|  |  |  |
| --- | --- | --- |
|  | Изображение выглядит как зарисовка, рисунок, корона, символ  Автоматически созданное описание |  |
| МИНОБРНАУКИ РОССИИ | | |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** | | |
| **Институт кибербезопасности и цифровых технологий** | | |
|  |  |  |

Кафедра «КБ-4»

**Отчет**

по выполнению практической работы № 5

по дисциплине «Система сбора событий и логов»

Выполнил:

Студент 2 курса

Группа ББМО-02-23

ФИО Брестер А.Н.

Москва, 2025

**Цель работы:**

Изучение практических методов организации процесса Threat Hunting с применением системы мониторинга событий безопасности и логов, развертывание виртуальной инфраструктуры с уязвимостями и внедрение средств защиты для обнаружения угроз.

**Задачи работы:**

1. Создать виртуальную инфраструктуру из нескольких машин для моделирования атак и уязвимостей.
2. Развернуть систему мониторинга событий безопасности с использованием SIEM-решения (Wazuh или DSIEM).
3. Установить IDS/IPS-систему (Snort или Suricata) и настроить сбор логов.
4. Настроить сканер уязвимостей (OpenVAS или Nessus) и провести проверку среды.
5. Организовать процесс Threat Hunting с помощью специализированных инструментов (Zeek, YARA).
6. Создать правила обнаружения угроз и провести тестирование системы.
7. Искусственно сгенерировать угрозы и атакующие действия для проверки работы защиты.
8. Проанализировать собранные данные и выявленные инциденты.
9. Подготовить отчет с описанием выявленных угроз, уязвимостей и предложениями по их устранению.

**ХОД ВЫПОЛНЕНИЯ РАБОТЫ**

1. **Развертывание виртуальной инфраструктуры**

В соответствии с заданием была создана виртуальная сеть с несколькими машинами, имитирующими потенциально уязвимую среду. Для работы использовались:

* 2 сервера на базе **Ubuntu** (один из которых выполнял роль сервера мониторинга, второй — генератора событий);
* 1 виртуальную машину с **Windows 10**;
* 1 виртуальную машину с **Kali Linux** для проведения атак и тестирования защиты. (в последствии данная машина умерла и была исключена, хотя очень хотелось с нее проводить атаки, чтобы буквально эмулировать киберполигон)

Данная архитектура позволила смоделировать работу корпоративной сети с потенциально уязвимыми узлами и организовать сбор событий для анализа угроз.

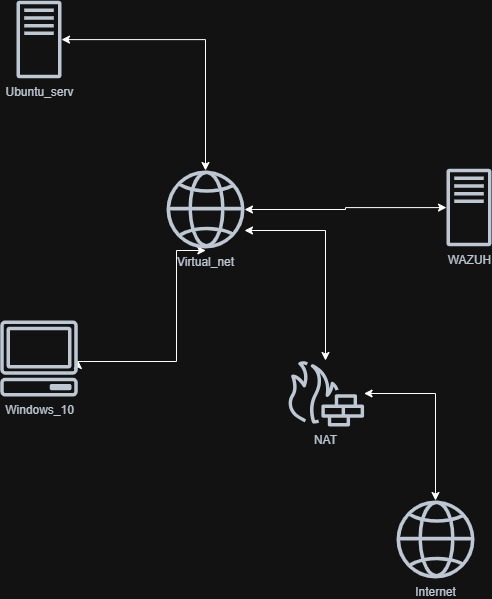


Рисунок 1 - Схема архитектуры киртуальной инфраструктуры

* 1. Проверка функциональности инфраструктуры

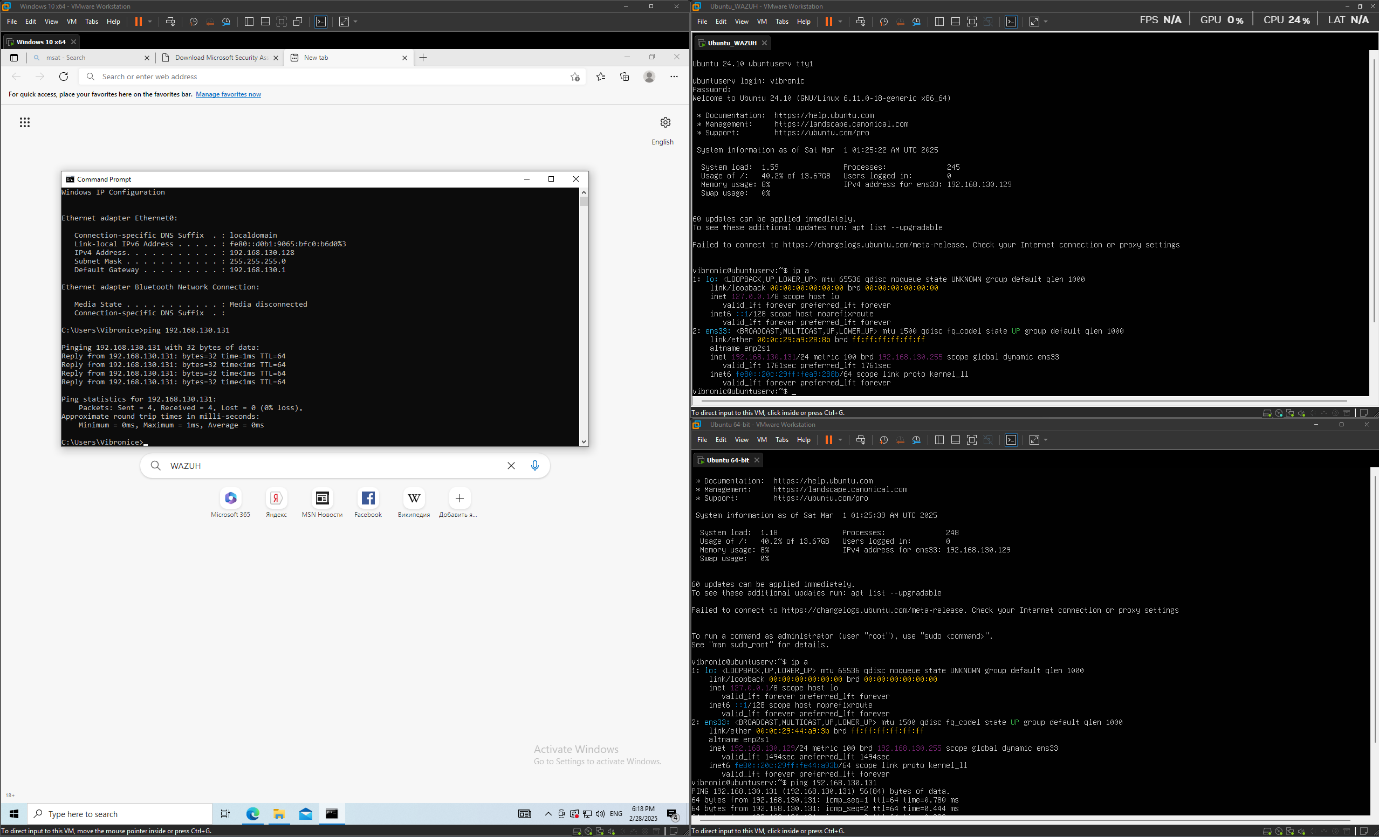


Рисунок 2 - Проверка сетевых взаимодействий и запоминание ip

1. **Устранение проблем с установкой ППО**

При установке компонентов программного обеспечения возникли ошибки, связанные с нехваткой дискового пространства. Анализ логов установки показал необходимость увеличения дискового объема.

Были выполнены следующие действия:

* расширение виртуального диска на 10 ГБ;
* увеличение файловой системы средствами ОС;
* очистка старых компонентов и повторная установка служб.

Ход моих мыслей продемонстрирован ниже (правда отчет формировался постфактум, так как до установки siem не видел смысла что-то показывать.)

* 1. Ход установки ППО

Потом было более **30 часов** попыток установить с разными ошибками и разными методами. В общем найти решение как установить найдено не было, пришлось лезть в логи…

Смотрим в логи скрипта почему не удается установить и видим это…

Загруженное изображение

Загруженное изображение

Пытаемая установить не скриптом, который устанавливает все сразу, а последовательно ручками, на моменте установки indexer, после установки manager у нас вылезает похожая ошибка. Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки. чистим все и получаем не сильно больше (да, я вижу, что я не снес установленный manager и indexer)

Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки. На основании этого идем расширять виртуальный диск ВМ на 10 ГБ. Правда при этом пришлось снести все снапшоты, что обидно. Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Расширили диск в гипервизоре, теперь надо, чтобы ОС поняла, что мы что-то натворили, для этого над расширить файловую систему. Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Далее по новой устанавливаем сервер Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

1. **Настройка SSH-доступа**

Для удобства работы и администрирования серверов был установлен SSH-сервер, настроены сетевые параметры и проброс портов. Это обеспечило возможность подключения к серверам с хостовой машины с использованием PuTTY и аналогичных инструментов.

Подымаем ssh-сервер, чтобы можно было более удобно подключиться к серваку через putty и проще копировать команды/ иметь историю команд и просто удобство, так как всегда работал через putty со своими серваками.

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Залазим в конфигуратор сетей и прокидываем порты, а также прокидываем порты, необходимые нам в будущем (на последний не смотрите, эт от proxmox осталось)

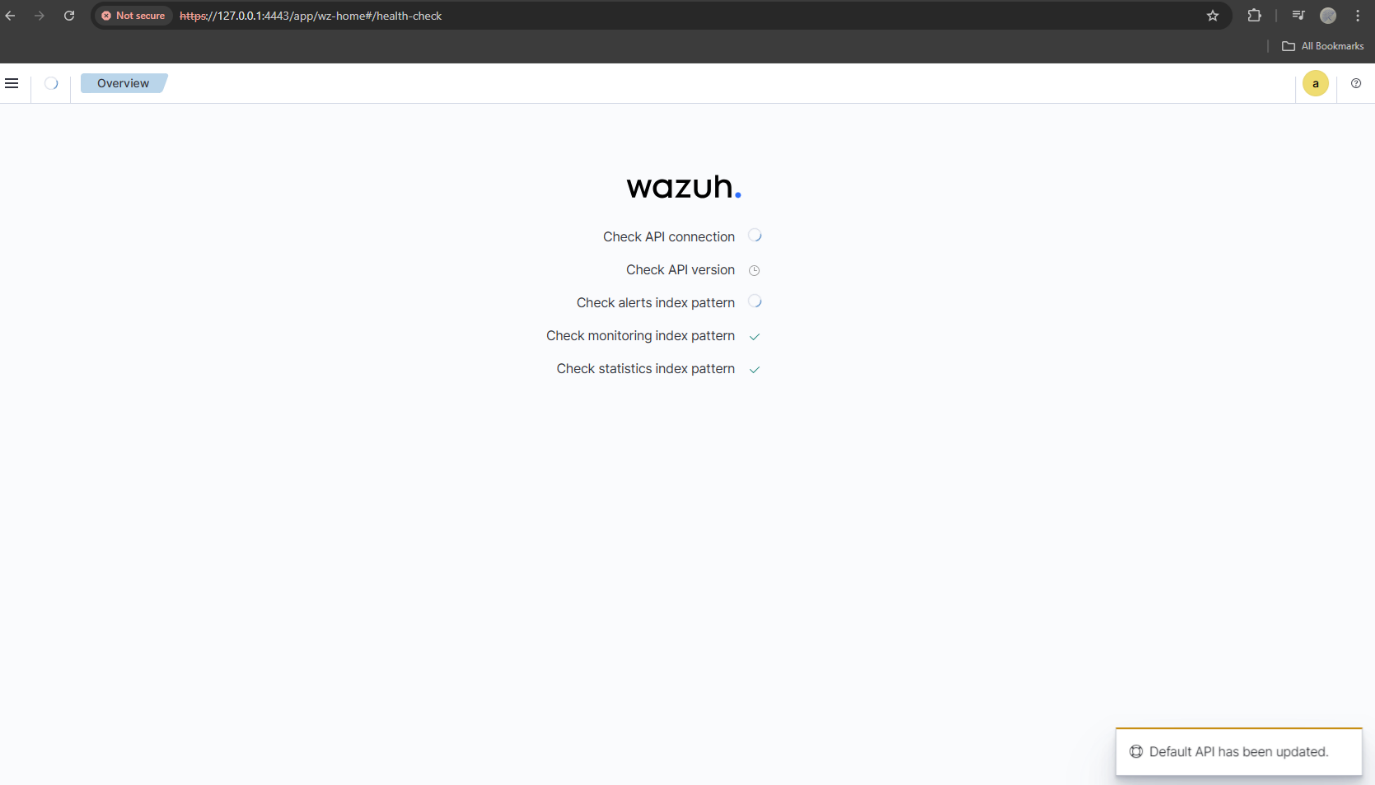
Изображение выглядит как текст, программное обеспечение, число, Значок на компьютере

Контент, сгенерированный ИИ, может содержать ошибки.

Теперь из под хостовой машины можем подключиться по ssh Изображение выглядит как текст, снимок экрана, дисплей, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

И о чудо, получилось!

Проверяем доступность веб-интерфейса из хостовой машины 

Для удобства ставим ssh-server на второй сервер для удобства и прокиним порты в сети.

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки. Изображение выглядит как текст, электроника, снимок экрана, дисплей

Контент, сгенерированный ИИ, может содержать ошибки.

1. **Установка и настройка агента SIEM-системы**

На сервере с Ubuntu был установлен агент **Wazuh**, предназначенный для сбора и отправки логов на сервер SIEM.

Этапы выполнения:

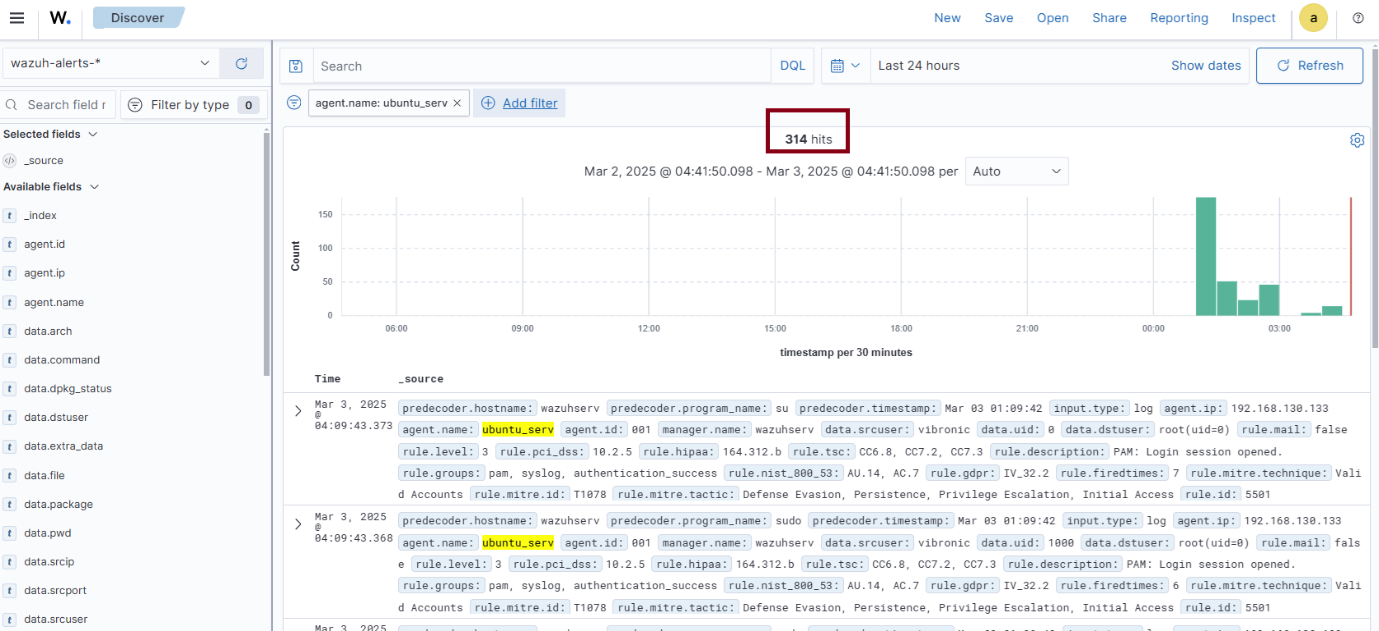
* установка агента Wazuh на сервер с Suricata;
* настройка подключения агента к серверу Wazuh Manager;

Следуя инструкции из Дашборда устанавливаем агента на сервер

Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Смотрим события в дашборде, которые собрал агент.



1. **Установка и настройка IDS/IPS системы Suricata**

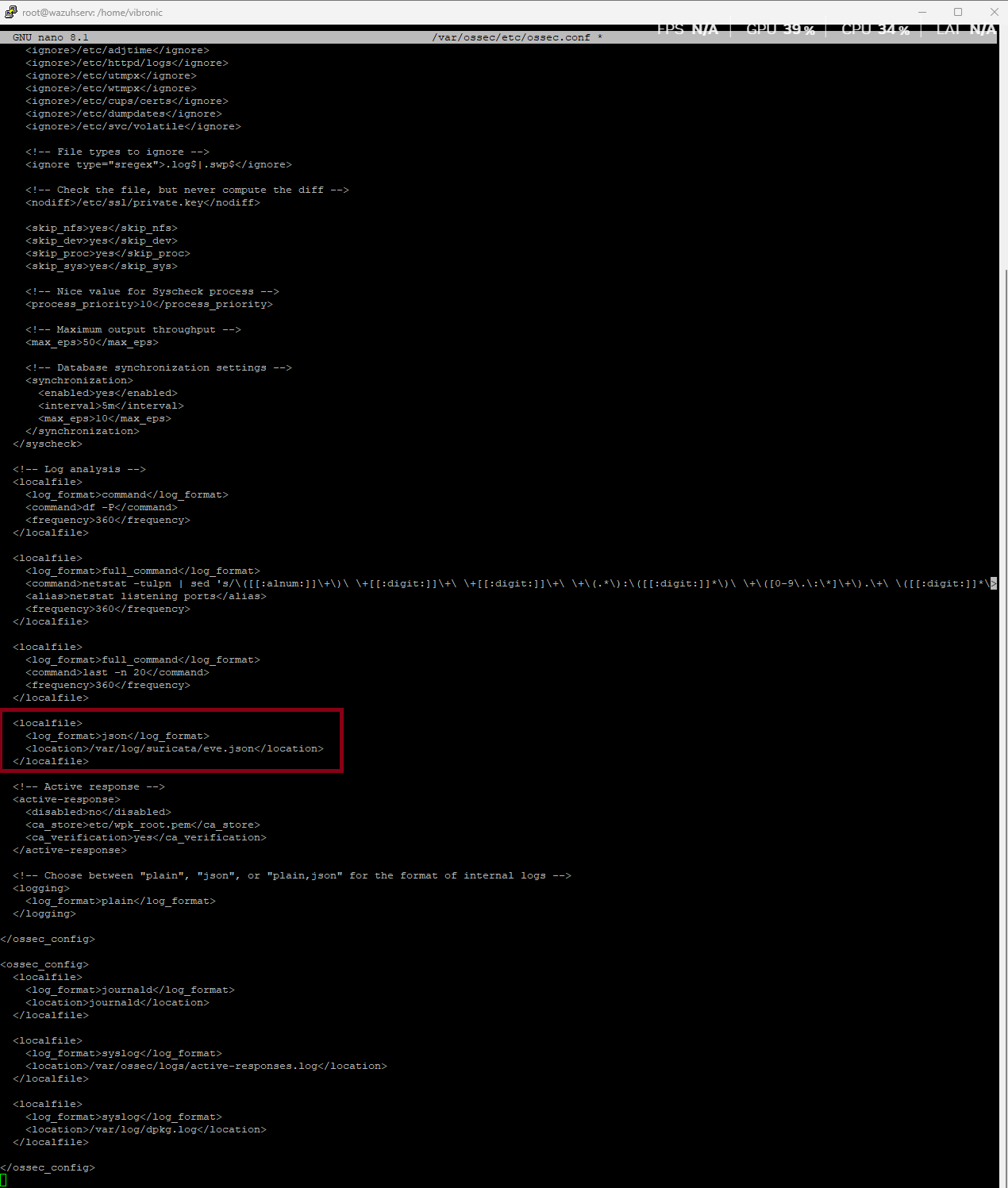
На том же сервере с агентом Wazuh была установлена IDS/IPS-система **Suricata**.

Устанавливаем сурикату, обновляем правила и запускаем ее.

Изображение выглядит как снимок экрана, текст

Контент, сгенерированный ИИ, может содержать ошибки.

Настраиваем агента, чтобы он воровал логи от сурикаты



Далее устанавливаем правила для сурикаты

Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Указываем в конфиге защищаемую или свою сеть для сурикаты, интерфейсы и папку, где хранятся правила.

Изображение выглядит как текст, электроника, снимок экрана, программное обеспечение

Контент, сгенерированный ИИ, может содержать ошибки.

Перезапустили агента и сурикату.

Смотрим в дашборде ивенты, которые пришли от сурикаты и ничго не находим!

Далее пошли несколько часов поиска как так…

1. **Проверка работоспособности системы**

После завершения установки и настройки всех компонентов была проведена проверка их взаимодействия. В ходе тестирования были выявлены следующие проблемы:

* агент **Wazuh** успешно передавал данные на сервер SIEM, однако логи, поступающие от **Suricata**, не интерпретировались корректно;
* события, генерируемые Suricata, поступали в систему в виде необработанных логов, без применения соответствующих декодеров и правил корреляции;
* в интерфейсе Wazuh отсутствовала классификация событий по сигнатурам Suricata, что не позволяло эффективно выявлять и анализировать атаки.

Для начала мучаем агента

Изображение выглядит как текст, снимок экрана, Шрифт, документ

Контент, сгенерированный ИИ, может содержать ошибки.

Проверяем все что можно, заходим во все логи, ищем почему нет упоминания забора файла у сурикаты агентом Вазуха

Изображение выглядит как текст, снимок экрана, черно-белый

Контент, сгенерированный ИИ, может содержать ошибки.

Потом включил режим отладки и о чудо, увидел, как передается лог из сурикаты

Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Теперь подем мучить сервак или менеджер

Перепроверяем подключения и правила корреляции.

Для теста запускаем тест лога, который вводим вручную из сурикаты с другой машины

Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Теперь видим, что у нас не классифицировались логи, как логи полученные с сурикаты, пытаемся найти правила и методику корреляции и видим, **что их нет!**

Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Спасибо интернету, откуда они благополучно были скопированы.

Но Wazuh сломался от таких потрясений… Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Сколько не пробовал декодер для suricata сделать – все безуспешно, а надо еще и работать…

Деревья снапшотов, сколько же раз они меня спасали, правда ветвистоти нет, так как я сносил до точки востановления последний шаг и делал заного.

Изображение выглядит как текст, снимок экрана, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Изображение выглядит как текст, снимок экрана, Шрифт, линия

Контент, сгенерированный ИИ, может содержать ошибки.