Критическая
Категория события: alert
Протокол: TCP
Сообщение: intrusion_detection[4405]: {"timestamp":"2026-02-24T16:38:48.147719+0500","flow_id":70284223234152,"in_iface":"dummy0","ev...
Действие: allowed

Из события можно перейти к правилу, сессии, активам и проанализировать более детально

Обнаружение вторжений (Suricata)

Так же можно писать сложные исключения (pass-правила) для исключения сработок по определенным IP-адресам/подсетям.

Для пользовательских правил (pass-правил в частности) зарезервирован диапазон 94000000-94999999

При создании pass-правил нельзя использовать конструкции threshold: type both и threshold: type limit (убирать при создании исключений)

Пример:

```
alert tcp any any -> any any (msg:"ET SCAN NMAP -sS window 1024"; fragbits:!D; dsize:0; flags:S,12; ack:0; window:1024; threshold: type both, track by_dst, count 1, seconds 60; reference:url,doc.emergingthreats.net/2009582; classtype:attempted-recon; sid:2009582; rev:3; metadata:created_at 2010_07_30, updated_at 2010_07_30;)
```

Исключение для него (не срабатываем, когда 192.168.0.1 сканирует 192.168.0.2):

```
pass tcp 192.168.0.1 any -> 192.168.0.2 any (msg:"ET SCAN NMAP -sS window 1024"; fragbits:!D; dsize:0; flags:S,12; ack:0; window:1024; reference:url,doc.emergingthreats.net/2009582; classtype:attempted-recon; sid: 94000000;)
```

События IDS могут свидетельствовать о сетевой атаке, однако довольно часто при отсутствии тюнинга правил происходят ложные сработки (из-за устаревших протоколов в АСУТП, легитимных сканирований сети и пр.).

В первую очередь надо реагировать на критичные сработки (поле «Дополнительная информация» <=3). Так же по результатам анализа надо создавать исключения.

Вопросы?