УДК 004.056

РАЗРАБОТКА СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SIEM-СИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ ПЛАТФОРМЫ WAZUH

Чу В. Д.[1], Чан Б. Л.[1], Доан Т. Х. Т.[1]
Научный руководитель - канд. техн. наук, доцент Канжелев Ю. А.[1]
[1]Университет ИТМО
chloemamxanhbenho@gmail.com

Введение

Современная ИТ-инфраструктура даже небольших организаций включает множество разнородных источников событий: рабочие станции и серверы, сетевые устройства, веб-сервисы. На фоне роста атак (перебор паролей, эксплуатация веб-уязвимостей, запуск несанкционированных процессов, внедрение вредоносных файлов и попытки скрытой активности) возрастает потребность в централизованном мониторинге и оперативном реагировании. Целью работы является разработка и практическая реализация лабораторного SIEM-стенда на базе платформы Wazuh, обеспечивающего сбор и корреляцию событий безопасности, выявление типовых атак и частичную автоматизацию реагирования за счёт интеграций.

Основная часть

В процессе исследования проведен аналитический обзор современной литературы по использованию SIEM-систем - рассматриваются назначение и ключевые функции SIEM (сбор, нормализация, корреляция и анализ событий ИБ), анализируются типовые источники телеметрии и проблемы внедрения. Выполнен обзор популярных SIEM/стеков и проведено обоснование выбора Wazuh как платформы для стенда, с кратким описанием её архитектуры и возможностей (агенты, анализ логов, FIM, обнаружение уязвимостей, интеграции).

В дальнейшем проведено развертывание и настройка SIEM-системы на базе Wazuh – описывается создание стенда VirtualBox с сегментацией WAN/LAN/DMZ, настройка pfSense+Suricata и NAT/Port Forward, установка Wazuh Server/Dashboard и агентов на Windows/Ubuntu/Debian-DVWA, включение FIM и Vulnerability Detection (CVE), а также интеграции Telegram, VirusTotal, DFIR-IRIS.

В заключительной части выполнена экспериментальная оценка и анализ результатов - проводится проверка детектирования на сценариях brute-force SSH, SQLi (DVWA), сканирование/попытки выявления уязвимостей, несанкционированные процессы и подозрительные файлы; анализируются полнота/качество алертов, корреляция сетевых и хостовых событий. Представлены материалы эффективности автоматизации уведомлений и оформления инцидентов, а также представлены выводы и направления развития.

Выводы

В ходе работы разработан и развернут лабораторный SIEM-стенд для малого предприятия на базе платформы Wazuh в среде VirtualBox с сегментацией WAN/LAN/DMZ. На стенде выполнена настройка централизованного сбора и корреляции событий безопасности как с конечных узлов (Windows, Ubuntu, Debian-DVWA), так и с периметра (pfSense + Suricata), включая контроль целостности

(FIM) и обнаружение уязвимостей (CVE). Проведённые сценарии атак (SSH brute-force, SQLi, запуск подозрительных процессов и файлов, сканирование) подтвердили работоспособность детектирования и удобство анализа результатов в Wazuh Dashboard. Интеграции с Telegram, VirusTotal, DFIR-IRIS повысили оперативность обработки алертов и упростили регистрацию и сопровождение инцидентов.

Литература

1. Wazuh. What is SIEM [Электронный ресурс]. - Режим доступа: https://wazuh.com/resources/what-is/siem/ (Дата обращения 21.02.2026).
2. Elastic. Elastic Stack [Электронный ресурс]. - Режим доступа: https://www.elastic.co/elastic-stack (Дата обращения 21.02.2026).
3. SIEMonster. Solution [Электронный ресурс]. - Режим доступа: https://siemonster.com/solution/ (Дата обращения 21.02.2026).
4. SOC Forum. Материал по Wazuh (PDF) [Электронный ресурс]. - Режим доступа: https://socforum.kz/pdf/3-4.pdf (Дата обращения 21.02.2026).
5. Wazuh Blog. Docker container security monitoring with Wazuh [Электронный ресурс]. - Режим доступа: https://wazuh.com/blog/docker-container-security-monitoring-with-wazuh/ (Дата обращения 21.02.2026).
6. Sandun D. Security Monitoring with Wazuh: Your Gateway to Modern Security [Электронный ресурс]. - Режим доступа: https://www.linkedin.com/pulse/security-monitoring-wazuh-your-gateway-modern-dil shara-sandun-dabgc/ (Дата обращения 21.02.2026).
7. Integrating Wazuh with Suricata (Scribd) [Электронный ресурс]. - Режим доступа: https://www.scribd.com/document/821232103/Integrating-Wazuh-with-Suricata (Дата обращения 21.02.2026).
8. Jesusjimsa. Integrating Telegram with Wazuh [Электронный ресурс]. - Режим доступа: http://medium.com/@jesusjimsa_12801/integrating-telegram-with-wazuh-4d8db9102 5f (Дата обращения 21.02.2026).
9. Raja A. VirusTotal integration Wazuh [Электронный ресурс]. - Режим доступа: http://linkedin.com/pulse/virustotal-integration-wazuh-aravind-raja-g2dyf/ (Дата обращения 21.02.2026).
10. Gupta R. Security Monitoring with Wazuh: A hands-on guide to effective enterprise security using real-life use cases in Wazuh. - Packt Publishing, 2024. 322 p.

Чу Ван Доан (автор) Подпись

Канжелев Ю. А. (научный руководитель) Подпись

Чан Бао Линь (соавтор) Подпись

Доан Тхи Хоай Тхыонг (соавтор) Подпись