

Архипов Алексей Витальевич

Магистрант

Направление: Информатика и вычислительная техника

Магистерская программа: Информационные системы

**Разработка системы сбора и мониторинга данных с удаленных
информационных ресурсов организации на базе Wazuh**

Аннотация. В статье рассматривается процесс разработки и внедрения системы централизованного сбора и мониторинга событий безопасности на основе платформы с открытым исходным кодом Wazuh. Анализируется архитектура решения, приводятся практические сценарии использования для инвентаризации ИТ-активов, управления уязвимостями и обнаружения атак. Показано, что предложенная система позволяет повысить уровень защищенности распределенной инфраструктуры организации.

Ключевые слова: Wazuh, мониторинг информационной безопасности, SIEM, управление уязвимостями, обнаружение вторжений, сбор логов, магистерская диссертация.

Современный ландшафт киберугроз характеризуется непрерывным ростом числа атак, их усложнением и увеличением скорости распространения. Согласно данным статистики, количество инцидентов информационной безопасности в корпоративном секторе ежегодно увеличивается на 15-20%, при этом среднее время обнаружения взлома составляет более 200 дней. Такая ситуация требует от организаций внедрения эффективных систем мониторинга и анализа событий безопасности, способных оперативно выявлять аномалии и предотвращать развитие атак [2].

Вместе с тем, на практике многие компании сталкиваются с серьезными проблемами при построении таких систем. Даже при наличии передовых средств защиты, в организациях нередко отсутствует целостная картина состояния

ИТ-инфраструктуры: не ведется актуальная инвентаризация активов, не систематизированы процессы управления уязвимостями, а сбор и корреляция событий безопасности носят фрагментарный характер. Это создает предпосылки для успешной реализации атак, которые могли бы быть обнаружены на ранних стадиях при правильно организованном мониторинге [1, с. 45].

Существующие коммерческие решения (например, KUMA, PT SIEM, Splunk, IBM QRadar, ArcSight) обладают широким функционалом, однако их внедрение требует значительных финансовых затрат как на приобретение лицензий, так и на последующее сопровождение [3]. Это делает их недоступными для средних и малых предприятий, а также для образовательных и исследовательских проектов. В связи с этим особую актуальность приобретают платформы с открытым исходным кодом, которые при правильной настройке могут обеспечить сопоставимый уровень защиты при минимальных затратах.

1. Архитектура системы сбора и мониторинга на базе Wazuh

Wazuh представляет собой современную платформу с открытым исходным кодом, объединяющую функции SIEM, обнаружения вторжений (HIDS) и реагирования на инциденты [5]. Архитектура системы строится по принципу «агент-сервер». Агенты устанавливаются на контролируемые узлы (рабочие станции, серверы, облачные VM) и передают данные центральному менеджеру. Менеджер, в свою очередь, анализирует события с помощью декодеров и правил, а затем передает обработанную информацию в сервис индексации (на базе OpenSearch) для долгосрочного хранения и визуализации через веб-интерфейс [6].

Агенты Wazuh представляют собой легковесные программы, устанавливаемые на контролируемые узлы – рабочие станции, серверы, виртуальные машины и контейнеры. Агенты выполняют функции сбора данных на месте, что позволяет минимизировать сетевой трафик и обеспечить работоспособность системы даже при временных сбоях сетевого соединения. В случае потери связи с центральным сервером, агенты сохраняют собранные события в локальном буфере и передают их при восстановлении соединения. Агенты поддерживают все основные операционные системы: Windows, Linux (включая различные дистрибутивы), macOS, а также могут

быть установлены на устройства IoT и в Docker-контейнерах.

Менеджер (Wazuh Manager) является центральным компонентом системы, который принимает данные от всех агентов и внешних источников. Основные функции менеджера включают:

- анализ поступающих событий с помощью декодеров и правил;
- корреляцию событий для выявления сложных атак;
- формирование оповещений при обнаружении угроз;
- управление конфигурацией агентов;
- взаимодействие с базой данных для хранения конфигурационных параметров.

Сервис индексации, построенный на базе OpenSearch (форк Elasticsearch), обеспечивает хранение, индексацию и быстрый поиск по всем поступающим событиям. Это позволяет администраторам оперативно получать доступ к историческим данным, строить аналитические отчеты и проводить расследования инцидентов. OpenSearch поддерживает распределенное хранение и репликацию данных, что обеспечивает отказоустойчивость системы [4].

Панель управления (Wazuh Dashboard), основанная на OpenSearch Dashboards, предоставляет пользователям удобный веб-интерфейс для визуализации данных, настройки системы и управления оповещениями. Через панель управления администраторы могут просматривать дашборды с ключевыми метриками безопасности, анализировать события в режиме реального времени, управлять правилами и настройками агентов.

Ключевыми источниками данных в системе являются:

- логи операционных систем (Windows, Linux) и прикладного ПО;
- данные мониторинга целостности файлов (FIM);
- результаты сканирования на наличие уязвимостей (Vulnerability Detector);
- события аутентификации и авторизации;
- инвентаризационные данные об оборудовании и программном обеспечении.

2. Сценарии практического применения

Система позволяет решать широкий спектр задач информационной безопасности. Рассмотрим основные варианты использования.

Инвентаризация ИТ-активов и управление уязвимостями. Первым этапом внедрения, как правило, становится полная инвентаризация всех подключенных к сети устройств с помощью агентов Wazuh. Система позволяет получать детальную информацию о версиях ОС, установленных пакетах и сетевых интерфейсах. На основе этих данных модуль Vulnerability Detector, который регулярно сверяет состав ПО с актуальными базами уязвимостей (включая CVE). Это обеспечивает оперативное обнаружение хостов, подверженных известным угрозам, еще до выпуска официальных патчей от вендоров.

Мониторинг критических событий безопасности. С помощью настраиваемых декодеров и правил можно реализовать сценарии защиты службы каталогов Active Directory. Например, создать правила для обнаружения атак DCSync (путем мониторинга EventID 4662) и Kerberoasting (анализ запросов TGS). Аналогичным образом организовать сбор и анализ журналов безопасности для систем управления базами данных (PostgreSQL), что позволяет выявлять несанкционированные изменения структуры таблиц или попытки подбора учетных данных.

Анализ потенциально опасных команд. Для контроля за действиями администраторов и злоумышленников интеграция с журналами PowerShell. Вместо тотального сбора всех событий, в системе используются списки «опасных» команд, что позволяет снизить количество ложных срабатываний и повысить качество оповещений.

3. Расширение функционала

Архитектура системы предусматривает интеграцию с внешними API и инструментами оркестрации. Модуль Wazuh Integrator позволяет подключаться к внешним сервисам для обогащения событий дополнительной информацией или отправки оповещений в системы управления инцидентами. В рамках работы протестирована возможность:

- интеграции с VirusTotal для проверки файлов и хэшей на наличие вредоносного кода;

- отправки оповещений в SOAR-платформы с целью запуска сценариев автоматического реагирования (например, блокировка сетевого порта, изоляция скомпрометированного узла).

Для мониторинга контейнерной инфраструктуры присутствует модуль Docker-listener, который отслеживает такие команды, как docker pull, docker push, docker kill, а также фиксирует создание и удаление контейнеров. Это позволяет контролировать все изменения в среде контейнеризации, выявлять несанкционированные действия и поддерживать безопасность контейнерных приложений.

Полученные результаты показывают, что предлагаемое решение:

1. обеспечивает полную инвентаризацию ИТ-активов и непрерывный мониторинг их состояния с детализацией вплоть до уровня установленных пакетов и версий ПО;
2. позволяет выявлять как типовые атаки (PtH, Kerberoasting, эксплуатация уязвимостей), так и аномальное поведение пользователей с помощью настраиваемых правил корреляции;
3. масштабируется и адаптируется под различные ИТ-ландшафты, включая гетерогенные среды с использованием российских операционных систем Astra Linux и Red OS;
4. обеспечивает автоматическую оценку соответствия настроек требованиям CIS Benchmarks и рекомендации по устранению обнаруженных нарушений;
5. интегрируется с внешними сервисами (VirusTotal, SOAR-платформы и др.) для расширения аналитических возможностей и автоматизации реагирования.

Литература

1. Донской К.А., Левин Л.С., Трушин В.А. Обзор SIEM на российском рынке // Сборник научных трудов Новосибирского государственного технического университета. 2017. № 3(89). С. 124-132.
2. Киселев А.А., Коротких И.В., Шотт В.В. Практика создания Центра мониторинга информационной безопасности // Безопасность цифровых технологий.

2022. № 4 (107). С. 39–51.

3. Головкин Н. Сравнение российских SIEM-систем – 2026, часть I / [Электронный ресурс] / URL: <https://www.anti-malware.ru/compare/SIEM-2026> (дата обращения: 15.08.2026).

4. Сдобникова И. Российский рынок SIEM-систем в 2025 году: тенденции, выбор и прогнозы развития / [Электронный ресурс] / URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Russian-SIEM-market-in-2025-AMLive (дата обращения: 12.09.2026).

5. Wazuh Documentation. Architecture Overview / [Электронный ресурс] / URL: <https://documentation.wazuh.com/current/getting-started/architecture.html> (дата обращения: 15.08.2026).

6. Официальный репозиторий Wazuh на GitHub. Документация по SCA и CIS Benchmarks / [Электронный ресурс] / URL: <https://github.com/wazuh/wazuh> (дата обращения: 15.08.2026).