# Лабораторна робота №14

## Побудова дашборду Wazuh у Splunk.

**Мета**: Метою роботи є освоєння процесу інтеграції системи моніторингу безпеки Wazuh із платформою аналітики Splunk шляхом перевірки надходження даних та ознайомлення з базовими дашбордами Splunk Wazuh App.

**Інструменти**: гіпервізор VirtualBox, модель комп'ютерної мережі.

## Теоретичні відомості

У попередніх роботах створено стендове середовище у VirtualBox, що складається з чотирьох хостів:

Serv-G-N-1 (Windows Server 2022) – контролер домену з ролями AD DS, DNS і DHCP. Налаштовано Wazuh Agent для локального моніторингу ресурсів.

Serv-G-N-5 (Ubuntu Server 24.04) – сервер на налаштовано Wazuh Agent для локального моніторингу ресурсів.

Serv-G-N-7 (Amazon Linux 2023) – сервер Wazuh Appliance, що містить компоненти Wazuh Server (Manager, API) та Elasticsearch + Kibana (Dashboard)

Serv-G-N-9 (Ubuntu Server 24.04) – сервер Splunk Free — локальний індексатор та аналітична платформа для збору, обробки та візуалізації журналів безпеки. Сервер призначений для прийому логів з операційних систем та сервісів мережі, а також для інтеграції з Wazuh через Wazuh Splunk App.

Мережеве середовище забезпечує взаємодію між вузлами з доменною інфраструктурою для подальшого моніторингу її елементів.

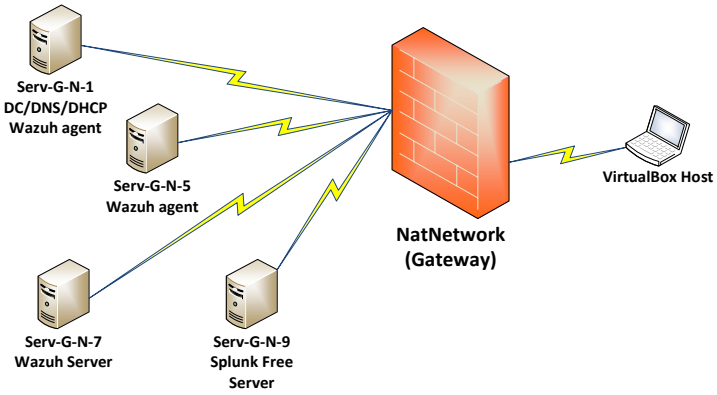



*Рис. 14.1. Топологія мережі*

## Перевірка прийому даних до індексу Wazuh у Splunk

Перевіряємо, чи Splunk бачить індекс wazuh. В меню Settings – Indexes шукаємо індекс wazuh, який має створитись автоматично під час першого успішного отримання подій Logstash – Splunk HEC.

Перевіряємо, що події надходять у Splunk через HEC. Відкриваємо меню Search & Reporting та виконуємо пошук ***index=wazuh | head 20*** (рис. 14.02). Результатом цієї операції мають бути JSON-події — інтеграція працює. Якщо результат порожній, повертаємося до попередніх кроків — дивимось лог pipeline.

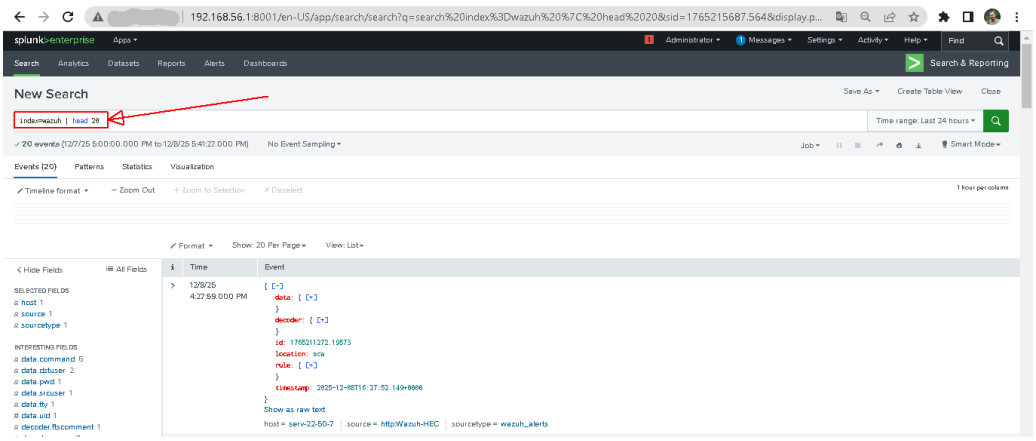



*Рис. 14.02. Меню Search & Reporting. Пошук index=wazuh | head 20*

Якщо індекс не з’явився, його можна створити через встановлення додатку Wazuh для Splunk, який створює індекс автоматично під час інсталяції.

Версія Wazuh App повинна відповідати серверній версії Wazuh, розгорнутій у середовищі лабораторної роботи. Оскільки віртуальний образ wazuh-4.14.0.ova базується на гілці Wazuh 4.14.x, для забезпечення повної сумісності REST-запитів, полів та дашбордів необхідно використовувати Wazuh App з тієї ж основної гілки (4.x). Найближчою сумісною та рекомендованою версією є wazuh_splunk-4.3.11_8.1.10-1.tar.gz

Ця версія забезпечує коректну роботу всіх компонентів інтеграції (агенти, події, вразливості, FIM, MITRE), тоді як новіші релізи (наприклад, 4.5.x) не підтримують Wazuh 4.14 та можуть призвести до помилок у панелях та пошукових запитах.

Завантажуємо Wazuh App (4.3.11) у браузері, локально на фізичний ПК (VirtualBox Host), з якого виконуємо всі дії у WEB UI Wazuh та Splunk.

Сторінка завантаження додатків https://github.com/wazuh/wazuh-splunk/releases.

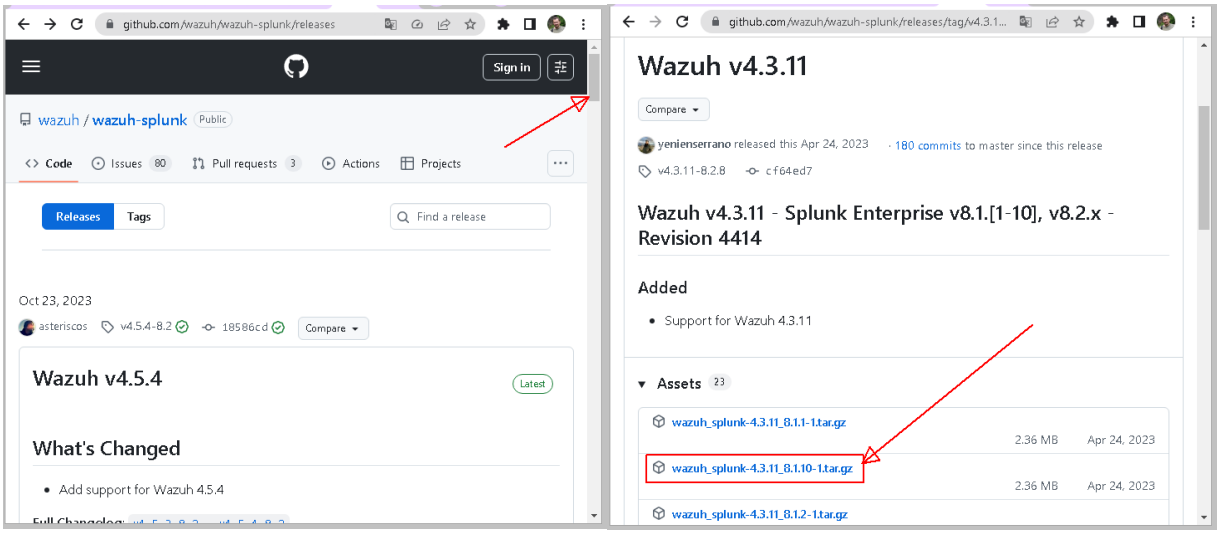
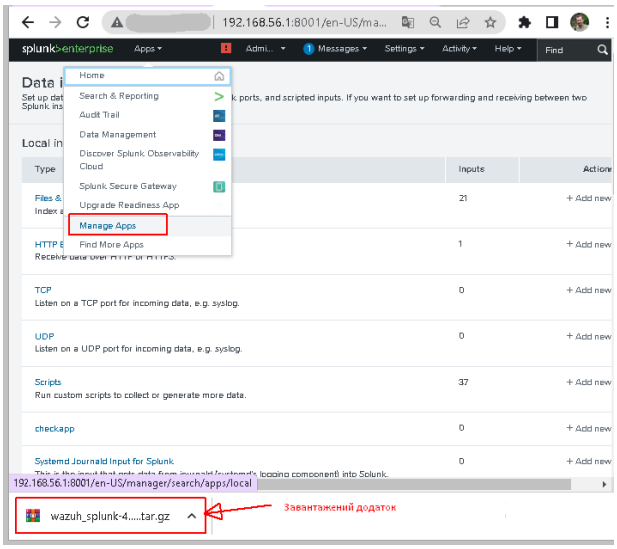
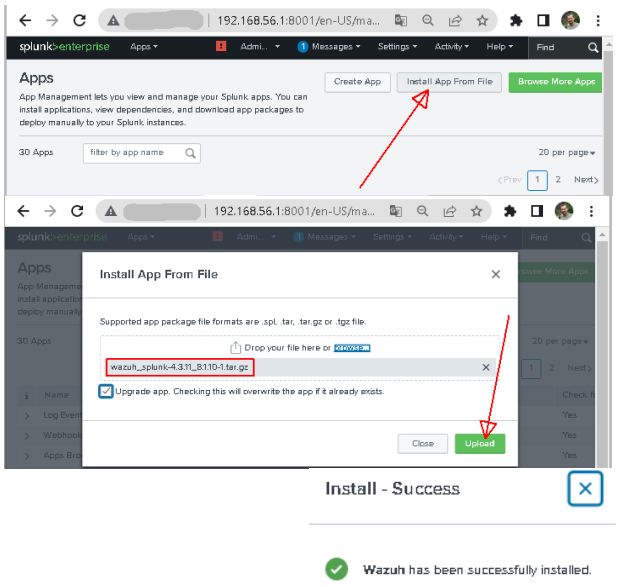



*Рис. 14.3. Завантаження файлу додатку wazuh_splunk-4.3.11_8.1.10-1.tar.gz на VirtualBox Host*

Перемикаємось на сторінку Splunk Web: https://192.168.50.11:8000 та підключаємось як admin. Обираємо Menu – Apps – Manage Apps – Install app from file та обираємо завантажений на фізичний ПК (VirtualBox Host) файл wazuh_splunk-4.3.11_8.1.10-1.tar.gz. Після завершення завантаження додаток автоматично встановлюється. Переглянути доступність додатку та його версію можна набравши у цьому ж меню в рядку пошуку wazuh (рис. 14.4).



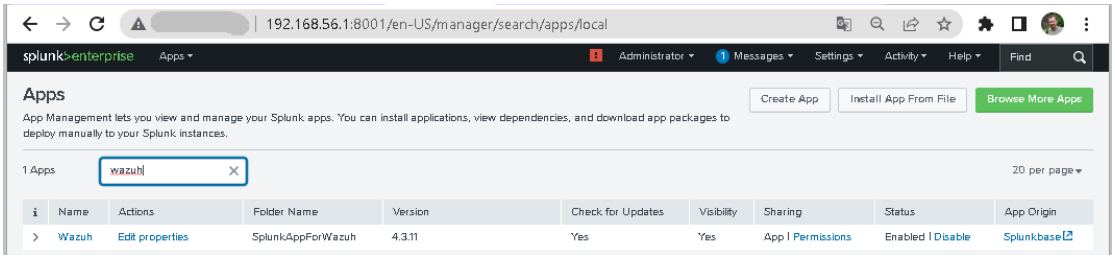



*Рис. 14.4. Встановлення додатку wazuh_splunk-4.3.11_8.1.10-1.tar.gz у Splunk Web*

Після створення індексу Splunk автоматично використовуватиме його для прийому даних. Якщо після встановлення Wazuh App індекс wazuh відсутній, створюємо його вручну. У Splunk Web відкриваємо Settings – Indexes – New Index та у полі Index Name вводимо wazuh. Інші параметри залишаємо за замовчуванням. Натискаємо Save.

## Створення робочого дашборду у Splunk на основі подій Wazuh

Створимо власний базовий дашборд у Splunk Dashboard Studio. У Splunk Web відкриваємо Search & Reporting, обираємо підменю Dashboards та натискаємо кнопку Create New Dashboard (рис. 14.5).

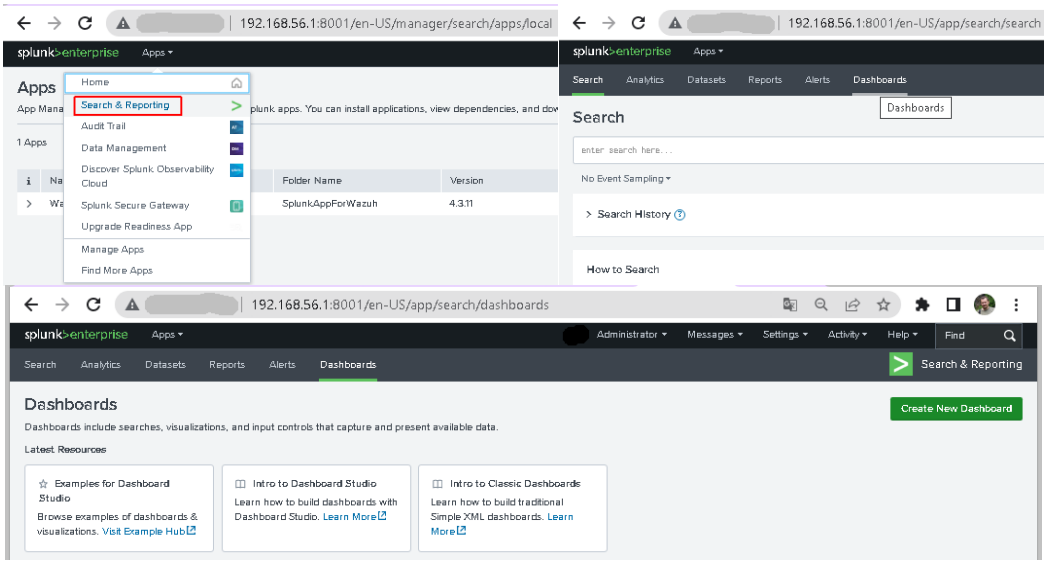



*Рис. 14.5. Меню створення нового Dashboard у Splunk Web*

Даємо назву, наприклад – Wazuh Monitoring Dashboard, обираємо тип Dashboard Studio та Layout – Absolute (найгнучкіший варіант). Відкриється пустий дашборд.

Після створення пустого дашборду переходимо до додавання перших візуалізацій. У новому вікні додаємо перший блок – лічильник усіх подій Wazuh по кнопці Add Visualization - Single Value. У вікні налаштувань доданого елементу додаємо назву та SPL-запит

```
index=wazuh
| stats count as "Total Wazuh Events"
```

Додамо другий елемент дашборду – графік подій по часу ("Events over time"). Add Visualization – Line . SPL-запит для цього елементу:

```
index=wazuh
| timechart span=1m count
```

Створюємо таблицю останніх подій "Recent Alerts". Add Visualization – Table . SPL-запит:

```
index=wazuh
| sort - _time
| head 20
| table _time, rule.id, rule.description, decoder.name, location
```

Додаємо діаграму за рівнем важливості "Alerts by severity". Add Visualization – Bar . SPL-запит:

```
index=wazuh
| stats count by rule.level
| sort - count
```

Зберігаємо створений дашборд. Перегляд його функціоналу доступний у меню Dashboard. Ми отримали повноцінний функціональний міні-Wazuh App на сучасному Dashboard Studio.

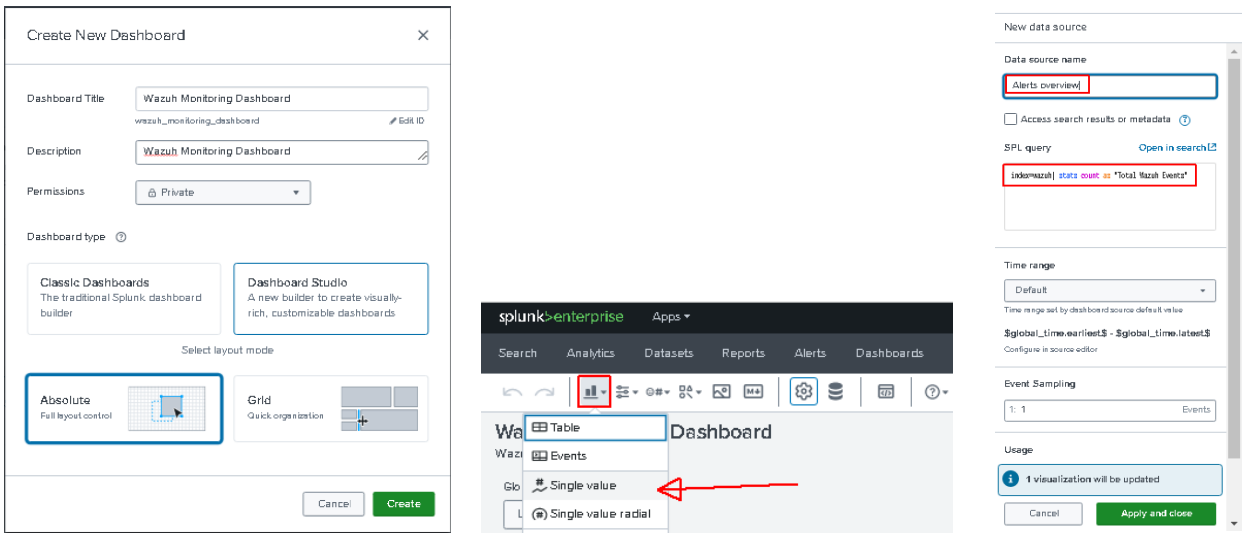



*Рис. 14.6. Кроки створення нового Dashboard у Splunk Dashboard Studio*

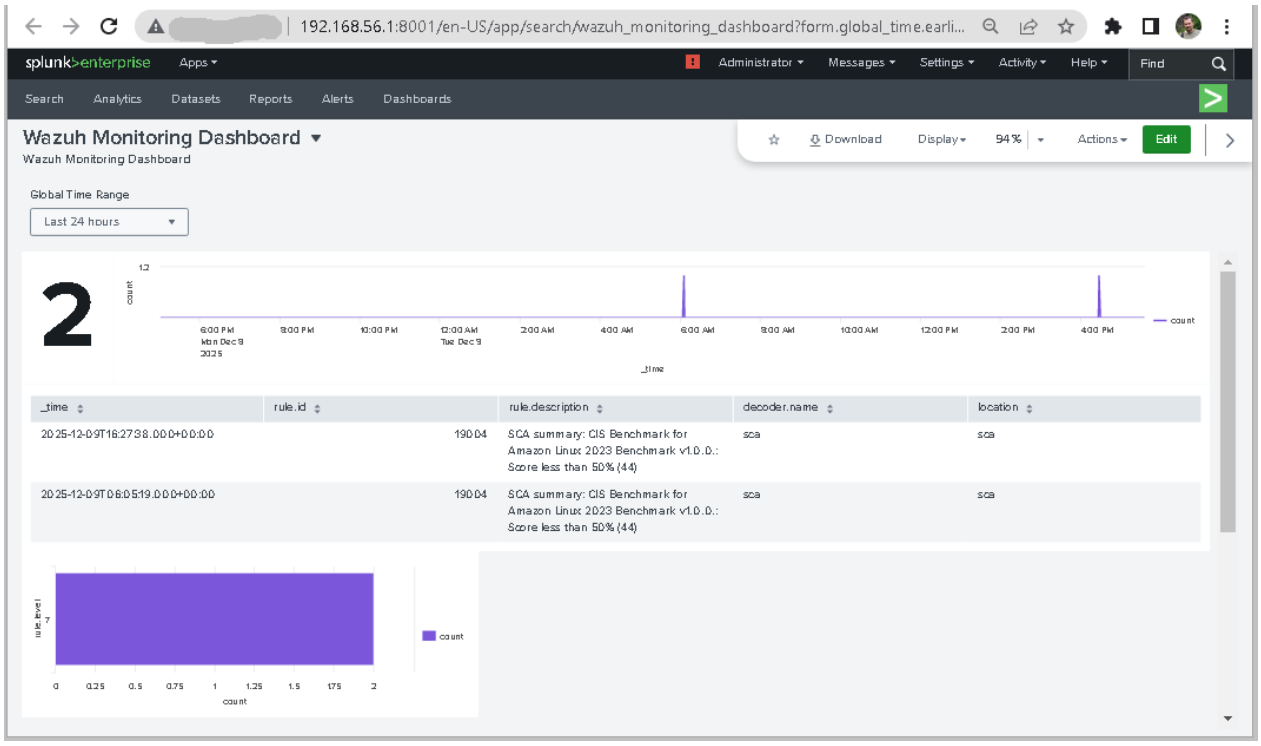



*Рис. 14.7. Перегляд створеного Wazuh Monitoring Dashboard*

## Завдання до лабораторної роботи

1. Перевірте стабільність передачі подій у Logstash та Splunk.
2. Перевірте створення та роботу індексу wazuh у Splunk. У разі відсутності індексу — створіть його та виконайте пошукові запити index=wazuh | head 20.
3. Створити власний дашборд у Splunk Dashboard Studio, додавши лічильник загальної кількості подій, графік подій у часі, таблицю останніх сповіщень та діаграму за рівнями критичності.
4. Перевірте повний шлях обробки подій (Wazuh → Filebeat → Logstash → Splunk HEC → індекс wazuh → дашборд). Зробіть короткі висновки щодо коректності роботи конвейера.
5. Оцініть доцільність використання побудованого конвеєра (Wazuh → Filebeat → Logstash → Splunk HEC) для централізованого збору подій безпеки. Визначте його переваги та недоліки (стабільність, масштабованість, складність адміністрування) і зробіть висновки щодо можливості застосування в реальному середовищі.

## Корисні посилання

- Wazuh. Splunk integration.
https://documentation.wazuh.com/current/integrations-guide/splunk/index.html

- Integrating Wazuh and Splunk
https://www.linkedin.com/pulse/integrating-wazuh-splunk-vaibhav-karayat-p2gnc

- Integrations guide: Elastic, OpenSearch, Splunk, Amazon Security Lake
https://documentation.wazuh.com/current/integrations-guide/index.html

- wazuh / wazuh-splunk
https://github.com/wazuh/wazuh-splunk

- IBM Storage Defender. Splunk® Configuration Guide
https://www.ibm.com/docs/en/SSDR5G6_prod/pdf/splunk_config_guide.pdf