КОНФИГУРАЦИЯ SIEM-СИСТЕМЫ WAZUH

Багонский И.А., Жук К.Д., студенты гр. 261401, 261402

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. тех. наук, доцент

Аннотация. В статье поясняется процесс установки SIEM Wazuh с открытым исходным кодом. Рассмотрены ключевые этапы установки системы: развертывание Wazuh Manager на сервере Ubuntu, смена пароля администратора, установка агентов на устройствах с операционной системой Windows и настройка мониторинга журналов. Платформа Wazuh обеспечивает сбор, анализ и визуализацию данных безопасности, что позволяет изучать методы обнаружения угроз, анализа событий и реагирования в реальных условиях. Внедрение SIEM Wazuh способствует формированию практических навыков работы с современными инструментами кибербезопасности.

Ключевые слова. SIEM, Wazuh, Windows 10, Wazuh Manager.

SIEM (Security Information and Event Management) – система, которая позволяет собирать данные о безопасности из компонентов информационной инфраструктуры и представлять эти данные в виде полезной информации через единый интерфейс [1].

SIEM-платформы представляют собой комплексные решения, объединяющие три основных уровня: уровень сбора данных, уровень управления и хранения данных и уровень визуализации и реагирования.

На рынке представлено большое количество SIEM-систем, отличающиеся способами сбора данных, реализацией расположения и конфигурации самой системы. Одними из наиболее известными являются такие SIEM-решения как, MaxPotrol разработанная компанией Positive Technologies, KUMA (Kaspersky Unified Monitoring and Analysis Platform) разработанная компанией Лаборатория Касперского и Wazuh разработанная одноименной компанией Wazuh Inc.

Цель данной работы заключается в обосновании внедрения SIEM Wazuh в учебный процесс на кафедре защиты информации.

Wazuh – платформа безопасности с открытым исходным кодом для обнаружения угроз, мониторинга целостности файлов, анализа логов и соответствия стандартам [2]. SIEM Wazuh включает агенты на оконечных утсройстваъ и центральный сервер, интегрируемый с ELK для визуализации данных.

Процесс установки SIEM Wazuh может быть описан следующими этапами:

1 Установка Wazuh Manager. Для установки Wazuh Manager на сервер Ubuntu версии 24.02.2 [1] была использована команда загрузки и запуска помощника по установке Wazuh Manager wget https://packages.wazuh.com/4.11/wazuh-install.sh && sudo bash ./wazuh-install.sh –a. После завершения установки на выходе появляются учетные данные для доступа к веб-интерфейсу и информационное сообщение, что установка прошла успешно.

2 Смена пароля по умолчанию. Для смены пароля был использован инструмент смены паролей Wazuh. Для его использования, его необходимо загрузить скрипт с помощью команды wget wazuh-passwords-tool.sh https://packages.wazuh.com/4.11/wazuh-passwords-tool.sh. Скрипт запускался с помощью команды bash wazuh-passwords-tool.sh -u admin -p E58#QHCkn@g423i.

3 Установка агентов Wazuh. Агент работает на конечной точке и взаимодействует с

сервером Wazuh, отправляя данные практически в режиме реального времени через зашифрованный и аутентифицированный канал. Для установки агента Wazuh на конечную точку с операционной системой Windows10 был скачан установщик с ресурса [3]. После установки в главном меню программы указывается Manager IP, как показано на рисунке 1.

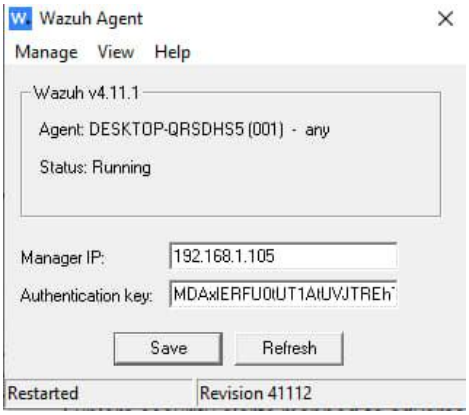

Рисунок 1 – Главное меню программы Wazuh Agent

4 Проверка регистрации агентов на SIEM Wazuh. На рисунке 2 показаны подключенные активные агенты.

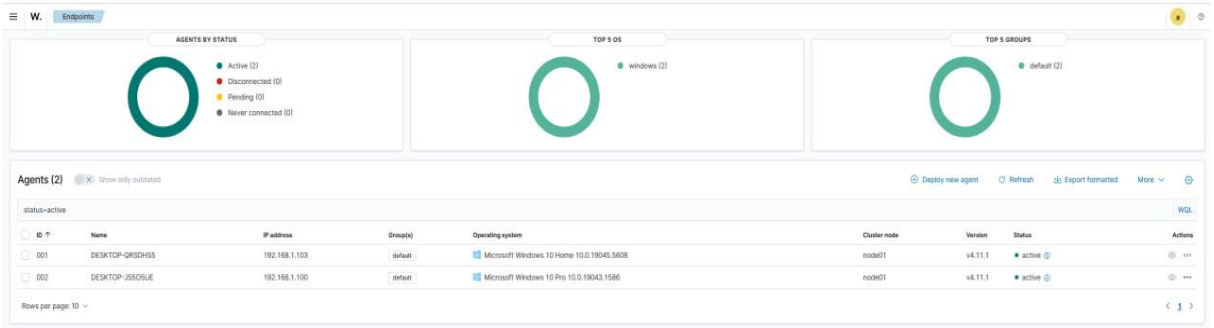

Рисунок 2 – Главная страница веб-интерфейса SIEM Wazuh

5 Настройка конфигурации для мониторинга файлов журнала. Файл ossec.conf является основным файлом конфигурации на сервере Wazuh и агенте Wazuh. Агент Wazuh собирает журналы с контролируемых конечных точек и пересылает эти журналы на сервер Wazuh для анализа. Файл ossec.conf в операционной системе Windows10 находится по пути C:\Program Files (x86)\ossec-agent\ossec.conf. После успешной настройки на SIEM Wazuh возможен просмотр журналов. Информацию об угрозах можно получить при помощи инструмента Theat Hunting. На рисунке 3 показан пример получения общей информации по виду, количеству и значимости угрозы в разделе Dashboard на SIEM Wazuh, которую более подробно можно изучить разделе Events, рисунок 4.

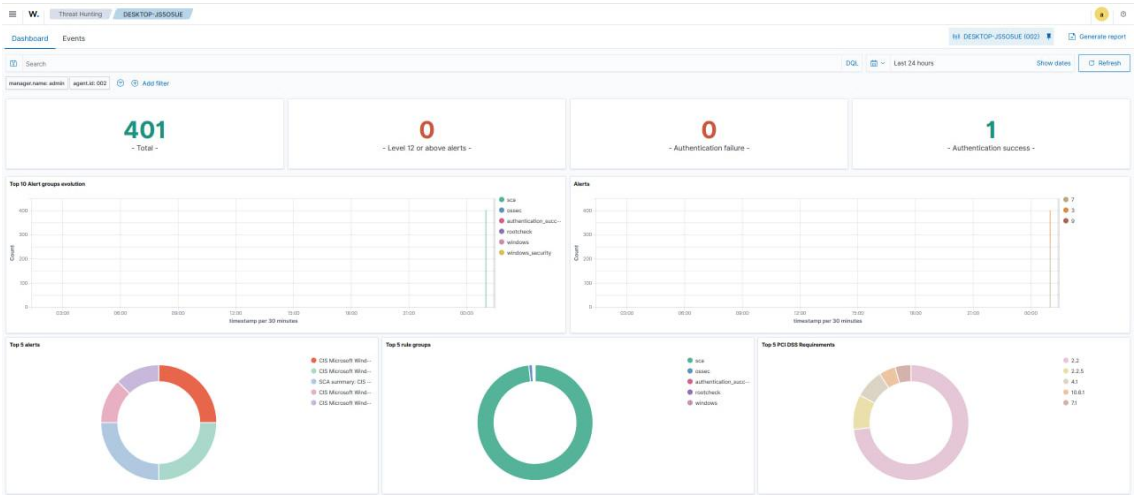

Рисунок 3 – Результат получения общей информации об угрозах на SIEM Wazuh

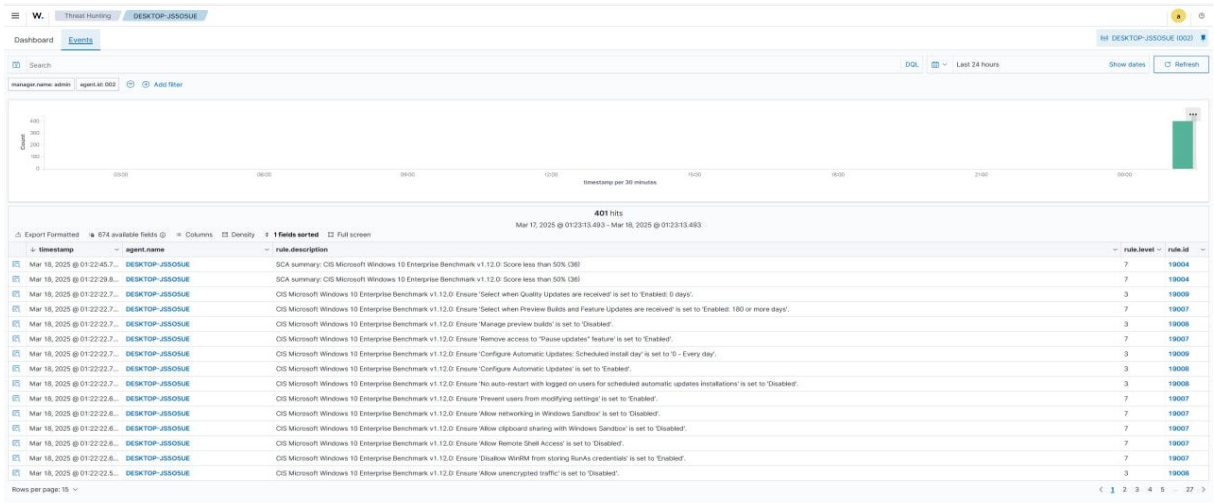

Рисунок 4 – Раздел Events SIEM Wazuh

Таким образом, были продемонстрированы простата и удобство установки и конфигурации SIEM Wazuh, что подтверждает его актуальность внедрения в учебный процесс на кафедре защиты информации для развития следующих навыков у студентов:

1 Определение уязвимостей информационной системы с помощью платформы Wazuh.

2 Работа с системами мониторинга и журналирования событий информационной системы.

3 Устранение выявленных уязвимостей в информационной системе.

Список использованных источников:

1 Computer security resource center [Электронный ресурс]. – Режим доступа: https://csrc.nist.gov/glossary/term/security_information_and_event_management_tool

2 Платформа Wazuh [Электронный ресурс]. – Режим доступа: https://documentation.wazuh.com/

3 Установщик Wazuh Агента [Электронный ресурс]. – https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html

WAZUH SIEM SYSTEM CONFIGURATION

Bahonski I.A., Zhuk K.D.

Belarusian State University of Informatics and Radioelectronics,

Minsk, Republic of Belarus

Belousova E.S. – PhD (Tech.), Ass. Prof. of Department of IP

Annotation. This article explains how to deploy the open-source Wazuh SIEM platform. It covers key installation steps: deploying Wazuh Manager on an Ubuntu server, changing the administrator password, installing agents on Windows devices, and configuring log monitoring. The Wazuh platform provides collection, analysis, and visualization of security data, allowing you to study threat detection, event analysis, and response methods in real-world conditions. Implementing the Wazuh SIEM helps you develop practical skills in working with modern cybersecurity tools.

Keywords. SIEM, Wazuh, open source, threat detection, file integrity monitoring, log analysis, ELK, agents, Ubuntu, Windows 10, Wazuh Manager, installation, ossec.conf configuration, Threat Hunting, Dashboard, Events, web interface, agent registration, security logs, cybersecurity, information infrastructure, data visualization, threat management, systems integration.