УТВЕРЖДАЮ

Генеральный директор
АО «Эшелон Технологии»

_____ А.В. Дорофеев

«___» _____ 2025 г.

NTA ESENSOR

Руководство администратора

АПДГ.11100-01 91

Листов 48

2025

АННОТАЦИЯ

Настоящий документ представляет собой руководство администратора изделия «NTA eSensor» АПДГ.11100-01 (далее – eSensor, изделие).

В документе содержатся следующие сведения:

– общие сведения о программе (п. 1 настоящего документа);

– структура программы (п. 2 и настоящего документа);

– настройка программы (п. 3 настоящего документа);

– проверка программы (п. 4 настоящего документа);

– сообщения администратору (п. 5 настоящего документа).

Настоящий документ предназначен для администратора eSensor.

Под администратором понимается любое лицо, допущенное до эксплуатации изделия с ролью «Администратор».

Под «машиной» понимается автоматизированное рабочее место и/или электронно-вычислительная машина (прим. сервер), используемая пользователем eSensor.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ПРИНЯТЫХ ТЕРМИНОВ И СОКРАЩЕНИЙ

SCTP	—	(англ. *Stream Control Transmission Protocol*) – протокол транспортного уровня
SIEM	—	(англ. *Security information and event management*) – управление информацией о безопасности и событиями безопасности
SSH	—	(англ. *Secure Shell*) – защищенный сетевой протокол для удалённого управления сервером через интернет
ИБ	—	информационная безопасность
МЭ	—	межсетевой экран
НСД	—	несанкционированный доступ
ОС	—	операционная система
ПО	—	программное обеспечение
СЗИ	—	средство защиты информации
СУБД	—	система управления базами данных
СУС	—	сервер управления сенсорами
Терминал	—	встроенный системный терминал «Fly» операционной системы специального назначения Astra Linux

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1. Назначение программы

eSensor предназначен для обнаружения компьютерных атак на оборудование сетей связи и передачи данных, подключенные к ним комплексы средств автоматизации и автоматизированные (информационные) системы управления.

1.2. Функции программы

eSensor обеспечивает выполнение следующих основных функций:

– управление сенсорами;

– регистрацию информации о сетевых взаимодействиях (сессиях);

– анализ сетевого трафика с использованием сигнатурных и эвристических методов, и регистрацию событий информационной безопасности (далее – ИБ);

– управление базой решающих правил сигнатурного анализа;

– анализ фрагментированного сетевого трафика;

– захват сетевого трафика с последующей записью в PCAP-файлы;

– выгрузку PCAP-файлов с трафиком за заданный период времени;

– анализ PCAP-файлов с использованием сигнатурных и эвристических методов;

– отправку событий ИБ в SIEM-системы.

2. СТРУКТУРА ПРОГРАММЫ

eSensor имеет модульную структуру, функционал модулей реализуется набором служб операционной системы. Сведения о структуре eSensor представлены в таблице 1.

Таблица 1 – Структура eSensor

Модуль	**Служба**
Сенсор	ids-sensor@<Порт>.service, где <Порт> – порт, по которому по умолчанию доступен сенсор (задается при установке сенсора)
Сервер аутентификации	pauth-server.service
Сервер управления сенсорами	ids-backend.service
СУБД «ClickHouse»	clickhouse-server.service
NoSQL СУБД «Redis»	ids-redis.service

Кроме того, для работы eSensor используется внешняя система управления базами данных (далее – СУБД) «PostgreSQL», которая не входит в состав изделия. Её функционал реализуется двумя службами: `postgresql.service` и `postgresql@11-main.service`.

Может быть один или несколько сенсоров, на одной или нескольких машинах. Каждый сенсор состоит из набора подмодулей, которые реализуют различные функции:

– модуля регистрации сессий, обеспечивающего регистрацию информации о сетевых сессиях;

– модуля сигнатурного анализа, обеспечивающего обнаружение вредоносной активности с использованием специальных правил (п. 3.8 настоящего документа);

– модуля эвристического анализа, обеспечивающего извлечение файлов, передаваемых в сессиях;

– модуля захвата трафика, обеспечивающего циклическую запись копии захватываемого трафика;

– модуля отправки событий, обеспечивающего отправку данных об атаках, регистрируемых сенсорами, в СУБД «ClickHouse» и внешние системы.

Сервер аутентификации предназначен для управления доступом к eSensor.

Сервер управления сенсорами предназначен для управления и конфигурации сенсоров, управления базой правил сигнатурного анализа и хранилищем PCAP-файлов.

СУБД «ClickHouse» используется для хранения метаинформации о сетевых сессиях и атаках, регистрируемой сенсорами.

СУБД «Redis» используется при выполнении различных внутрисистемных задач, происходящих на сервере управления сенсорами.

СУБД «PostgreSQL» используется для хранения данных сервера управления сенсорами и сервера аутентификации.

На рис. 1 изображена структурная схема eSensor.

Структурная схема eSensor

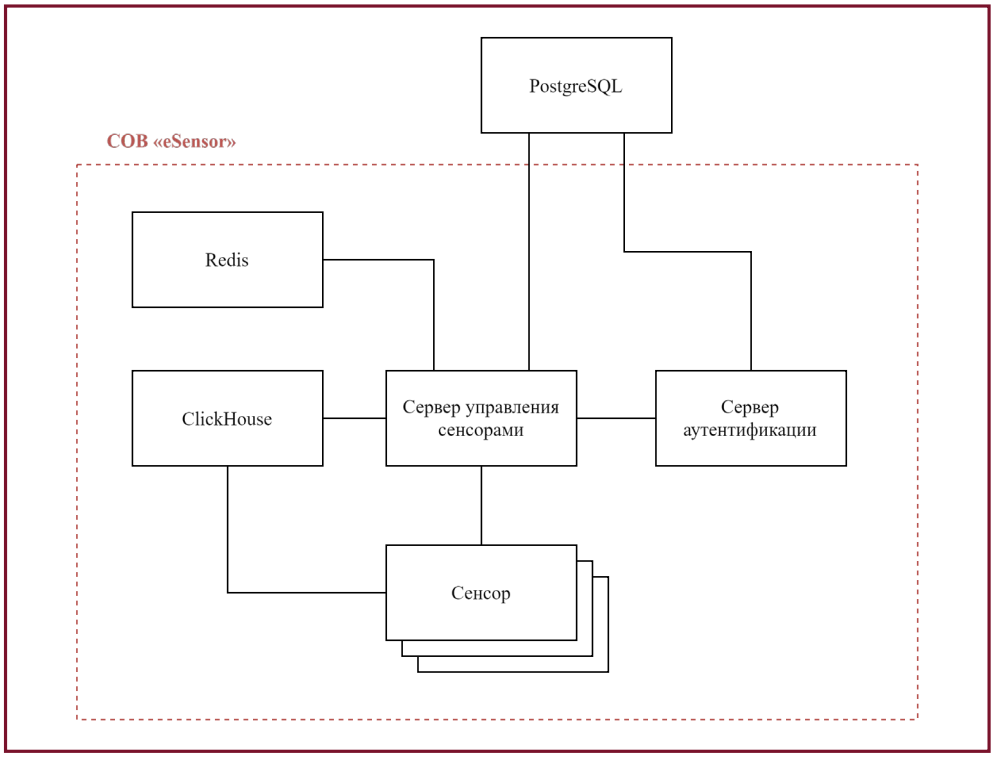

Рис. 1

3. НАСТРОЙКА ПРОГРАММЫ

3.1. Выбор схемы развертывания

Перед установкой eSensor необходимо выбрать схему развертывания – состав выделенных под нее машин, а также то, как должны быть распределены по ним ее модули.

Установка eSensor выполняется с использованием ролей – логических объединений модулей eSensor, выполняющих вместе определенный набор функций.

Используются три роли:

– роль «sensor». В данную роль входят сенсоры. Выполняет захват и анализ трафика;

– роль «server». В данную роль входят: сервер управления сенсорами (далее – СУС), СУБД «PostgreSQL», «ClickHouse» и «Redis». Обеспечивает управление сенсорами и хранение данных, поступающих от сенсоров;

– роль «pauth». В данную роль входит сервер аутентификации. Обеспечивает управление учетными записями пользователей, их ролями, идентификацией, аутентификацией и авторизацией пользователей.

Модули одной роли устанавливаются совместно на одну машину. Модули разных ролей могут быть установлены на одну машину или на разные машины.

Типовая схема развертывания (см. рис. 2) заключается в установке модулей ролей «server» и «pauth» вместе на одну машину (машину 1), а сенсоров (роль «sensor») – отдельно, на другую машину (машину 2) или несколько других машин (машин 2-n). На одной машине может быть развернут один или несколько сенсоров.

Типовая схема развертывания

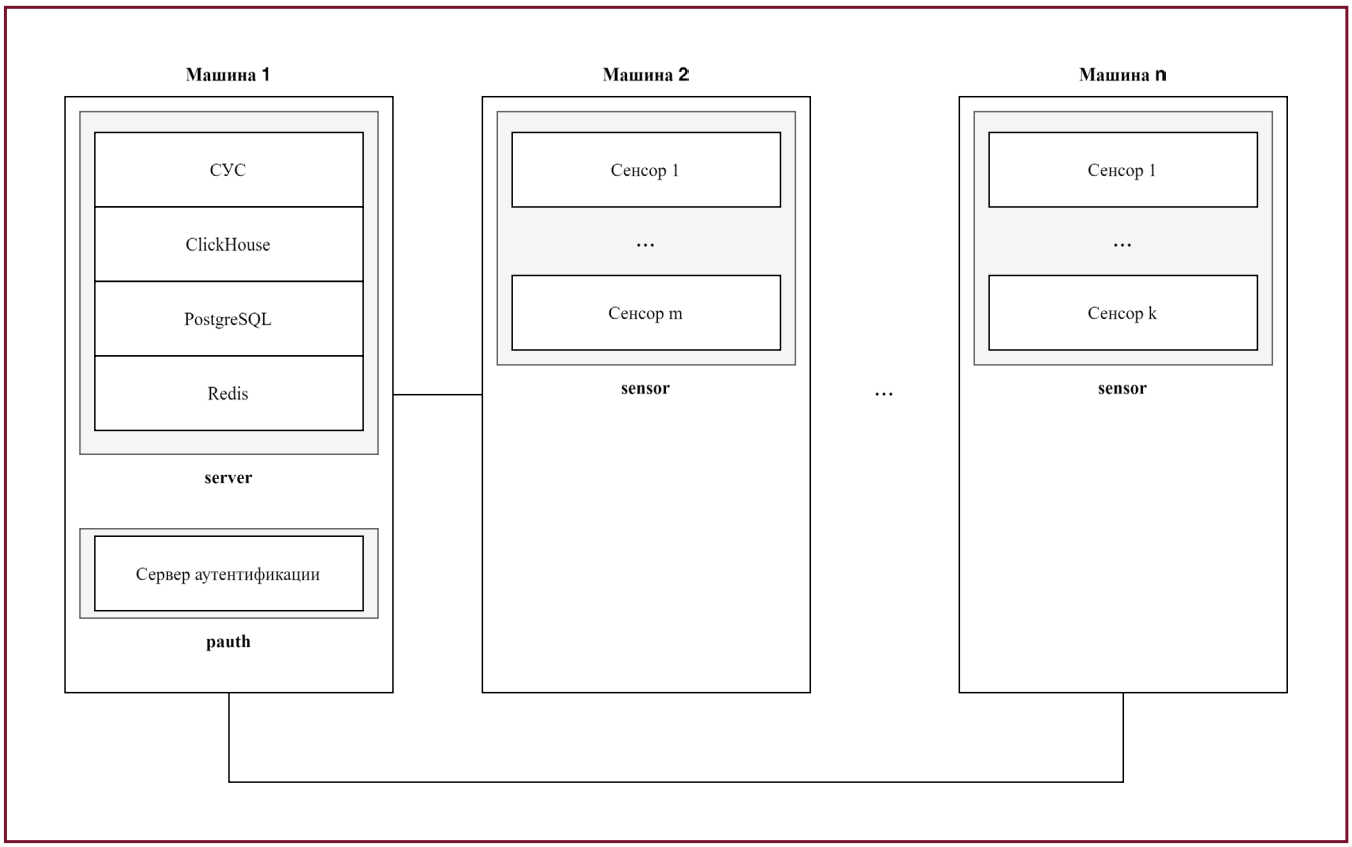

Рис. 2

3.2. Выбор точек и технологии захвата трафика

Перед установкой eSensor необходимо выбрать точки захвата трафика – места в сети организации, трафик в которых необходимо анализировать.

Рекомендуется выбирать точки захвата на основе того, насколько может быть полезен для оператора анализ трафика, захватываемого из данной точки, и какие будут затраты на оборудование – чем больше трафика захватывается, тем более производительное оборудование потребуется для его анализа.

3.2.1. Пример сети с точками захвата трафика

Далее на примере сети организации, включающей сегменты, встречающиеся во многих сетях, показаны возможные точки захвата трафика с кратким описанием особенностей захвата и анализа трафика из данных точек.

На рис. 3 представлена схема сети организации, включающая следующие сегменты:

– две локальные подсети (LAN), в которые могут входить, например, рабочие компьютеры сотрудников, IP-телефоны, IP-камеры видеонаблюдения, принтеры и сканеры;

– локальные сервисы, например, прокси-сервер, DNS-сервер и файловое хранилище;

– демилитаризованная зона (DMZ), в которую могут входить, например, веб-сервер и почтовый сервер организации.

Конечные узлы объединены в подсети коммутаторами уровня доступа, которые, в свою очередь, подключены к межсетевому экрану (далее – МЭ) с функциями маршрутизатора. МЭ также обеспечивает соединение внутренних узлов с интернетом.

Схема сети организации

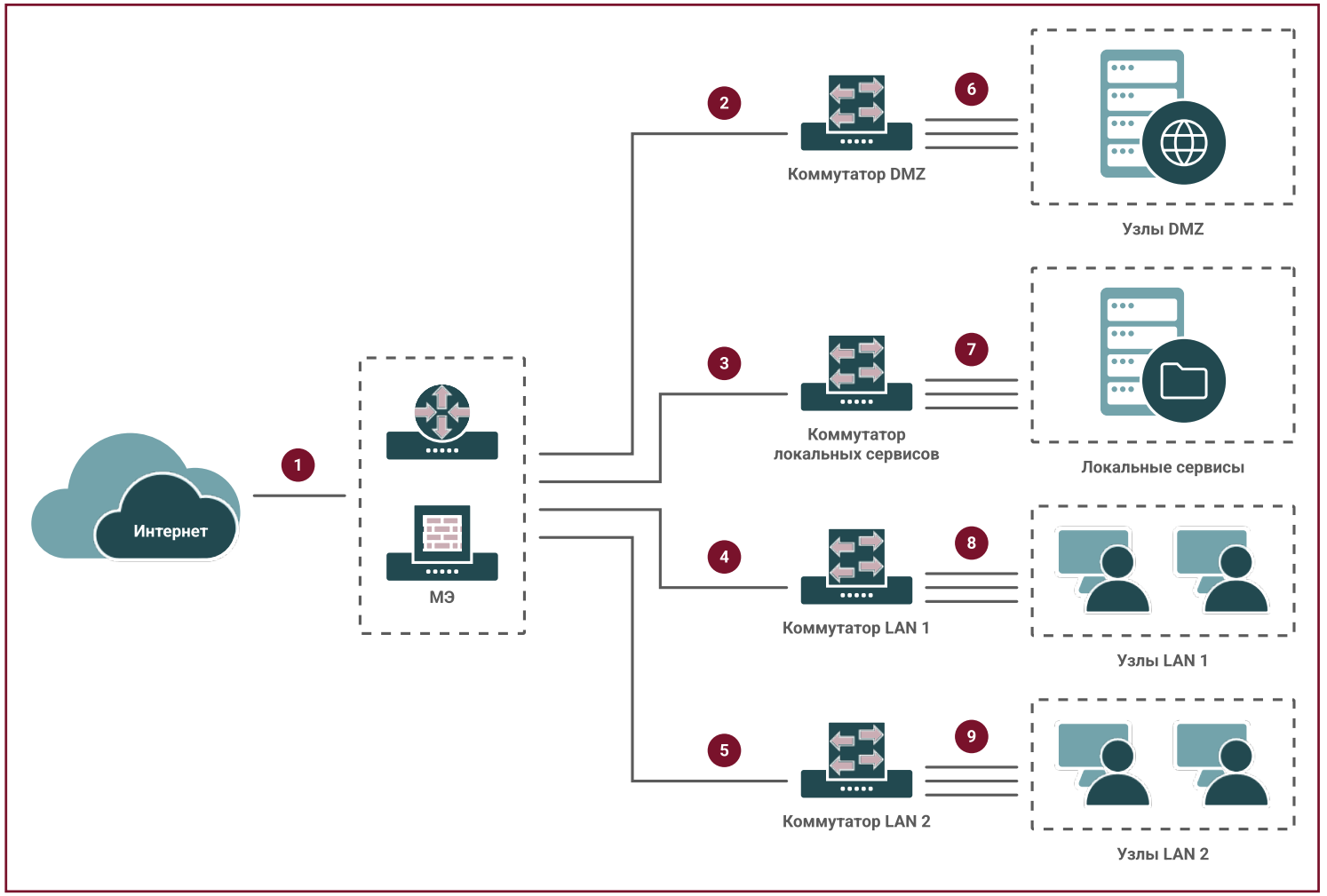

Рис. 3

3.2.1.1. Захват трафика с интерфейсов МЭ

Через WAN-интерфейс МЭ проходит весь трафик между узлами сети организации и интернетом (точка 1 на рис. 3). Захват и анализ трафика из данной точки позволяет обнаруживать вредоносный трафик, идущий из интернета, в том числе, ту его часть, которая направлена на сам МЭ. Кроме того, в случае компрометации МЭ, здесь можно обнаружить обмен данными между ним и внешними узлами.

Однако захват трафика только из этой точки не позволит выявлять вредоносный трафик внутри сети организации. Для этого необходимо захватывать трафик из других точек.

Дополнительный захват трафика с LAN-интерфейсов МЭ (точки 2, 3, 4 и 5 на рис. 3) позволит обнаруживать вредоносный трафик, идущий между внутренними сегментами сети, а также от внутренних узлов на МЭ и обратно, в случаях компрометации каких-либо из данных узлов. Однако для уменьшения объема анализируемого трафика стоит оценить, нужно ли захватывать весь трафик, идущий через данные точки, или только какую-то определенную его часть.

3.2.1.2. Захват трафика DMZ

Специфика DMZ в том, что к ресурсам, расположенным на узлах этой сети, есть доступ не только из внутренней, но и из внешней сети. Это повышает вероятность атак на данные узлы, поэтому контроль входящего и исходящего из DMZ трафика (точка 2 на рис. 3) может быть очень полезен.

Если необходимо контролировать трафик только конкретных узлов DMZ, для этого подойдет точка 6 на рис. 3. Трафик, которым обмениваются узлы DMZ между собой, можно контролировать только из этой точки.

3.2.1.3. Захват трафика локальных сервисов

Локальные сервисы, как правило, являются критически важными активами, поэтому потенциально может быть очень полезно контролировать трафик между узлами с ними и другими узлами организации в точке 3 на рис. 3.

Если необходимо контролировать трафик только конкретных узлов с локальными сервисами, для этого подойдет точка 7 на рис. 3. Трафик, которым обмениваются узлы локальных сервисов между собой, можно контролировать только из этой точки.

3.2.1.4. Захват трафика узлов LAN

В локальных сетях, в которых находятся рабочие места сотрудников, потенциально может быть большое количество узлов – как правило, это зависит от размера самой организации. Захват и анализ всего трафика из этих подсетей (точки 4 и 5 на рис. 3) может быть очень затратен и при этом не всегда целесообразен. Стоит рассмотреть захват только некоторой части данного трафика, представляющей наибольший интерес, или захватывать трафик только определенных узлов (точки 8 и 9 на рис. 3). Как и в случае с DMZ и локальными сервисами, трафик между узлами внутри LAN 1 можно контролировать только из точки 8 на рис. 3, а LAN 2 – из точки 9 на рис. 3.

3.2.2. Технологии захвата трафика

Для захвата трафика используются специализированные TAP-устройства, а также технология зеркалирования (дублирования) трафика с сетевых интерфейсов коммутаторов – SPAN.

3.3. Аппаратные и программные требования

3.3.1. Аппаратные требования

Аппаратные требования зависят от скорости захвата трафика в организации.

Ориентировочные аппаратные требования представлены в таблице 2.

Требования составлены с учетом следующих условий:

1) используются 2 машины: одна для сенсора («Sensor»), другая для всех остальных модулей eSensor («Server»);

2) на машине «Sensor» развернут 1 экземпляр программного обеспечения (далее – ПО) сенсора;

3) одновременно используется только 1 из 2 механизмов записи трафика: либо запись копии трафика сетевых сессий (записи трафика разбиты по сетевым сессиям – это позволяет выгружать записи конкретных сетевых сессий), либо модуль захвата трафика сенсора (записывается весь трафик без разделения его на сессии – это позволяет выгружать запись за определенный период времени);

4) записанную копию сетевого трафика необходимо хранить 3 дня;

5) метаданные о сессиях и атаках необходимо хранить 7 дней;

6) извлеченные файлы необходимо хранить 7 дней – с учетом стандартного значения настройки ограничения максимального размера сохраняемых извлекаемых файлов.

Приведенный в таблице 2 объем SSD и HDD, используемых для хранения данных и метаданных о сетевом трафике, примерный. Реальный объем сильно зависит от специфики трафика в конкретной сети.

Таблица 2 – Аппаратные требования

Аппаратное обеспечение	**Параметр**	**Значения**					
		Для обработки трафика до 10 Мбит/сек		**Для обработки трафика до 100 Мбит/сек**		**Для обработки трафика до 1000 Мбит/сек**	
		Сенсор	**Сервер**	**Сенсор**	**Сервер**	**Сенсор**	**Сервер**
Сетевая карта	Сетевой интерфейс для захвата трафика	1 x 10 Мбит/сек	–	1 x 100 Мбит/сек	–	1 x 1000 Мбит/сек	–
	Сетевой интерфейс для внутреннего взаимодействия компонентов eSensor	1 x 1000 Мбит/сек					
	Сетевой интерфейс для доступа к пользовательскому интерфейсу	1 x 100/1000 Мбит/сек					
Центральный процессор	Частота	2.2 ГГц					
	Ядра	8		16		32	
Память (ОЗУ)	Объем	32 ГБ	16 ГБ	32 ГБ	32 ГБ	64 ГБ	64 ГБ
Твердотельные накопители (SSD) для работы ОС и компонентов eSensor	Объем	500 ГБ					

Аппаратное обеспечение	**Параметр**	**Значения**					
		Для обработки трафика до 10 Мбит/сек		**Для обработки трафика до 100 Мбит/сек**		**Для обработки трафика до 1000 Мбит/сек**	
		Сенсор	**Сервер**	**Сенсор**	**Сервер**	**Сенсор**	**Сервер**
Твердотельные накопители (SSD) для хранения метаданных трафика	Объем	–	5 ГБ	–	50 ГБ	–	500 ГБ
Жесткие диски (HDD) для хранилища PCAP-файлов	Объем	–	Зависит от объема данных, который необходимо хранить	–	Зависит от объема данных, который необходимо хранить	–	Зависит от объема данных, который необходимо хранить
Жесткие диски (HDD) для хранения файлов с записанным трафиком*	Объем	500 ГБ	–	5 ТБ	–	50 ТБ	–
	Скорость записи	2 МБ/сек	–	20 МБ/сек	–	200 МБ/сек	–
Жесткие диски (HDD) для хранения извлеченных из трафика файлов	Объем	500 ГБ	–	500 ГБ	–	5 ТБ	–
* – Значения объема указаны с запасом, с учетом дополнительного объема, добавляемого служебными данными в файлах с записанным трафиком							

Для увеличения надежности хранения данных рекомендуется объединять диски с данными при сетевой нагрузке:

– до 100 Мбит/сек – в RAID 1;

– до 1000 Мбит/сек – в RAID 10.

Рекомендуется выключить SWAP на обеих машинах.

3.3.2. Программные требования

Программные требования:

– на машине, с которой будет производиться установка eSensor, **и всех машинах, на которые необходимо установить компоненты eSensor**:

1) установлена операционная система (далее – ОС) Astra Linux Special Edition 1.7 с уровнем защищенности «Максимальный»;

2) установлены обновления Astra Linux Special Edition 1.7.4;

3) доступны репозитории пакетов Astra Linux Special Edition 1.7.4:

а) основной репозиторий – main;

б) обновления основного репозитория – update;

в) базовый репозиторий – base;

г) расширенный репозиторий – extended.

4) режимы мандатного управления доступом, мандатного контроля целостности и замкнутой программной среды выключены.

Примечания:

1. При необходимости часть или все компоненты eSensor можно установить на ту же машину, с которой будет производиться установка.

2. Информацию о том, как выполнить условия п. 3.3.2 подп. 1) – 4) настоящего документа, можно найти в официальной документации ОС Astra Linux Special Edition 1.7.

3. Рекомендуется устанавливать все компоненты eSensor на машины с установленной ОС Astra Linux Special Edition 1.7.4 **без предварительно установленного стороннего прикладного ПО**.

– время, установленное на всех машинах, должно быть синхронизировано;

– всем машинам, на которые необходимо установить компоненты eSensor, присвоены доменные имена. Во время установки данные машины должны быть доступны по данным доменным именам друг для друга, а также для машины, с которой будет производиться установка.

ВНИМАНИЕ!

Машины с установленными компонентами eSensor **должны оставаться доступными** друг для друга по заданным доменным именам и после установки, на протяжении всего времени эксплуатации eSensor.

Примечание. Присвоить доменные имена машинам можно, например, отредактировав файл `/etc/hosts` (см. ПРИЛОЖЕНИЕ 1 настоящего документа).

3.4. Установка и подключение к веб-интерфейсу программы

3.4.1. Установка

ВНИМАНИЕ!

Перед установкой необходимо удостовериться, что выполнены все аппаратные и программные требования (см. раздел 3.3 настоящего документа).

Установка осуществляется из-под учетной записи пользователя ОС, обладающего правами администратора, т.е. находящегося в группе пользователей astra-admin.

Примечание. Удаление eSensor также осуществляется из-под данной учетной записи (см. п. 3.12 настоящего документа).

ВНИМАНИЕ!

Установка из-под учетной записи «`root`» не допускается.

Все шаги установки (п. 3.4.1 подп. 3.4.1.1 – 3.4.1.4 настоящего документа) выполняются во встроенном системном терминале «Fly» ОС специального назначения Astra Linux (далее – терминал) машины, с которой необходимо произвести установку.

3.4.1.1. Шаг 1. Установка необходимых библиотек

Необходимо выполнить следующие действия:

1) выполнить следующие команды:

```
sudo apt update
sudo astra-update -A -r -T
sudo apt install -y --no-install-recommends ansible python3-netaddr python3-requests sshpass apache2-utils
```

3.4.1.2. Шаг 2. Распаковка архива с дистрибутивом eSensor и подготовка файла лицензии

Необходимо выполнить следующие действия:

1) скопировать архив с дистрибутивом eSensor в любой каталог;

Примечание. Архив имеет название `esensor-v<Номер версии>.tar.gz`, например, `esensor-v0.1.6.tar.gz`.

2) перейти в директорию с архивом;

3) распаковать архив, выполнив команду:

```
tar -xvf <Название архива>
```

4) скопировать файл лицензии `production.lic` в распакованную поддиректорию `esensor/roles/ids-backend/files/`.

3.4.1.3. Шаг 3. Настройка Ansible

На данном шаге настраивается, на какие машины необходимо установить модули eSensor, а также задаются настройки подключения к данным машинам.

Необходимо выполнить следующие действия:

1) перейти в директорию `esensor`, распакованную на предыдущем шаге установки и выполнить команду:

```
cd esensor
```

2) открыть файл `hosts_esensor.yml` и указать в нем, какие модули системы и на какие машины необходимо установить:

```
nano hosts_esensor.yml
```

В блоке настроек `all.children.pauth.hosts` необходимо задать настройки установки сервера аутентификации:

– `<pauth_hostname>` – доменное имя машины, на которую необходимо установить сервер аутентификации. Данная машина должна быть доступна по данному доменному имени для всех других машин, на которые будут установлены остальные модули eSensor, а также для машины, с которой производится установка;

– `<pauth_user>` – имя пользователя машины `<pauth_hostname>`, от имени которого будет производиться установка на данной машине;

– `<pauth_user_password>` – пароль пользователя `<pauth_user>`.

Примечание. В стандартных конфигурациях Astra Linux SE 1.7 пароль для входа по SSH и пароль для выполнения административных команд (sudo) совпадают. Поэтому в полях ansible_password и ansible_become_password следует указать один и тот же пароль пользователя <pauth_user>.

Аналогичным образом необходимо задать настройки установки:

– СУС, СУБД ClickHouse, PostgreSQL и Redis (`all.children.esensor_server.hosts`):

1) `<server_hostname>`;
2) `<server_user>`;
3) `<server_user_password>`.

– сенсоров (`all.children.esensor_sensors.hosts`):

1) `<sensors_hostname>`;
2) `<sensors_user>`;
3) `<sensors_user_password>`.

ВНИМАНИЕ!

Пользователи `<pauth_user>`, `<server_user>` и `<sensors_user>` должны обладать правами администратора на своих машинах (находиться в группе пользователей astra-admin), при этом указание суперпользователя «`root`» **не допускается**. Пароли пользователей `<pauth_user_password>`, `<server_user_password>` и `<sensors_user_password>` необходимо вводить в двойных кавычках (`"`).

На одну машину можно установить один или нескольких сенсоров. В блоке настроек `all.children.esensor_sensors.hosts.<sensors_hostname>.sensors` необходимо задать настройки установки каждого сенсора:

– `<port>` – сетевой порт, который будет использоваться установленным сенсором для связи с другими модулями eSensor. Указываемый порт должен быть уникальным для каждого сенсора на машине и должен быть не занят;

– `<iface>` – название сетевого интерфейса, трафик которого должен анализировать сенсор.

Сенсоры можно устанавливать на несколько разных машин. Для этого в блоке настроек `all.children.esensor_sensors.hosts` необходимо задать настройки установки сенсоров на каждой машине.

ВНИМАНИЕ!

Максимальное допустимое количество сенсоров, которые можно установить и подключить к СУС, определяется используемой лицензией. Файл с лицензией уже присутствует среди установочных файлов и будет определен при установке автоматически, дополнительных действий не требуется.

Пример полной настройки:

```
all:
  children:
    # Настройки установки сервера аутентификации
    pauth:
      hosts:
        esensor-server:
          ansible_user: user0
          ansible_password: "password0"
          ansible_become_password: "password0"



    # Настройки установки сервера управления сенсорами, а также СУБД
ClickHouse, PostgreSQL и Redis
    esensor_server:
      hosts:
        esensor-server:
          ansible_user: user0
          ansible_password: "password0"
          ansible_become_password: "password0"



    # Настройки установки сенсоров
    esensor_sensors:
      hosts:
        esensor-sensors1:
          ansible_user: user1
```

```
          ansible_password: "password1"
          ansible_become_password: "password1"
          sensors:
            - port: 7110
              iface: eth0
            - port: 7111
              iface: eth1
        esensor-sensors2:
          ansible_user: user2
          ansible_password: "password2"
          ansible_become_password: "password2"
          sensors:
            - port: 7110
              iface: eth0
            - port: 7111
              iface: eth1

  vars:
    ansible_connection: ssh
    ansible_ssh_common_args: '-o StrictHostKeyChecking=no'
```

В данном примере заданы следующие настройки:

– сервер аутентификации будет установлен на машину `esensor-server` от имени пользователя `user0` с паролем `password0`;

– СУС, ClickHouse, PostgreSQL и Redis также будут установлены на машину `esensor-server` от имени пользователя `user0`;

– 2 сенсора будут установлены на машину `esensor-sensors1` от имени пользователя `user1` с паролем `password1`. Данные сенсоры будут доступны на портах `7110` и `7111` и будут захватывать и анализировать трафик сетевых интерфейсов `eth0` и `eth1` машины `esensor-sensors1` соответственно;

– еще 2 сенсора будут установлены на машину `esensor-sensors2` от имени пользователя `user2` с паролем `password2`. Для них заданы те же настройки, что и для сенсоров на машине `esensor-sensors1`.

После завершения ввода настроек **необходимо сохранить изменения в файле**.

3.4.1.4. Шаг 4. Запуск установочного скрипта

Необходимо выполнить следующие действия:

– находясь в распакованном каталоге `esensor`, выполнить команду:

```
ansible-playbook -vv -i hosts_esensor.yml --ask-become-pass -e
installer_data=installer_data install.yml
```

– при передаче ОС последней команды начнется выполнение установочного скрипта;

– в процессе установки потребуется ввести пароль **текущего пользователя**. Сообщение с запросом на ввод данного пароля выглядит следующим образом:

```
SUDO password:
```

– далее необходимо задать желаемый пароль учетной записи администратора eSensor и подтвердить его. Сообщение с запросом на ввод пароля выглядит следующим образом:

```
При установке в eSensor будет создан пользователь с логином root,
обладающий правами администратора.
Необходимо задать для него пароль.
Введите пароль:
```

ВНИМАНИЕ!

При задании пароля допустимо использовать только строчные и прописные буквы латинского алфавита и цифры.

– успешное выполнение установочного скрипта завершается сообщением `PLAY RECAP` с последующим перечислением, на какие машины были установлены модули eSensor, и текущей машиной (`127.0.0.1`), при этом **у всех машин** `unreachable=0` и `failed=0`. Пример сообщения показан на рис. 4.

Пример завершения установки без ошибок

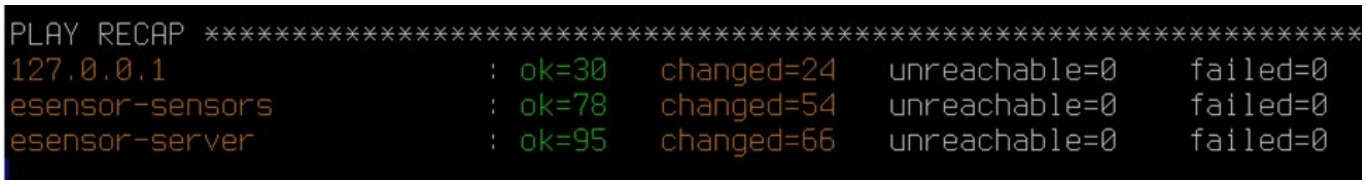

Рис. 4

Примечание. Числа `ok` и `changed` могут отличаться от изображенных на рис. 4.

Если число `unreachable` или `failed` для какой-либо из перечисленных машин больше нуля, это означает, что в процессе выполнения установочного скрипта произошли ошибки (см. рис. 5). В таком случае необходимо **исправить ошибки** и **перезапустить установочный скрипт**.

Пример завершения установки с ошибками

Рис. 5

Примечания:

1. Большинство сообщений об ошибках, отображаемых в терминале в процессе выполнения установочного скрипта, начинаются со слова `failed` или `fatal`. Пример сообщения об ошибке:

```
failed: [127.0.0.1] (item=esensor-sensors) => {"changed": true, "cmd":
"ping -c1 -W10 esensor-sensors", "delta": "0:0ensors", "msg": "non-
zero return code", "rc": 1, "start": "2025-01-28 14:49:13.996667",
"stderr": "", "stderr_lines":data.\nFrom esensor-server
(192.168.1.102) icmp_seq=1 Destination Host Unreachable\n\n---
esensor-sensors ping statisoss, time 0ms", "stdout_lines": ["PING
esensor-sensors (192.168.1.101) 56(84) bytes of data.", "From esensor-
server (nsor-sensors ping statistics ---", "1 packets transmitted, 0
received, +1 errors, 100% packet loss, time 0ms"]}
```

2. Ошибка `ERROR! the playbook: install.yml could not be found` означает, что `install.yml`, один из установочных файлов, не был найден. Вероятно, команда на запуск установочного скрипта была запущена из директории, отличной от распакованной директории `esensor` (см. п. 4) подп. 1) настоящего документа). Необходимо перейти в данную директорию и перезапустить установочный скрипт.

– рекомендуется сохранить каталог `esensor` со всем его содержимым до тех пор, пока не потребуется удалить eSensor (см. п. 3.12 настоящего документа).

3.4.1.5. Учетные записи по умолчанию

Во время установки eSensor будут созданы учетные записи по умолчанию, которые представлены в таблице 3.

Таблица 3 – Учетные записи по умолчанию

Роль	Логин	Пароль
Администратор сервера аутентификации и администратор СУС (используется для входа в веб-интерфейс eSensor)	root	Пароль, заданный в процессе установки на шаге «Шаг 4. Запуск установочного скрипта» (см. п. 3.4.1.4 настоящего документа)
Пользователь ClickHouse для управления данными eSensor		
Пользователь PostgreSQL для управления данными eSensor		
Администратор PostgreSQL	postgres	Без пароля

3.4.2. Подключение к веб-интерфейсу

После установки eSensor будет запущен автоматически.

Инструкция по подключению к веб-интерфейсу eSensor приведена в п. 3.2 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90.

Для входа в веб-интерфейс используется учетная запись «`root`» (администратор сервера аутентификации и администратор СУС).

3.5. Первоначальная настройка eSensor

После установки eSensor необходимо произвести ее первоначальную настройку.

3.5.1. Настройка неразборчивого режима и MTU на сетевых интерфейсах

Чтобы сенсоры могли анализировать пакеты, проходящие через сетевые интерфейсы, которые они «прослушивают», независимо от того, кому адресованы данные пакеты, необходимо перевести данные интерфейсы в неразборчивый режим.

Если в трафике сети организации могут встречаться jumbo-фреймы (пакеты увеличенного размера, до 9000 байт) и сетевая карта, используемая на машине с сенсорами eSensor, может обрабатывать фреймы такого размера, рекомендуется настроить такую возможность. Для этого необходимо установить значение `9000` параметру MTU сетевого интерфейса, используемого сенсором для захвата трафика.

Если сетевой интерфейс на машине настроен через файл `/etc/network/interfaces`, там же можно настроить и автоматический перевод сетевого интерфейса в неразборчивый режим, а также установку значения MTU `9000` при запуске ОС.

Для этого необходимо выполнить следующее:

1) открыть файл /etc/network/interfaces:

```
sudo nano /etc/network/interfaces
```

2) для настройки неразборчивого режима добавить в конец файла строки:

```
up ip link set <Интерфейс> promisc on
down ip link set <Интерфейс> promisc off
```

где `<Интерфейс>` – имя сетевого интерфейса, используемого сенсором для захвата трафика;

Примечание. Если необходимо настроить неразборчивый режим для нескольких интерфейсов, нужно добавить в файл строки, приведенные выше, для каждого из данных интерфейсов.

3) для настройки MTU `9000` добавить в конец файла строки:

```
up ip link set <Интерфейс> mtu 9000
```

где `<Интерфейс>` – имя сетевого интерфейса, используемого сенсором для захвата трафика;

Примечание. Если необходимо настроить неразборчивый режим для нескольких интерфейсов, нужно добавить в файл строку, приведенную выше, для каждого из данных интерфейсов.

4) сохранить изменения в файле;

5) перезагрузить машину, чтобы активировать новые настройки:

```
sudo reboot
```

3.5.2. Настройка обработки и регистрации сессий

Сенсоры разбирают поступающий на них для анализа сетевой трафик по протоколам и регистрируют информацию о сессиях – сетевых взаимодействиях между узлами сети. Данная информация может быть полезна при поиске следов вредоносной активности и расследовании атак, т.к. позволяет составить более полное представление о том, что происходит в сети.

Регистрация сессий осуществляется модулем регистрации сессий сенсора.

По умолчанию регистрация сессий на сенсоре включена.

Примечание. При необходимости регистрацию сессий можно выключить (п. 4.6.2.1 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90).

Если модуль регистрации сессий включен, он будет регистрировать общую информацию о каждой сессии.

Дополнительно можно настроить:

– сохранение копии сетевого трафика (дампов) сессий, которые могут быть полезны для более детального анализа. По умолчанию данная функция выключена;

– извлечение файлов, передаваемых в сессиях. По умолчанию данная функция выключена.

Описание настройки записи и хранения дампов сессий приведено в п. 4.6.2.2.1 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90.

Примечание. В eSensor предусмотрен еще один способ записи сетевого трафика, который позволяет экспортировать дамп трафика, записанный за определенный период времени без разбиения его по сессиям (п. 3.5.3 настоящего документа).

Извлечение файлов, передаваемых в сессиях, осуществляет модуль эвристического анализа сенсора. Чтобы данная функция работала, модуль должен быть включен.

Модуль эвристического анализа сенсора регистрирует метаинформацию об извлекаемых файлах. Кроме того, можно настроить сохранение извлекаемых файлов (п. 4.6.2.2.3 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90). По умолчанию сохранение выключено.

Информация о зарегистрированных сессиях отображается на вкладке «Сессии» раздела «Дашборды» и в разделе «Сессии» (п. 4.3.2 и п. 4.4 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90).

3.5.3. Настройка записи сетевого трафика за период времени

Наряду с механизмом записи дампов сессий в eSensor предусмотрен еще один способ записи сетевого трафика, который позволяет экспортировать дамп трафика за определенный период времени без разбиения его по сессиям. Данную функцию реализует модуль «Захват трафика» сенсора.

Подробное описание настроек модуля «Захват трафика» приведено в п. 4.6.2.2.4 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90.

ВНИМАНИЕ!

Использование обоих способов записи трафика одновременно приведет к увеличению объема записываемых данных примерно в 2 раза, так как каждый из модулей («Регистрация сессий» и «Захват трафика») сохраняет свою копию сетевого трафика. Для экономии дискового пространства рекомендуется использовать **одновременно только один** из способов записи.

3.5.4. Настройка обнаружения атак

Для настройки обнаружения атак на сенсоре с использованием правил необходимо выполнить следующее:

1) загрузить правила на СУС, а именно: добавить группу правил и загрузить в нее правила (п. 3.8 настоящего документа);

2) настроить группы узлов и портов на сенсоре (п. 4.6.2.2.2 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90);

3) далее загрузить правила на сенсор (п. 4.6.5.5.2 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90);

4) просмотреть журнал модуля «Сигнатурный анализ» на вкладке «Логи» (п. 4.6.2.2.2 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90) на наличие сообщений об ошибках. Если есть ошибки, необходимо исправить их;

5) перейти на вкладку «Сенсоры» раздела «Администрирование» (п. 4.6.2 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90). Если модуль сигнатурного анализа сенсора выключен, необходимо включить его;

6) перейти на вкладку «Сенсоры» раздела «Дашборды» (п. 4.3.4 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90). Убедиться, что модуль «Сигнатурный анализ» находится в статусе «Работает». Далее настройку обнаружения атак на сенсоре с использованием правил можно считать законченной.

Информация о зарегистрированных атаках отображается на вкладке «Атаки» раздела «Дашборды» и в разделе «Атаки» (п. 4.3.3 и п. 4.5 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90).

3.5.5. Настройка хранения данных об атаках и сессиях

По умолчанию данные о зарегистрированных атаках и сессиях, за исключением дампов трафика сессий, хранятся 14 дней. При необходимости период хранения можно изменить.

Для настройки хранения данных об атаках и сессиях с помощью терминала машины с СУС необходимо выполнить следующие действия:

1) открыть конфигурационный файл СУС:

```
sudo nano /opt/echelon/ids-backend/config.yaml
```

2) задать необходимые значения параметров в конфигурационном файле. Подробное описание параметров представлены в таблице 4;

Таблица 4 – Параметры хранения данных об атаках и сессиях

Поле	Описание и возможные значения	Пример
clickhouse.flow-expires-in	Период хранения данных о сессиях. Если не задано, очистка производиться не будет	"14d"
clickhouse.attack-expires-in	Период хранения данных об атаках. Если не задано, очистка производиться не будет	"14d"

3) сохранить внесенные изменения в конфигурационном файле;

4) перезапустить службу СУС:

```
sudo systemctl restart ids-backend
```

3.6. Запуск служб

Для запуска необходимой службы с помощью терминала машины, на которой нужно запустить службу (раздел 2 настоящего документа) следует выполнить следующую команду:

```
sudo systemctl start <Имя_службы>
```

3.7. Остановка служб

Для остановки необходимой службы с помощью терминала машины, на которой запущена служба (раздел 2 настоящего документа) следует выполнить следующую команду:

```
sudo systemctl stop <Имя_службы>
```

3.8. Управление правилами

Для проведения сигнатурного анализа сетевого трафика в eSensor используются решающие правила (далее – правила), написанные на специальном языке.

3.8.1. Группы правил

Для работы с правилами используется механизм групп правил.

Группа правил – это объединение множества правил, полученных из одного источника. Правила можно загружать в группу из источника правил, загружать из архива или создавать непосредственно в самой группе. Источником правил может быть удаленный Git-репозиторий, FTP- или SMB-сервер или другая группа правил. Группы правил хранятся на СУС и загружаются на выбранные сенсоры.

Описание возможностей по управлению группами правил приведено в п. 4.6.5 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90.

3.8.2. Формат загрузки правил

eSensor поддерживает решающие правила формата: Suricata 5.

Правила, загружаемые из внешнего источника/архива, должны храниться в данном источнике/архиве в файлах с расширением «.rules», где каждое правило должно находиться в отдельной строке.

Пример содержимого файла с двумя правилами:

```
alert udp any any -> any any (msg:"test udp rule"; sid:1;)
alert tcp any any -> any any (msg:"test tcp rule"; sid:2;)
```

Архив с правилами должен иметь расширение «.zip», «.tar.gz» или «.tgz».

Атаки, обнаруживаемые с помощью правил, можно классифицировать. Для этого присваиваются классы соответствующим правилам.

По умолчанию в eSensor используется классификация, представленная в приложении .

При необходимости можно использовать свою классификацию. Для этого, если правила загружаются в группу правил из архива, необходимо поместить в данный архив вместе с файлами с правилами файл с названием `classification.config`, в котором в формате «Suricata» должны быть определены необходимые классы правил. Если правила загружаются из удаленного источника, файл `classification.config` должен находиться в одной директории/в одном репозитории с файлами с правилами.

Пример содержимого файла `classification.config`:

```
# config classification: <Краткое название класса>,<Полное название класса>,<Уровень опасности атак>
config classification: not-suspicious,Not Suspicious Traffic,3
config classification: unknown,Unknown Traffic,3
config classification: bad-unknown,Potentially Bad Traffic, 2
```

Возможные уровни опасности атак:

– 1 – критический;

– 2 – высокий;

– 3 – средний;

– 4 – низкий.

3.9. Обновление базы данных GeoIP

Для обновления используемой базы данных для определения географического положения узлов по их IP-адресам, необходимо:

1) заменить на машине с СУС и Clickhouse следующие файлы на новые:

– /var/lib/clickhouse/user_files/GeoIP-Country-Blocks-IPv4.csv

– /var/lib/clickhouse/user_files/GeoIP-Country-Blocks-IPv6.csv

– /var/lib/clickhouse/user_files/GeoIP-Country-Locations-ru.csv

2) перезапустить службу ClickHouse:

```
sudo systemctl restart clickhouse-server.service
```

После этого, обновленная база будет использоваться для определения географического положения узлов в новых сессиях и атаках.

3.10. Интеграция с внешними системами

3.10.1. Отправка событий в SIEM-систему

События ИБ, регистрируемые модулем сигнатурного анализа сенсора, можно отправлять в SIEM-систему в формате «CEF».

Отправка событий ИБ сенсора осуществляется его модулем отправки событий.

Для настройки отправки событий с сенсора в SIEM-систему необходимо:

1) перейти на вкладку «Настройки» подменю «Отправка событий» карточки сенсора (п. 4.6.2.2.5 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90);

2) активировать настройку «Использовать продвинутые настройки»;

3) добавить в появившееся поле код для настройки отправки данных в SIEM-систему, не удаляя текущее содержимое поля. Шаблон кода:

```
    siem-sink:
      type: "socket"
      inputs: ["suricata_events_cef"]
      address: "<IP-адрес:Порт_коллектора>"
      mode: "tcp"
      buffer:
        type: "disk"
        max_size: <Объем буфера>
        when_full: "drop_newest"
      healthcheck:
        enabled: false
      encoding:
        codec: "text"
```

Данный код необходимо поместить после строк:

```
sinks:
{{- with .Sinks }}
{{ include "sinks-main.tpl" . | indent 4 }}
{{- end }}
```

Значения параметров, описание которых приведено в таблице 5, необходимо определить самостоятельно в зависимости от желаемой конфигурации системы.

Таблица 5 – Параметры подключения к SIEM-системе

Поле	**Описание и возможные значения**	**Пример**
IP-адрес:Порт_коллектора	IP-адрес и порт syslog-коллектора SIEM-системы	10.0.5.74:49000
Объем буфера	Объем буфера на диске в байтах, в котором будут сохраняться данные для отправки при отсутствии соединения с SIEM-системой. Формат: целое положительное число	1073741824 # 1 Гб

Если необходимо, чтобы при отправке событий в SIEM-систему использовалось защищенное соединение, необходимо дополнительно указать следующие настройки:

```
      tls:
        enabled: true
        ca_file: "<Корневой сертификат>"
        crt_file: "<Сертификат клиента>"
        key_file: "<Закрытый ключ>"
```

Значение данных параметров, описание которых представлено в таблице 6, необходимо определить самостоятельно.

Таблица 6 – Параметры для установления защищенного соединения

Поле	Описание и возможные значения	Пример
Корневой сертификат	Путь к корневому сертификату SIEM-системы. Данный сертификат необходимо предварительно загрузить на машину с сенсором	/opt/echelon/tls/syslog-collector/ca.pem
Сертификат клиента	Путь к сертификату клиента для связи с SIEM-системой. Данный сертификат необходимо предварительно загрузить на машину с сенсором	/opt/echelon/tls/syslog-collector/client.pem
Закрытый ключ	Путь к ключу сертификату клиента для связи с SIEM-системой. Данный ключ необходимо предварительно загрузить на машину с сенсором	/opt/echelon/tls/syslog-collector/client-key.pem

Пример полной настройки:

```
{{- with .DataDir -}}
data_dir: "{{ . }}"
{{- end }}

sinks:
{{- with .Sinks }}
{{ include "sinks-main.tpl" . | indent 4 }}
{{- end }}
    siem-sink:
      type: "socket"
      inputs: ["suricata_events_cef"]
      address: "10.0.5.81:49000"
      mode: "tcp"
      buffer:
        type: "disk"
        max_size: 1073741824
        when_full: "drop_newest"
      healthcheck:
        enabled: true
      encoding:
        codec: "text"
      tls:
```

```
        enabled: true
        ca_file: "/opt/echelon/tls/syslog-collector/ca.pem"
        crt_file: "/opt/echelon/tls/syslog-collector/client.pem"
        key_file: "/opt/echelon/tls/syslog-collector/client-key.pem"

sources:
{{- with .Sources }}
{{ include "sources-main.tpl" . | indent 4 }}
{{- end }}

transforms:
{{- with .Transforms }}
{{ include "transforms-main.tpl" . | indent 4 }}
{{- end }}
```

4) нажать кнопку «Проверить» и убедиться, что на экране появилось сообщение «Успех». Если на экране появилось сообщение «Ошибка», необходимо исправить ошибки и нажать кнопку «Проверить» повторно;

5) нажать кнопку «Сохранить»;

6) перейти на вкладку «Сенсоры» раздела «Дашборды» (п. 4.3.4 документа «NTA eSensor. Руководство пользователя» АПДГ.11100-01 90) и убедиться, что модуль отправки событий сенсора находится в статусе «Работает».

3.11. Изменение пароля пользователя «root»

Для изменения пароля пользователя «root» необходимо с помощью терминала машины, с которой производилась установка eSensor, выполнить следующие действия:

1) выполнить команду:

```
htpasswd -bnBC 10 "" <Новый пароль> | tr -d ':'
```

где `<Новый пароль>` – это новый пароль пользователя «root». В консоли терминала появится строка с хэш-последовательностью;

2) выполнить на машине с сервером аутентификации следующую команду:

```
sudo -u postgres psql -d pauth-preferences -c "UPDATE
preferences.users SET password_hash = '"'<Хэш>'"' WHERE login =
'root'"
```

где `<Хэш>` – хэш-последовательность, полученная на предыдущем шаге.

3) в результате выполнения команды должна вернуться строка: `UPDATE 1`.

Примечание. Если в результате выполнения последней команды также вернется предупреждение вида `could not change directory to "<Директория>": Отказано в доступе`, следует проигнорировать его, т.к. на результат выполнения команды это не влияет.

Пароль пользователя «root» успешно изменен.

3.12. Обновление лицензии

Для обновления лицензии в eSensor необходимо:

1) заменить на машине с СУС текущий файл лицензии /var/opt/echelon/ids-backend/license/production.lic на новый;

2) перезапустить службу СУС:

```
sudo systemctl restart ids-backend.service
```

3.13. Удаление программы

Для удаления программы необходимо с помощью терминала машины, на которой предварительно был установлен eSensor, выполнить следующие действия:

1) перейти в каталог `esensor` с установочными файлами eSensor, который был создан на этапе установки. Если данный каталог был удален, необходимо заново выполнить все действия, указанные в п. 3.4.1.2 настоящего документа, а затем перейти в распакованный каталог;

2) выполнить команду:

```
ansible-playbook -vv -i hosts_esensor.yml --ask-become-pass -e
installer_data=installer_data uninstall.yml
```

При передаче ОС последней команды начнется процесс удаления eSensor.

В процессе удаления потребуется ввести несколько паролей:

– пароль **текущего пользователя**. Сообщение с запросом на ввод пароля выглядит следующим образом:

```
SUDO password:
```

– пароль пользователя «root» Clickhouse;

– пароль пользователя «root» PostgreSQL.

Успешное завершение выполнения последней команды означает, что eSensor удален.

ВНИМАНИЕ!

При удалении eSensor **СУБД PostgreSQL не будет удалена** – будут **удалены только данные eSensor**, хранящиеся в ней.

Примечание. Если СУС и сервер аутентификации eSensor устанавливались на разные машины, то СУБД PostgreSQL есть на каждой из этих машин.

Для **полного удаления СУБД PostgreSQL** необходимо на машине, на которой он установлен, выполнить следующие действия:

1) остановить службы `postgresql.service` и `postgresql@11-main.service`:

```
sudo systemctl stop postgresql*
```

2) проверить, что службы установлены:

```
sudo systemctl status postgresql*
```

3) для базового удаления пакета PostgreSQL выполнить команду:

```
sudo apt remove postgresql*
```

4) для полного удаления пакета и его зависимостей:

```
sudo apt --purge remove postgresql*
```

5) проверить, что СУБД PostgreSQL полностью удалена, для этого выполнить следующую команду:

```
sudo dpkg -l | grep postgres
```

Если **вывод пустой**, это означает, что СУБД PostgreSQL **успешно удалена**.

ВНИМАНИЕ!

После удаления рекомендуется перезагрузить машину для применения всех изменений.

4. ПРОВЕРКА ПРОГРАММЫ

4.1. Проверка работоспособности модулей

Для проверки работоспособности модулей необходимо с помощью терминала машины, на которой функционирует необходимый модуль eSensor, выполнить следующие действия:

1) запустить команду:

`sudo systemctl status <Имя службы>`,

где `<Имя службы>` – наименование службы, реализующей функциональность модуля или имя одной из служб СУБД PostgreSQL (раздел 2 настоящего документа);

2) убедиться, что служба находится в статусе «active (running)».

5. СООБЩЕНИЯ АДМИНИСТРАТОРУ

5.1. Журналирование системных событий

Для просмотра журнала системных событий, происходящих в процессе работы службы, реализующей функционал конкретного модуля eSensor (раздел 2 настоящего документа), необходимо запустить следующую команду:

```
sudo journalctl -u <Имя_службы>
```

ПРИЛОЖЕНИЕ 1.

Настройка доменных имен в файле /etc/hosts

На всех машинах, на которые будет производиться установка модулей eSensor, и на машине, с которой будет производиться установка, необходимо задать в файле `/etc/hosts` IP-адреса и названия машин, на которые необходимо установить модули eSensor.

Для этого необходимо с помощью терминала машины, с которой будет производиться установка, а также терминалов всех машин, на которые необходимо установить модули eSensor, выполнить следующие действия:

1) открыть файл `/etc/hosts`:

```
sudo nano /etc/hosts
```

2) добавить в конец файла `/etc/hosts` IP-адреса и доменные имена машин, на которые необходимо установить модули eSensor. Например, если сенсоры необходимо установить на машину, имеющий IP-адрес `192.168.1.101`, а остальные модули – на машину с IP-адресом `192.168.1.102`, то в конец файла `/etc/hosts` необходимо добавить следующие строки:

```
192.168.1.101           esensor-sensors
192.168.1.102           esensor-server
```

3) сохранить изменения в файле.

Таким образом, машине `192.168.1.101` назначено доменное имя `esensor-sensors`, а машине `192.168.1.102` – `esensor-server`. По данным доменным именам машины будут доступны друг для друга, а также для машины, с которой будет производиться установка eSensor.

ПРИЛОЖЕНИЕ 2.

Классы атак по умолчанию

```
# config classification: <Краткое название класса>,<Полное название класса>,<Уровень опасности атак>


config classification: not-suspicious,Not Suspicious Traffic,3
config classification: unknown,Unknown Traffic,3
config classification: bad-unknown,Potentially Bad Traffic, 2
config classification: attempted-recon,Attempted Information Leak,2
config classification: successful-recon-limited,Information Leak,2
config classification: successful-recon-largescale,Large Scale Information Leak,2
config classification: attempted-dos,Attempted Denial of Service,2
config classification: successful-dos,Denial of Service,2
config classification: attempted-user,Attempted User Privilege Gain,1
config classification: unsuccessful-user,Unsuccessful User Privilege Gain,1
config classification: successful-user,Successful User Privilege Gain,1
config classification: attempted-admin,Attempted Administrator Privilege Gain,1
config classification: successful-admin,Successful Administrator Privilege Gain,1


config classification: rpc-portmap-decode,Decode of an RPC Query,2
config classification: shellcode-detect,Executable code was detected,1
config classification: string-detect,A suspicious string was detected,3
config classification: suspicious-filename-detect,A suspicious filename was detected,2
config classification: suspicious-login,An attempted login using a suspicious username was detected,2
config classification: system-call-detect,A system call was detected,2
config classification: tcp-connection,A TCP connection was detected,4
config classification: trojan-activity,A Network Trojan was detected, 1
```

```
config classification: unusual-client-port-connection,A client was
using an unusual port,2

config classification: network-scan,Detection of a Network Scan,3

config classification: denial-of-service,Detection of a Denial of
Service Attack,2

config classification: non-standard-protocol,Detection of a non-
standard protocol or event,2

config classification: protocol-command-decode,Generic Protocol
Command Decode,3

config classification: web-application-activity,access to a
potentially vulnerable web application,2

config classification: web-application-attack,Web Application Attack,1

config classification: misc-activity,Misc activity,3

config classification: misc-attack,Misc Attack,2

config classification: icmp-event,Generic ICMP event,3

config classification: inappropriate-content,Inappropriate Content was
Detected,1

config classification: policy-violation,Potential Corporate Privacy
Violation,1

config classification: default-login-attempt,Attempt to login by a
default username and password,2


config classification: targeted-activity,Targeted Malicious Activity
was Detected,1

config classification: exploit-kit,Exploit Kit Activity Detected,1

config classification: external-ip-check,Device Retrieving External IP
Address Detected,2

config classification: domain-c2,Domain Observed Used for C2
Detected,1

config classification: pup-activity,Possibly Unwanted Program
Detected,2

config classification: credential-theft,Successful Credential Theft
Detected,1

config classification: social-engineering,Possible Social Engineering
Attempted,2

config classification: coin-mining,Crypto Currency Mining Activity
Detected,2

config classification: command-and-control,Malware Command and Control
Activity Detected,1
```

Лист регистрации изменений

Изм	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					