**ГЛАВА 3 ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ К СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ**

**3.1 Проект СЗИ для автоматизированной системы (АС)**

Система защиты информации (СЗИ) представляет собой комплекс организационных и технических мер, направленных на обеспечение конфиденциальности, целостности и доступности данных в автоматизированной системе. В рамках проекта для Управления «К» СЗИ включает:

* Программно-аппаратные средства (Wazuh, Suricata, UFW, ClamAV).
* Нормативно-правовые акты (ФЗ-152, ФЗ-432, внутренние регламенты).
* Организационные меры (пропускной режим, видеонаблюдение, контроль доступа).

Основные цели внедрения СЗИ:

* Минимизация рисков утечки, модификации или уничтожения конфиденциальных данных.
* Обеспечение соответствия законодательным требованиям в области информационной безопасности.
* Повышение устойчивости системы к кибератакам.

Основные характеристики СЗИ:

* Многоуровневая защита
  + Контроль доступа (двухфакторная аутентификация, разграничение прав)
  + Шифрование данных при передаче и хранении
  + Регулярное обновление ПО и сигнатур угроз
* Мониторинг и реагирование
  + Системы обнаружения вторжений (IDS/IPS)
  + Анализ журналов событий (SIEM)
* Отказоустойчивость
  + Резервное копирование данных
  + Защита от DDoS-атак

Топология защищенности сети

Для Управления «К» предложена следующая структура:

* Внешний периметр:
* Межсетевой экран (UFW) с фильтрацией трафика
* Система защиты от DDoS-атак (Suricata)
* Внутренняя сеть:
* Изолированные VLAN для работы с конфиденциальными данными
* Серверная зона с контролем доступа и мониторингом («Wazuh»)

Внедрение средств защиты

Таблица 11 – Средства защиты и их предназначение

|  |  |
| --- | --- |
| **Средство защиты** | **Назначение** |
| Wazuh (SIEM) | Контроль целостности ПО, Аудит системы |
| ClamAV | Антивирусная защита, контроль запускаемых процессов |
| UFW | Фильтрация трафика |
| Suricata (IDS) | Мониторинг трафика, выявление аномалий |

Используемое ПО:

1. Suricata — это высокопроизводительная система обнаружения и предотвращения вторжений с открытым исходным кодом, предназначенная для мониторинга сетевого трафика в реальном времени. Её основная цель заключается в обнаружении и блокировке кибератак, анализе угроз и обеспечении безопасности сети. Suricata способна выявлять атаки на основе сигнатур и аномалий, предотвращать вторжения в режиме IPS, а также поддерживает современные протоколы, такие как HTTP, TLS, DNS и SSH. Она легко интегрируется с системами SIEM, включая Wazuh, что позволяет централизованно собирать и анализировать события безопасности.

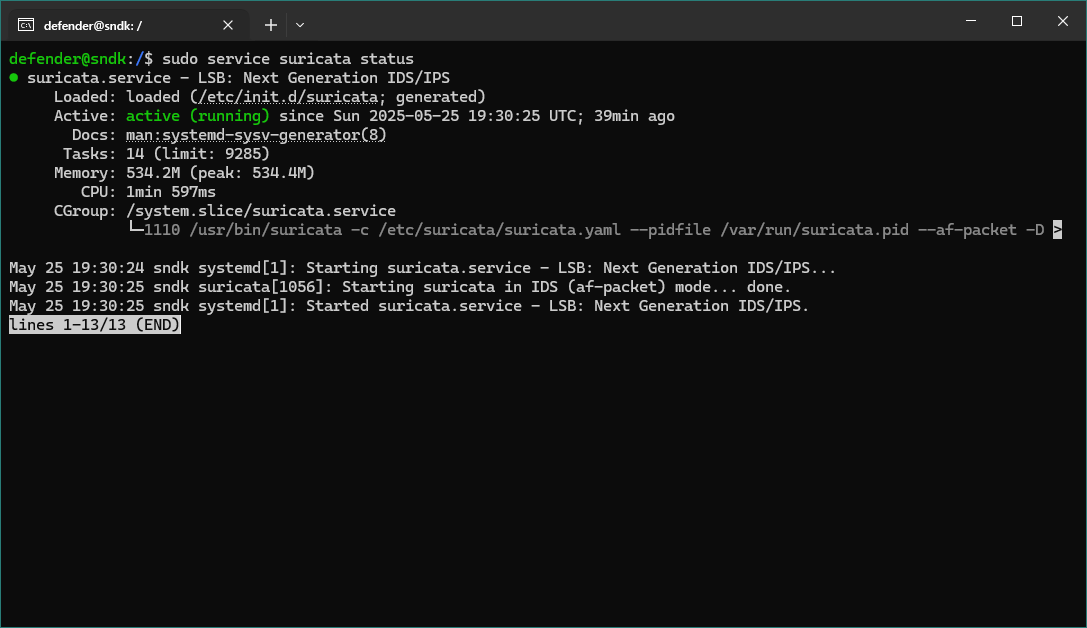
Ключевые преимущества Suricata включают её открытый исходный код, что делает её бесплатной и гибкой в настройке. Благодаря поддержке многопоточности и аппаратного ускорения (например, через Intel Hyperscan), система демонстрирует высокую производительность даже под большой нагрузкой. Suricata отличается масштабируемостью, работая как в небольших сетях, так и в крупных корпоративных средах. Она поддерживает анализ зашифрованного трафика (TLS) и современных протоколов, таких как HTTP/2 и DNS-over-HTTPS, что особенно важно в условиях роста сложных киберугроз.   


Рисунок 3 - Проверка статуса программы Suricata (IDS)

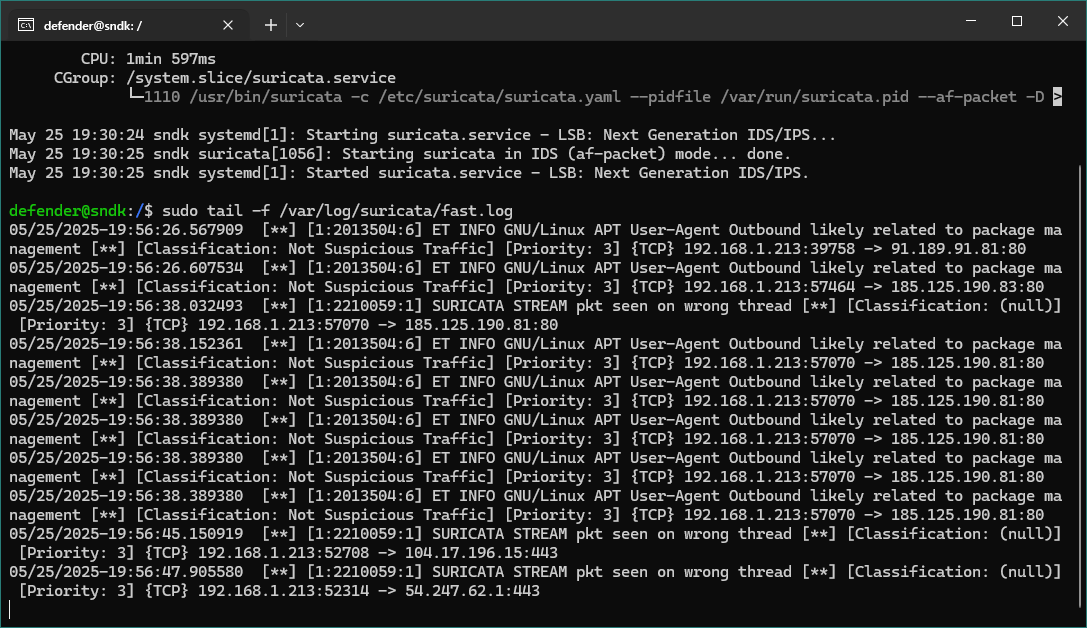
****

Рисунок 4 – Проверка «Alert» в логах программы

2. UFW – Программа Uncomplicated Firewall (UFW) представляет собой фронтенд для управления межсетевым экраном iptables, разработанный для упрощения настройки и администрирования брандмауэра в Linux-системах. Основная цель UFW — предоставить пользователям интуитивно понятный интерфейс для настройки правил фильтрации сетевого трафика без необходимости глубокого изучения сложного синтаксиса iptables.

Ключевые преимущества UFW включают простоту использования благодаря понятному синтаксису команд, позволяющему разрешать или запрещать трафик одной командой (например, `ufw allow 22/tcp`). Программа хорошо интегрирована с системой, входит в стандартные репозитории популярных дистрибутивов Linux и совместима с различными сетевыми сервисами. Несмотря на кажущуюся простоту, UFW поддерживает гибкие настройки, включая сложные правила фильтрации по IP-адресам, портам и протоколам, а также функции NAT и перенаправления портов. Дополнительными преимуществами являются встроенные механизмы логирования сетевой активности и возможность автоматизации через скрипты. Важной особенностью является политика безопасности по умолчанию, при которой блокируется весь входящий трафик, что соответствует принципу минимальных привилегий и существенно повышает уровень базовой защиты системы.

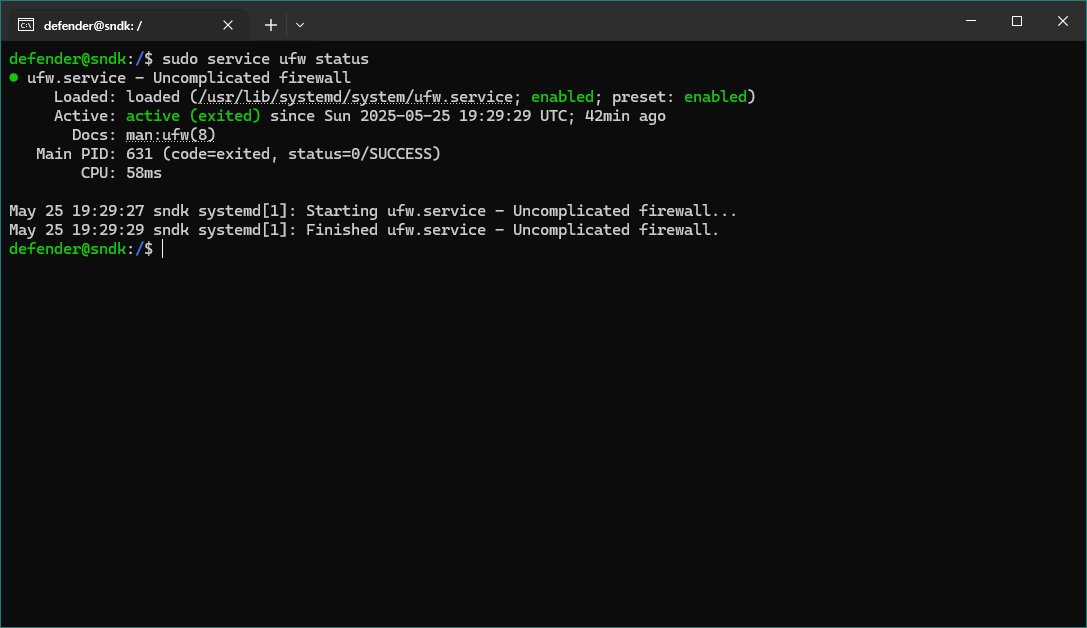


Рисунок 5 – Проверка статуса программы UFW

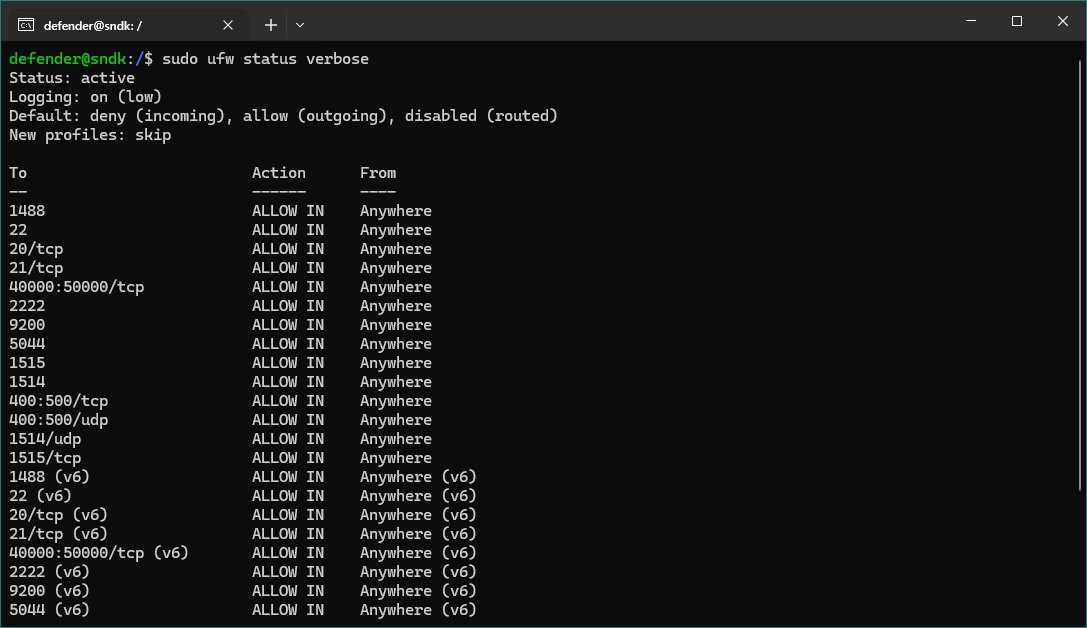


Рисунок 6 – Конфигурация политик UFW

3. Wazuh — это платформа с открытым исходным кодом, предназначенная для обеспечения безопасности информационных систем, включая обнаружение вторжений, мониторинг целостности файлов, анализ уязвимостей и соответствия требованиям, а также реагирование на инциденты. Основная цель Wazuh — предоставить комплексное решение для защиты инфраструктуры организаций, объединяя возможности SIEM (Security Information and Event Management) и XDR (Extended Detection and Response). Платформа работает на основе агентов, которые устанавливаются на конечные устройства, и централизованного сервера управления, что позволяет собирать, анализировать и коррелировать данные о безопасности в режиме реального времени.

Благодаря модульной архитектуре Wazuh поддерживает интеграцию с другими инструментами безопасности, такими как Suricata и ClamAV, что расширяет его функциональность. Платформа обеспечивает детектирование аномалий и угроз на основе сигнатур и поведенческого анализа, а также позволяет автоматизировать реакции на инциденты через предопределённые правила. Кроме того, Wazuh поддерживает соответствие различным стандартам безопасности, включая PCI DSS, GDPR и HIPAA, что упрощает процесс аудита и compliance-отчётности.

Ещё одним важным преимуществом Wazuh является его способность работать в гетерогенных средах, поддерживая Windows, Linux, macOS, а также облачные платформы, такие как AWS, Azure и Google Cloud. Это делает его универсальным решением для гибридных инфраструктур. Механизм мониторинга целостности файлов (FIM) позволяет отслеживать изменения критически важных файлов и конфигураций, а система сканирования уязвимостей помогает выявлять потенциальные точки компрометации до их эксплуатации злоумышленниками. Благодаря активному сообществу и постоянным обновлениям Wazuh остаётся актуальным инструментом в условиях быстро меняющегося ландшафта киберугроз.

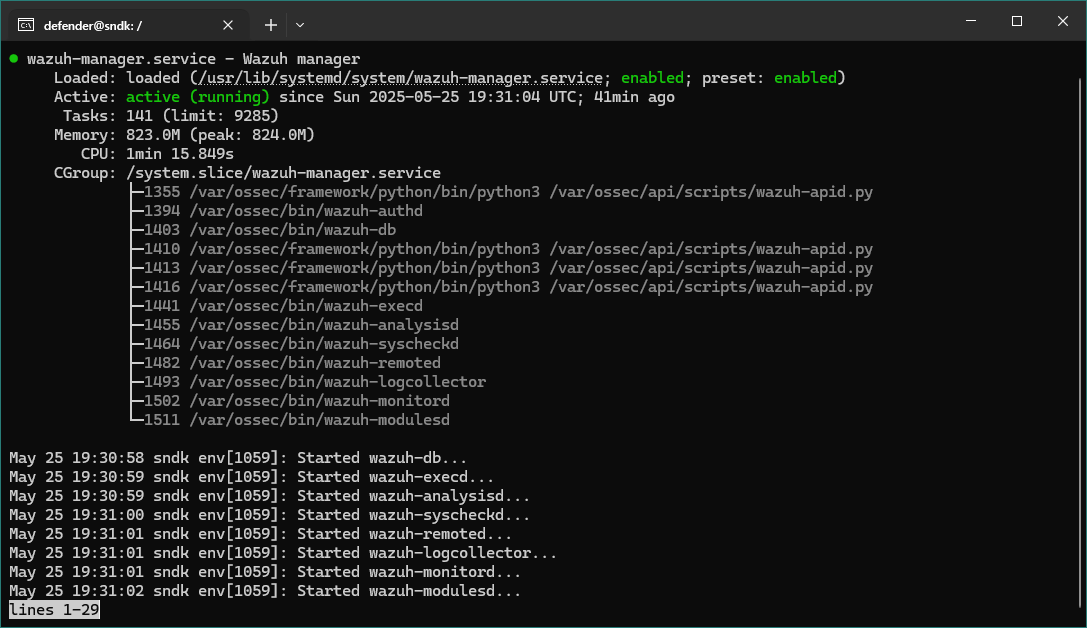


Рисунок 7 - Проверка статуса программы Wazuh

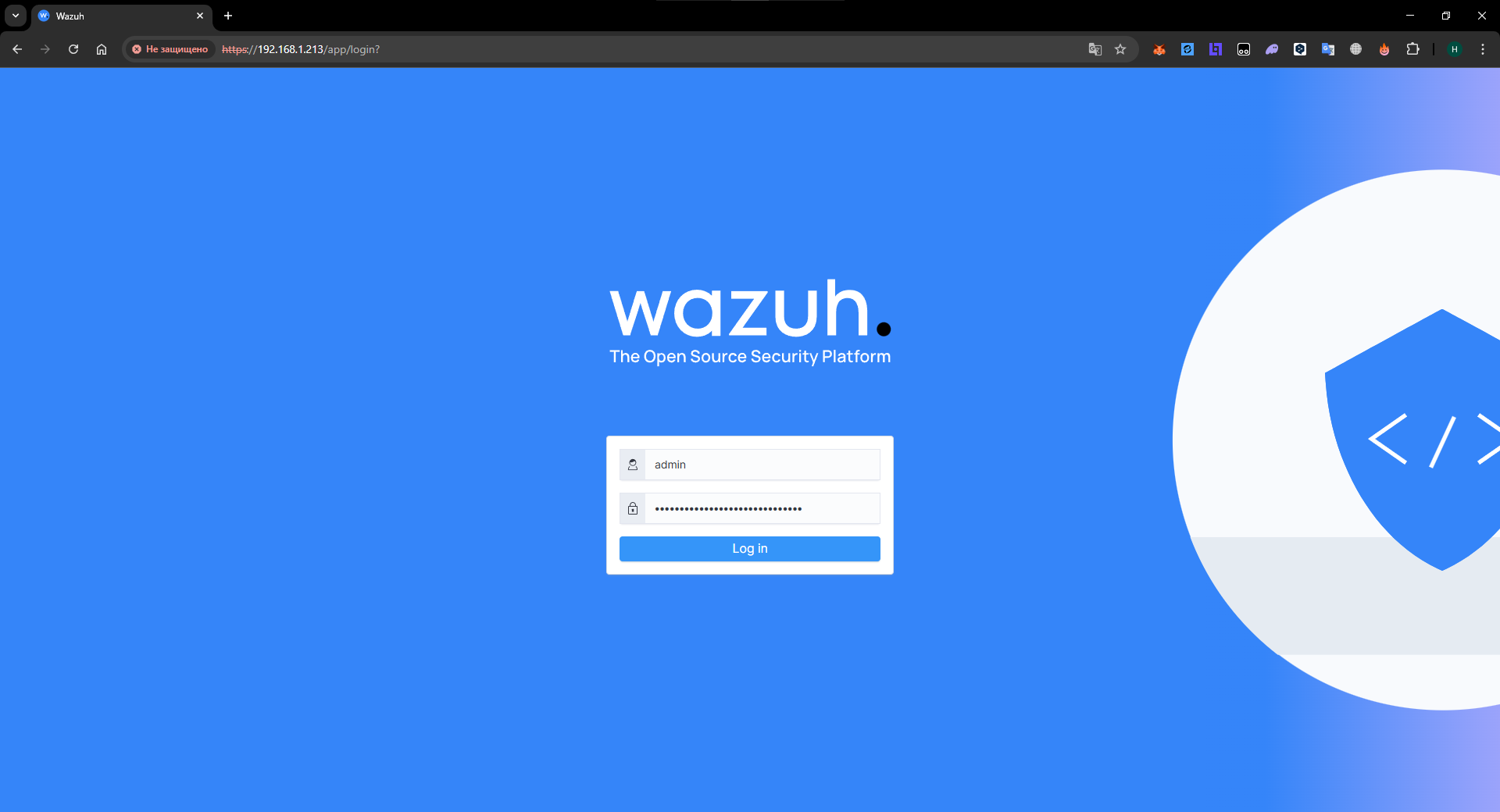
****

Рисунок 8 – Переходим в браузер и попадаем в Dashboard Wazuh

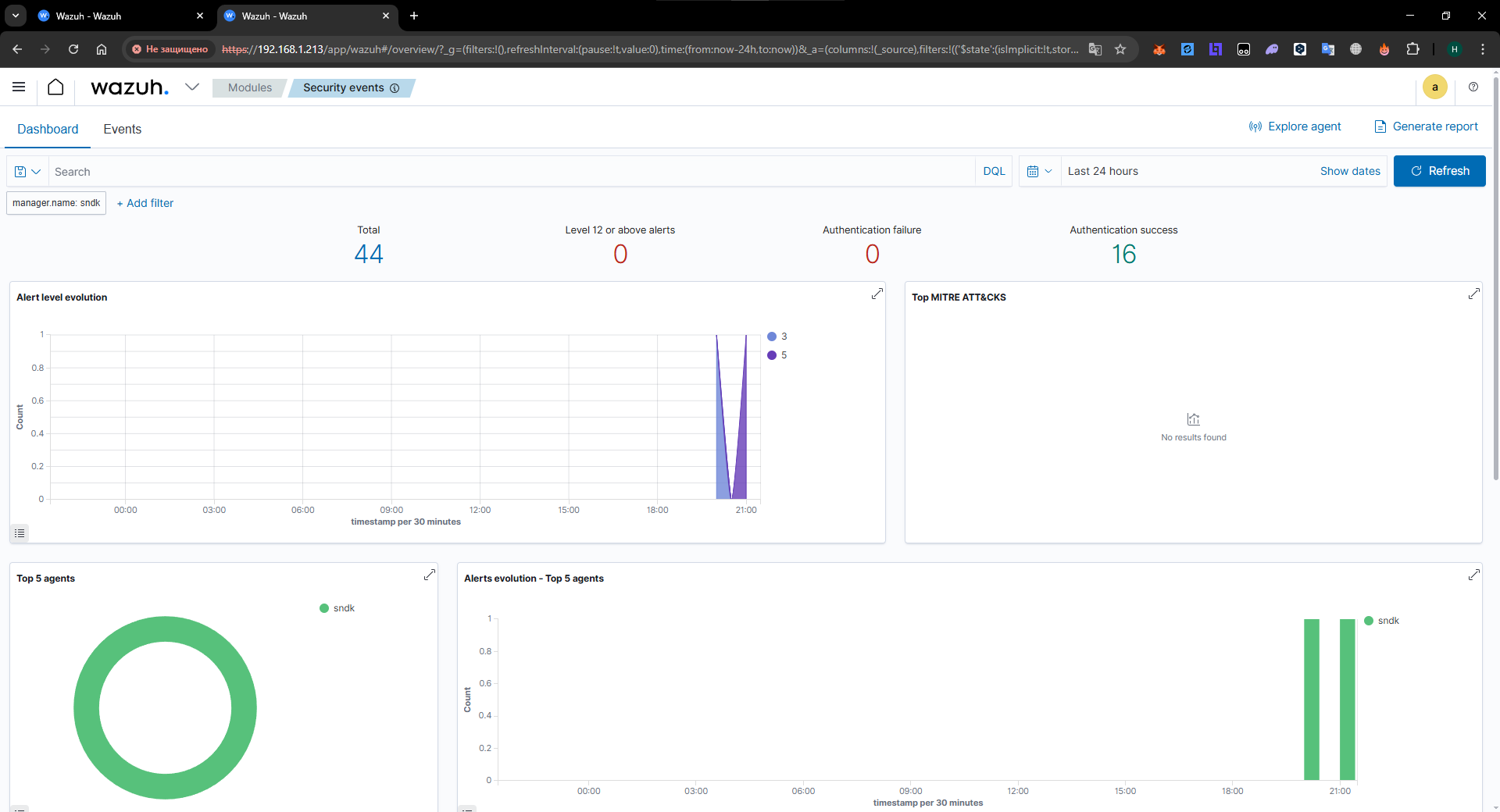


Рисунок 9 – Dashboard программы Wazuh

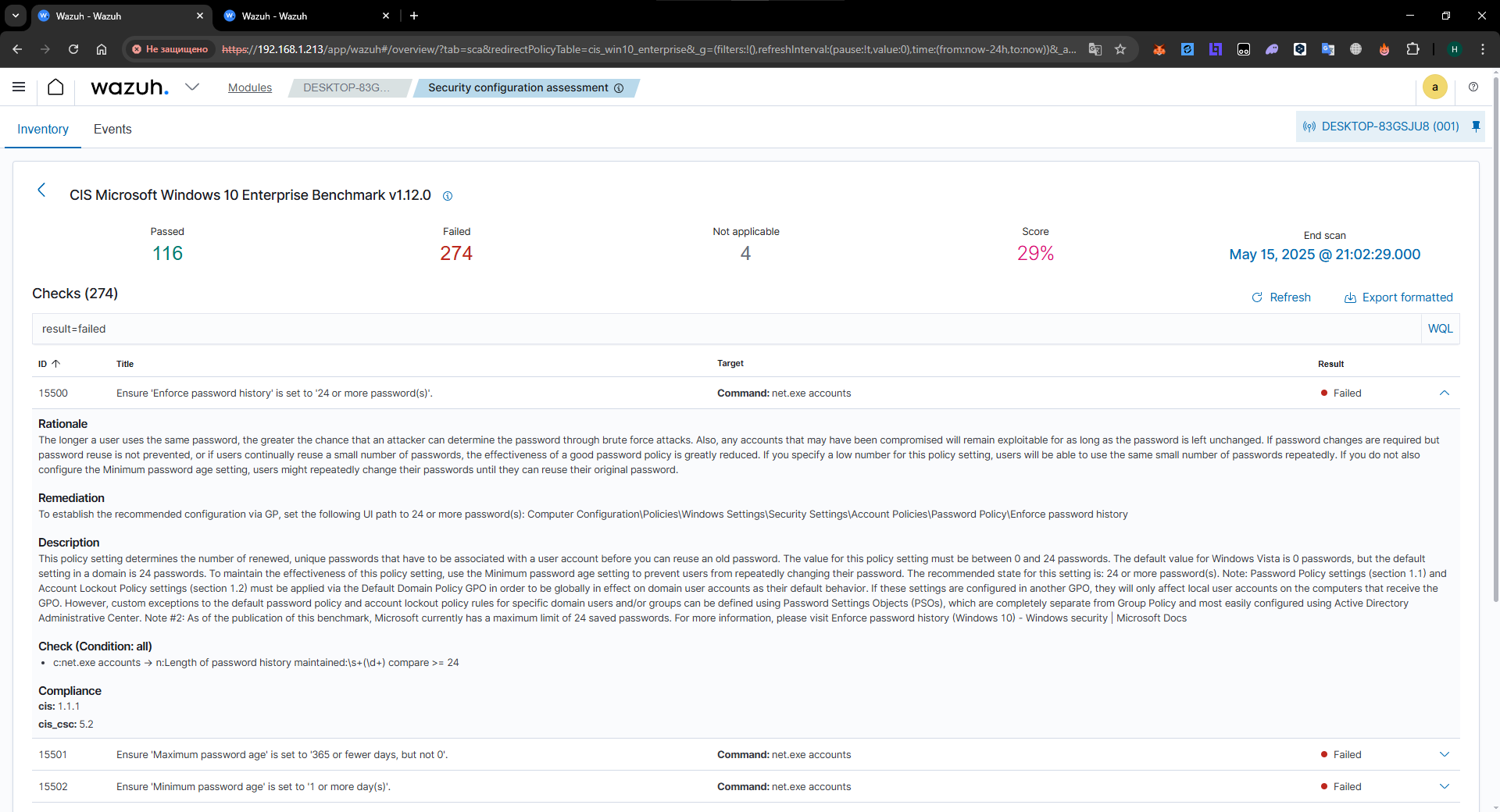


Рисунок 10 – Обнаруженные уязвимости безопасности на «Агенте»

3. ClamAV — это высокопроизводительный антивирусный сканер с открытым исходным кодом, предназначенный для обнаружения и нейтрализации широкого спектра вредоносных программ, включая вирусы, трояны, черви, руткиты и шпионское ПО. Система сочетает в себе несколько методов анализа: сигнатурное сканирование на основе регулярно обновляемых вирусных баз, эвристический анализ для выявления новых и неизвестных угроз, а также детектирование обфусцированного и упакованного вредоносного кода.

Ключевым преимуществом ClamAV является его кроссплатформенность — антивирус работает на Linux, Windows, macOS и различных Unix-системах, что делает его универсальным решением для защиты разнородной ИТ-инфраструктуры. Благодаря модульной архитектуре, ClamAV легко интегрируется с платформами SIEM для централизованного мониторинга угроз. Для крупных организаций особенно ценна поддержка распределенного сканирования через Clamd — демон, позволяющий проверять файлы на нескольких узлах одновременно.

ClamAV отличается высокой производительностью даже при обработке больших объемов данных, что достигается за счет оптимизированных алгоритмов сканирования и поддержки многопоточности. Система также включает дополнительные защитные механизмы, такие как анализ файлов в карантинной зоне (sandbox) и проверка цифровых подписей. Благодаря этим особенностям ClamAV остается одним из наиболее востребованных антивирусных решений для организаций, ищущих надежную, гибкую и экономически эффективную защиту от киберугроз.

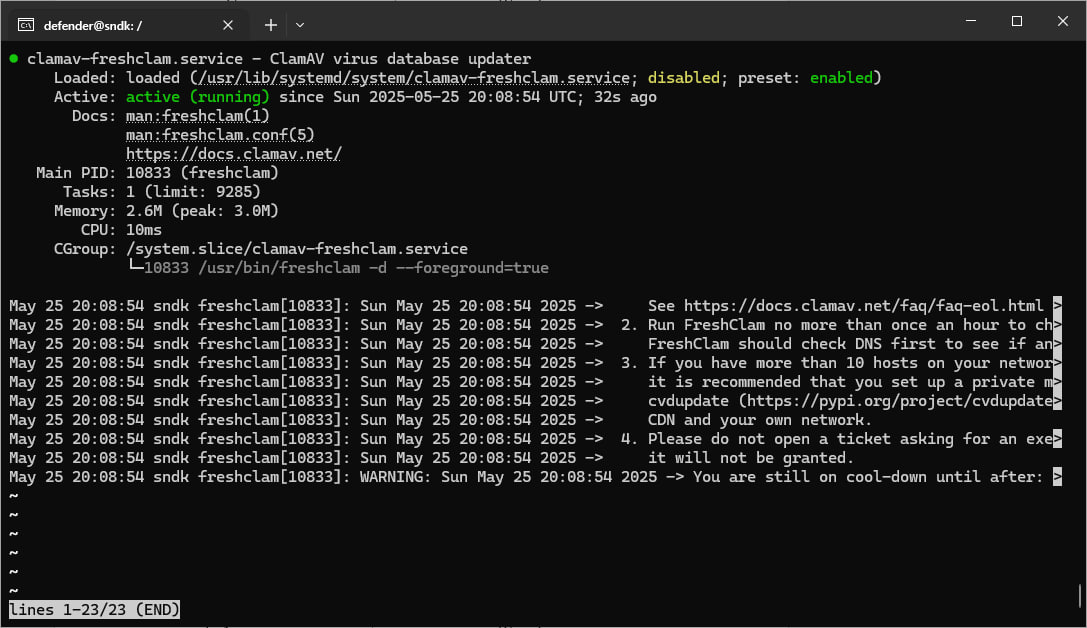


Рисунок 11 – Запустили ClamAV на активное сканирование