ЛАБОРАТОРНА РОБОТА №5
СТВОРЕННЯ ДАШБОРДІВ ТА ВІЗУАЛІЗАЦІЇ

Мета роботи:

1. Формування практичних навичок побудови дашбордів в SIEM-системі Wazuh.

2. Аналіз ключових метрик безпеки та застосування принципів ефективної візуалізації для оперативного прийняття рішень.

Теоретичні відомості

Security Dashboard – це централізована панель моніторингу, призначена для агрегування, кореляції та візуального представлення показників інформаційної безпеки в режимі реального часу або за визначений період.

У контексті Security Operations Center (SOC) дашборд виконує функцію інтерфейсу ситуаційної обізнаності (situational awareness). Він дозволяє аналітику швидко оцінити поточний стан безпеки інфраструктури, виявити аномалії, відстежити динаміку інцидентів та визначити пріоритети реагування.

Класифікація дашбордів за рівнем управління

Ефективність візуалізації залежить від того, для кого вона призначена. В архітектурі SOC прийнято виділяти три основні рівні:

1. Operational (Операційний).

2. Tactical (Тактичний).

3. Strategic (Стратегічний).

Операційний дашборд орієнтований на аналітиків першої та другої лінії. Його ключова характеристика – робота в режимі реального часу. Такий дашборд містить деталізовану інформацію про алерти, активні інциденти, статус агентів, події високої критичності. Основна задача – забезпечення швидкого виявлення та первинного реагування.

Тактичний дашборд використовується керівниками груп або менеджерами SOC. Він відображає агреговану статистику за день або тиждень, демонструє тренди, ефективність обробки інцидентів, навантаження на команду. Фокус зміщується з окремих подій на продуктивність процесів.

Стратегічний дашборд призначений для топ-менеджменту та C-level. Такий дашборд показує високорівневі показники за місяць або квартал, концентруючись на бізнес-ризиках, рівні зрілості безпеки та відповідності вимогам. Деталізація мінімальна, натомість акцент робиться на ризик-орієнтованих метриках.

Ключові метрики безпеки (KPIs)

Ефективність SOC оцінюється через систему кількісних показників, які можна умовно поділити на три категорії:

1. Detection Metrics (Метрики виявлення).
2. Response Metrics (Метрики реагування).
3. Coverage Metrics (Метрики покриття).

Метрики виявлення характеризують якість моніторингу. Mean Time to Detect (MTTD) відображає середній час від моменту виникнення події до її виявлення. Зменшення цього показника свідчить про підвищення ефективності системи детекції. Важливими також є обсяг алертів (alert volume) та частка істинно-позитивних спрацювань (True Positive Rate), що демонструє якість кореляційних правил.

Метрики реагування оцінюють швидкість та ефективність обробки інцидентів. Mean Time to Respond (MTTR) показує середній час до початку реагування, Mean Time to Contain (MTTC) – час локалізації загрози, а загальний час вирішення інциденту дозволяє оцінити повний цикл реагування.

Метрики покриття визначають рівень видимості інфраструктури. До них належать відсоток активів, охоплених моніторингом (asset coverage), доступність джерел логів (log source availability) та технічний стан агентів (agent health status). Недостатнє покриття створює «сліпі зони» у системі захисту.

Принципи ефективної візуалізації

Побудова дашборду повинна відповідати принципам інженерії візуалізації даних. Одним із базових є правило “5 секунд”: користувач має зрозуміти загальну ситуацію за мінімальний час без додаткового аналізу. Це

досягається через чітку ієрархію інформації, де критичні показники розміщуються у верхній частині екрана та виділяються розміром або кольором.

Ієрархія передбачає поділ на три рівні:

1. Критичні метрики – найбільш помітні.
2. Важливі показники – середній візуальний акцент.
3. Допоміжна інформація – менш виражена.

Колірне кодування використовується для швидкої інтерпретації статусу:

1. Червоний – критичний стан, необхідне негайне реагування.
2. Жовтий – попередження або потенційна проблема.
3. Зелений – нормальний стан.
4. Синій – інформаційні показники без ризику.

Надмірна кількість елементів, перевантаженість графіками або використання контрасних кольорів без логічної структури знижують ефективність сприйняття.

Типи візуалізацій у Wazuh

У системі Wazuh доступний широкий набір інструментів для побудови дашбордів, що дозволяє відображати події безпеки у різних аналітичних зрізах:

1. Area Chart - застосовується для відображення динаміки подій у часі та аналізу трендів.

2. Bar Chart - використовується для порівняння категорій, наприклад, розподілу атак за типами або хостами.

3. Pie Chart - демонструє пропорційний розподіл подій.

4. Data Table - надає деталізоване представлення сирих даних.

5. Metric - дозволяє відобразити окремий числовий показник (наприклад, кількість критичних алертів).

6. Heatmap - використовується для виявлення інтенсивності подій за часовими або категоріальними параметрами

7. Tag Cloud - демонструє частоту появи певних термінів або типів подій.

Завдання на лабораторну роботу

Завдання 1. Запуск середовища та базова навігація.

1. Запустіть Wazuh.

./lab-management.sh start wazuh

2. Підключіться до Wazuh Dashboard.

URL: https://localhost:443
Логін: admin
Пароль: SecretPassword

3. У лівому меню натисніть **Explore → Dashboards.**
4. Додайте тестові дані (Add Sample Data).

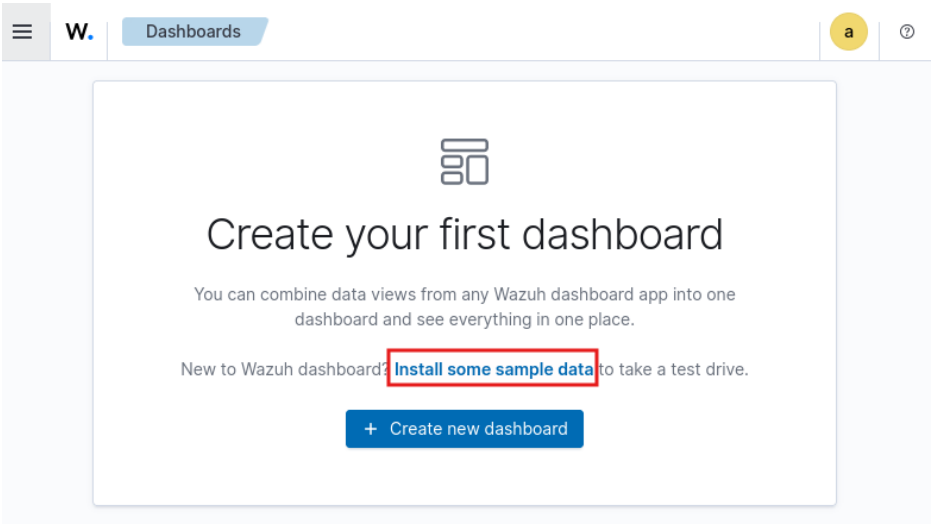

Рисунок 1 – Процес додавання тестових даних

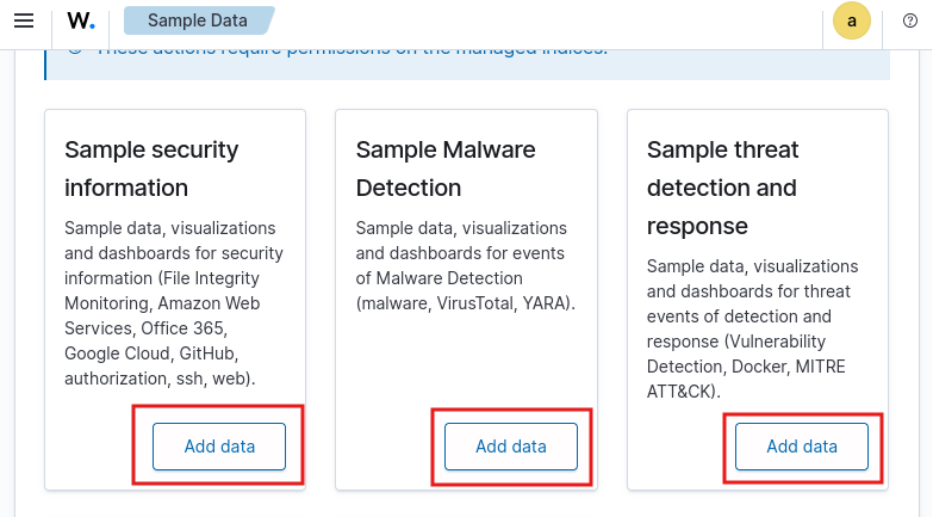

Рисунок 2 - Процес додавання тестових даних

У разі виникнення помилок – спробуйте повторно додати тестові дані декілька разів з інтервалом 1-2 хв.

Завдання 2. Створення базової візуалізації.

1. Поверніться до **Explore → Dashboards.**
2. Натисніть **Create new dashboard.**

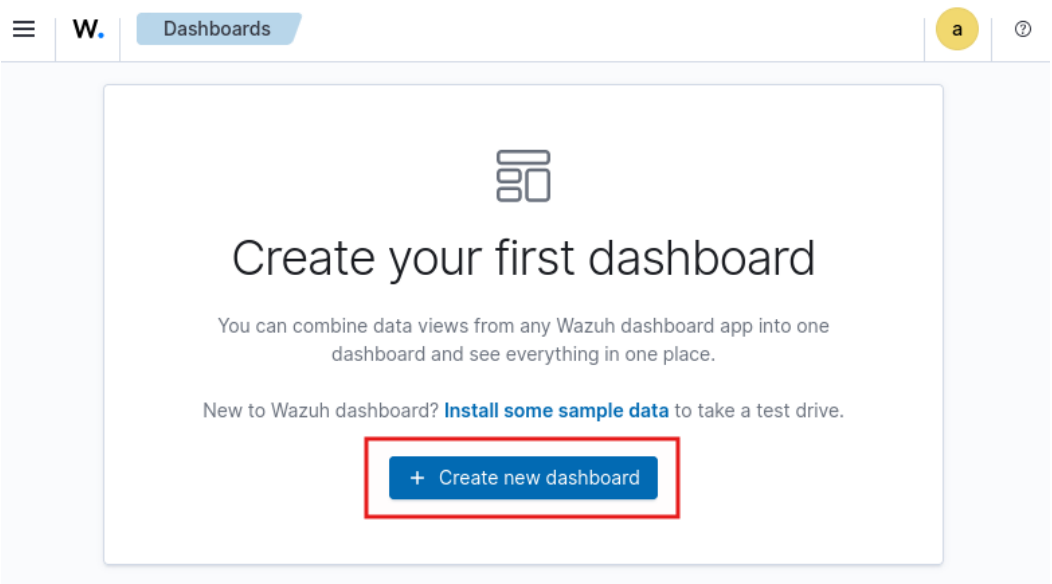

Рисунок 3 – Процес створення дашборду

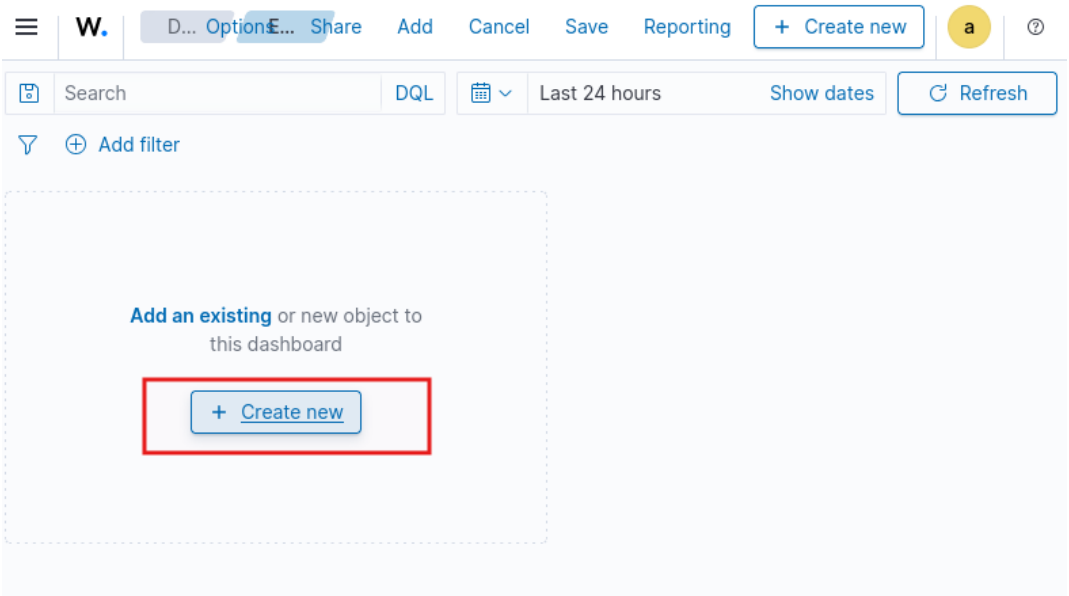

Рисунок 4 – Процес створення дашборду

3. Виберіть тип: **Vertical Bar Chart.**

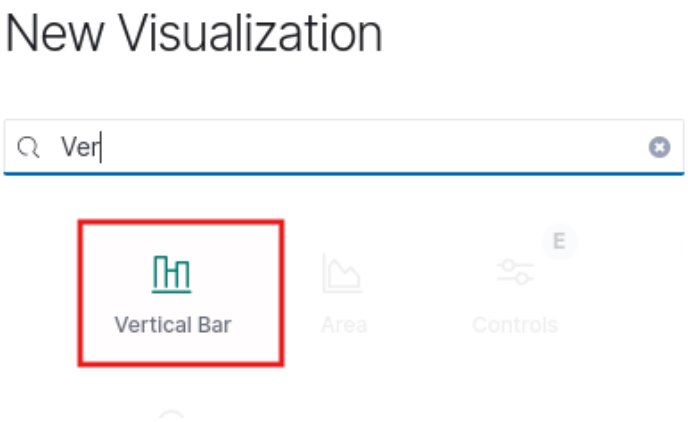

Рисунок 5 – Процес створення дашборду

4. Index pattern: wazuh-alerts-*
5. Налаштування метрик:

Y-axis *(Metrics):*

Aggregation: Count

Custom label: Number of Alerts

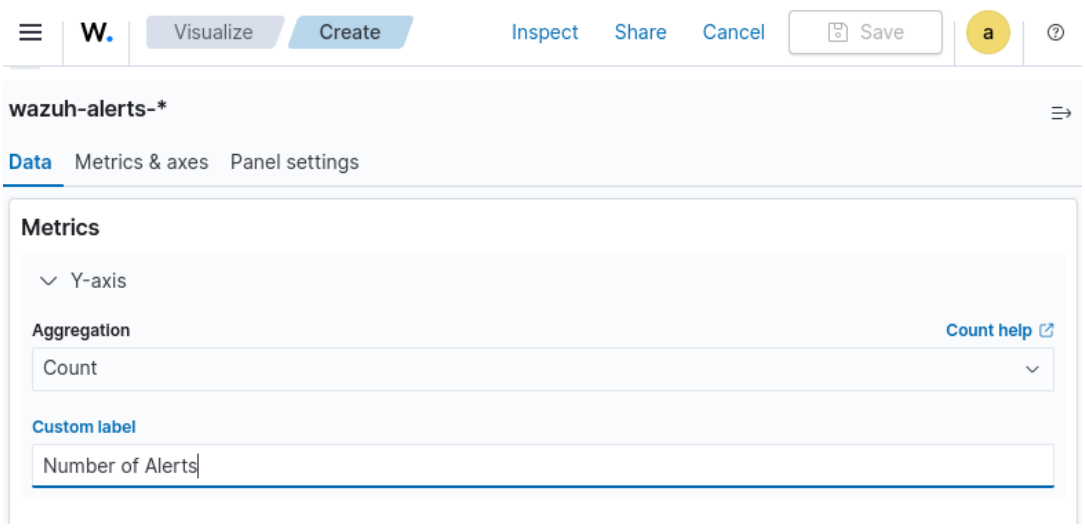

Рисунок 6 – Приклад налаштування метрик

6. Налаштування buckets:

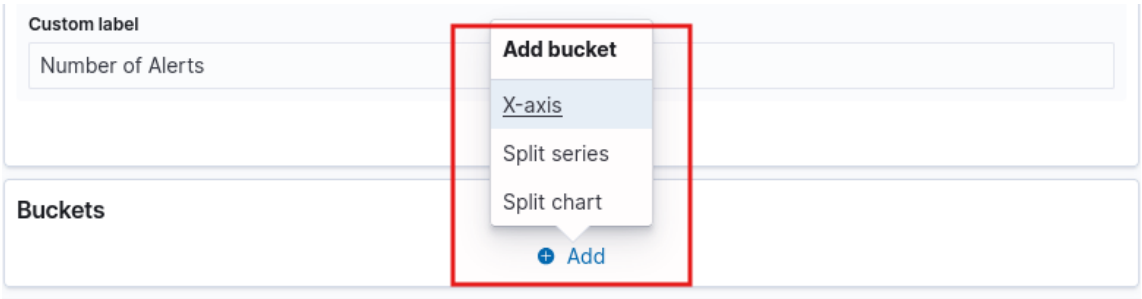

Рисунок 7 – Приклад налаштування buckets

***X-axis** (Buckets):*

Aggregation: Terms

Field: rule.description

Order: Descending

Size: 10

Custom label: Alert Rules

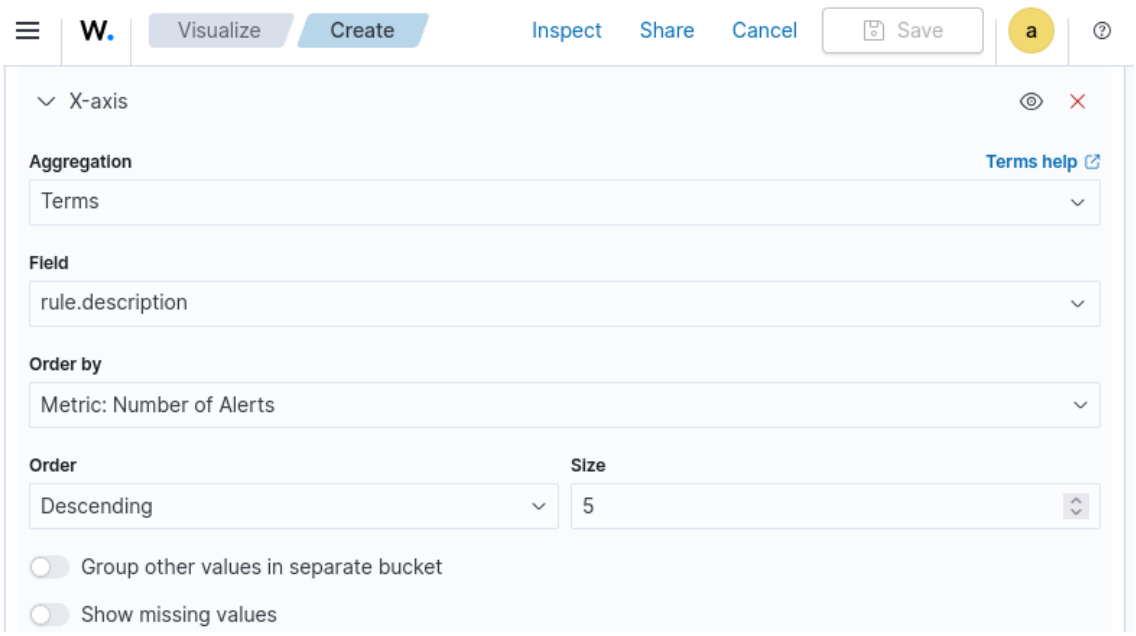

Рисунок 8 – Приклад налаштування buckets

7. Налаштування часового діапазону:

*У правому верхньому куті встановіть: **Last 24 hours***

8. Збережіть візуалізацію

*Натисніть **Update**, після чого натисність **Save***

Title: Top 10 Alert Rules - Last 24h

*Натисніть **Save and return***

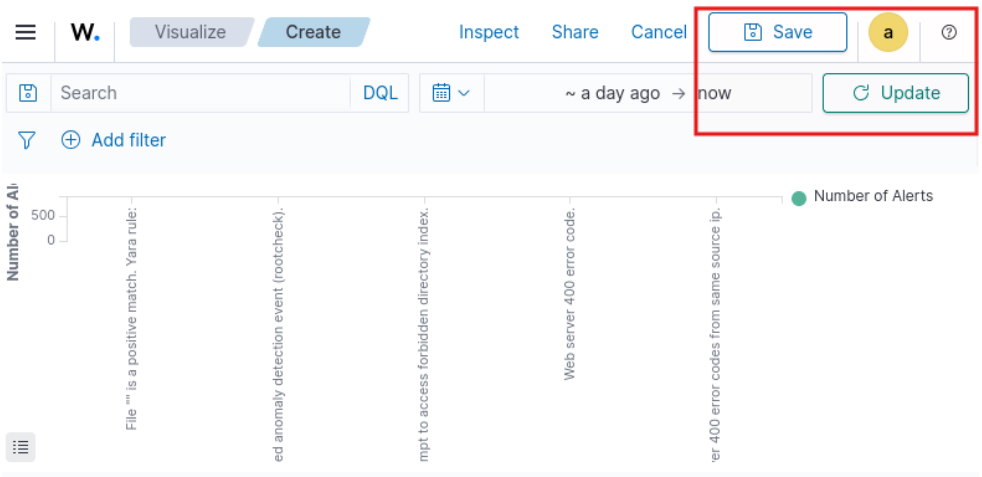

Рисунок 8 – Збереження дашборду

Завдання 3. Створення операційного дашборду SOC.

1. Створення нового дашборду.

Перейдіть до Explore → Dashboards → Create new dashboard

Натисніть Add an existing

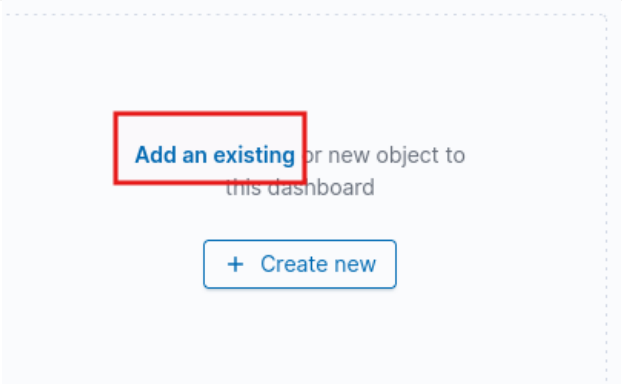

Рисунок 9 – Процес налаштування дашборду

2. Додайте вже створену візуалізацію

Знайдіть візуалізацію Top 10 Alert Rules - Last 24h

Клікніть на неї, щоб додати

3. Створіть метрику "Total Alerts".

- Натисніть + **Create new.**
- Виберіть тип: **Metric.**
- Index: wazuh-alerts-*.
- Metric aggregation: Count.
- Custom label: Total Alerts.
- Збережіть як: Total Alerts Today.

4. Створіть візуалізацію "Alerts by Severity".

- Тип: **Pie**

- Index: wazuh-alerts-*

- Slice size metric: Count

- Split slices (+ **Add** в розділі **Buckets**):

    - Aggregation: Range
    - Field: rule.level
    - Ranges:
        - 0-4 (Info)
        - 5-7 (Low)
        - 8-11 (Medium)
        - 12-15 (High)

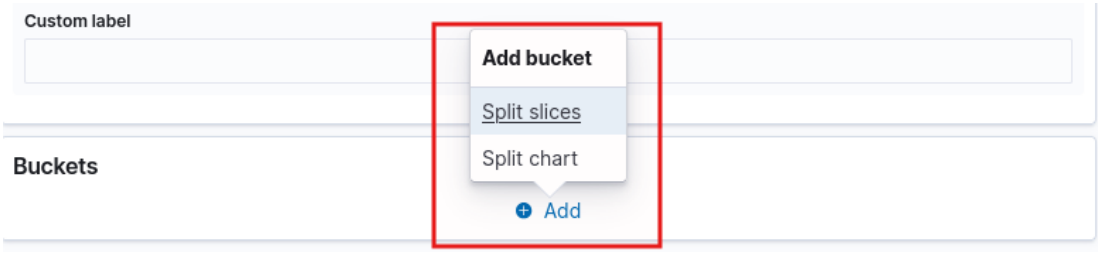

Рисунок 10 – Вибір Split slices

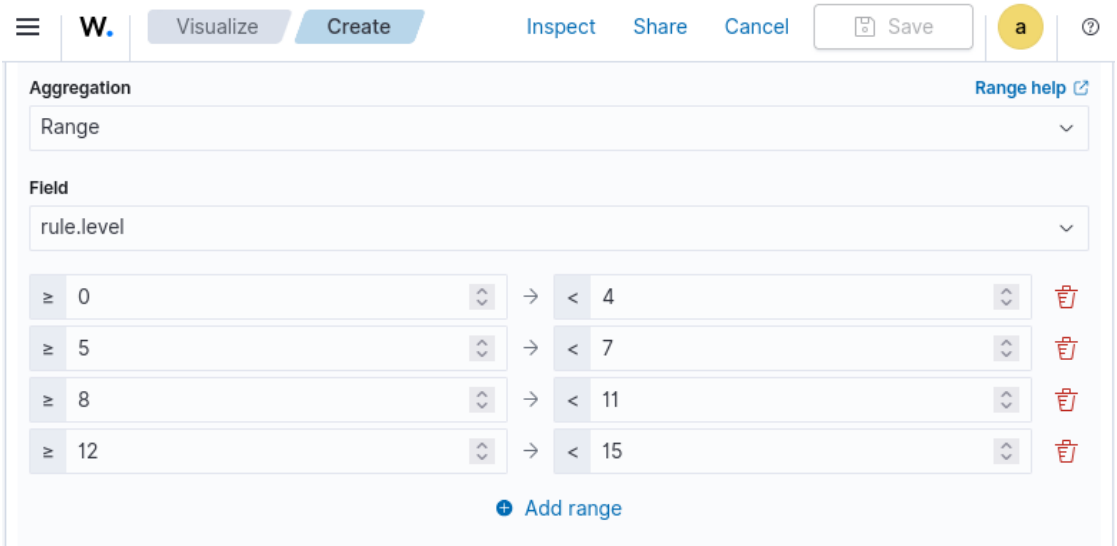

Рисунок 11 – Результат налаштувань

- Збережіть як: Alerts by Severity Level.

5. Створіть візуалізацію "Alert Timeline".
   - Тип: **Area**
   - Index: wazuh-alerts-*
   - Y-axis: Aggregation - Count
   - X-axis: Date Histogram
     - Field: timestamp
     - Interval: Auto
   - Split series:
     - Sub-aggregation: Terms
     - Field: rule.level
     - Order: Descending
     - Size: 5
   - Збережіть як: Alert Timeline by Level
6. Додайте таблицю "Recent Critical Alerts"
   - Тип: **Data Table**
   - Index: wazuh-alerts-*
   - Metrics: Count
   - Bucket: Split rows
     - Aggregation: Terms
     - Field: rule.description
     - Size: 15
   - Add sub-bucket: Split rows
     - Sub-aggregation: Terms
     - Field: agent.name
     - Size: 5
   - Збережіть як: Critical Alerts Table
7. Організація дашборду.
   - Розташуйте візуалізації логічно:
     - Зверху: Великі метрики (Total Alerts)

- Середина: Графіки трендів (Timeline)
- Знизу: Детальні таблиці

- Змінюйте розміри панелей, перетягуючи їх кути

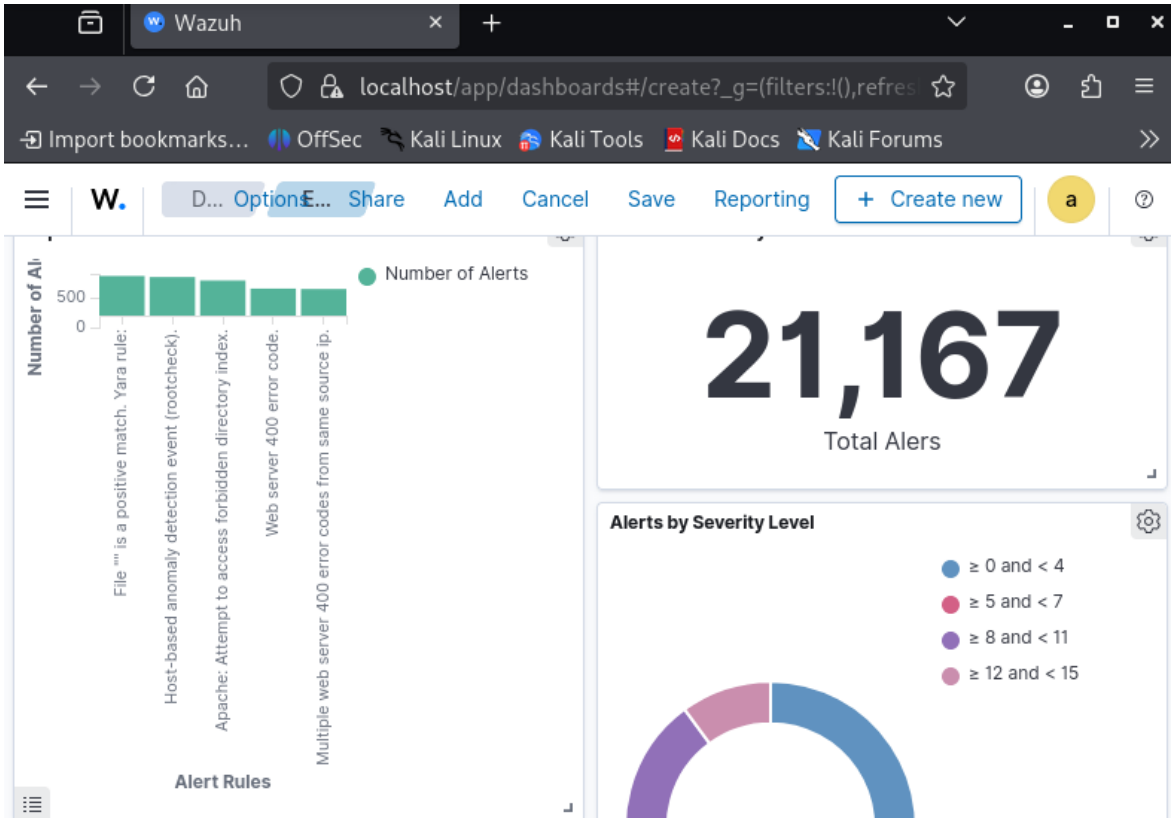

Рисунок 12 – Приклад організації дашборду

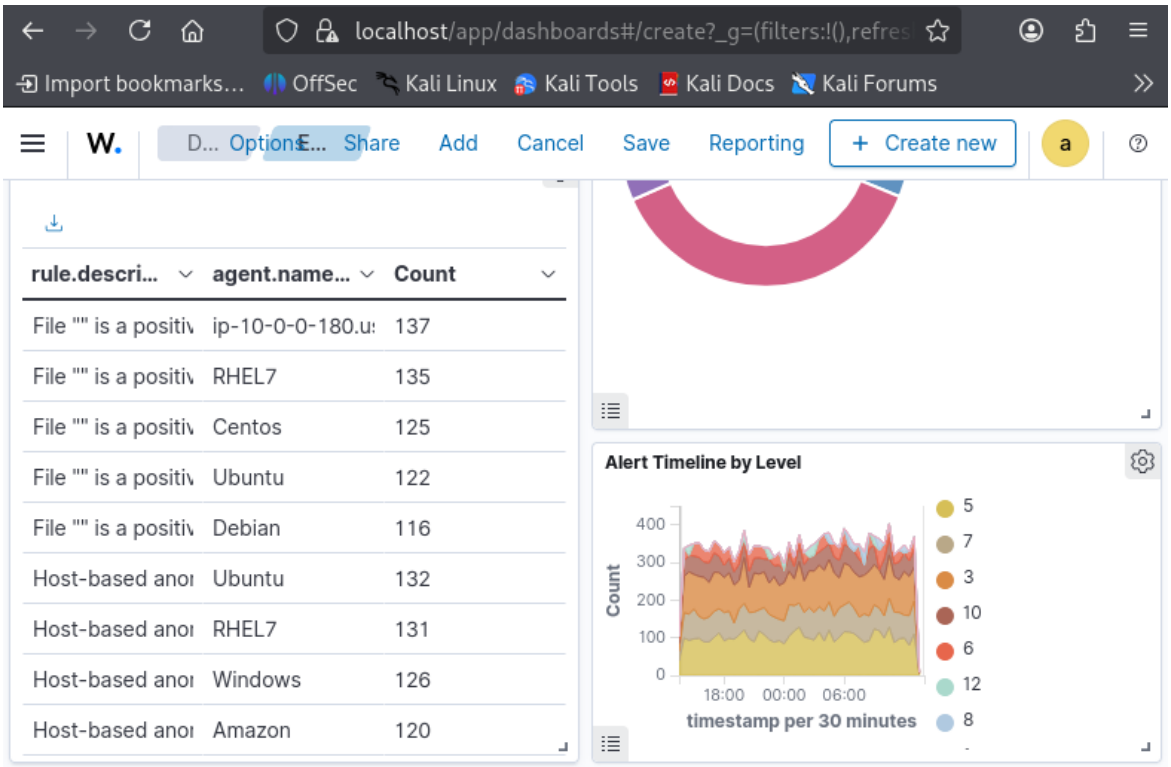

Рисунок 13 – Приклад організації дашборду

8. Збережіть дашборд.

   - Натисніть **Save**

   - Title: SOC Operations Dashboard

   - Description: Real-time security operations overview

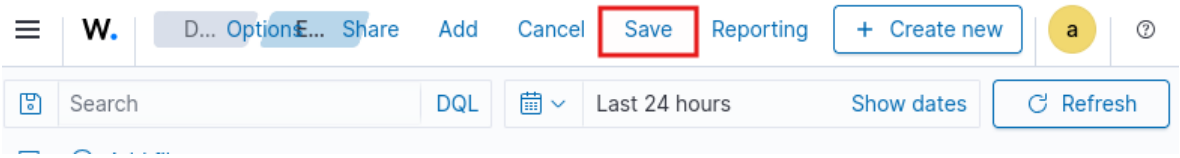

Рисунок 14 – Процес збереження дашборду

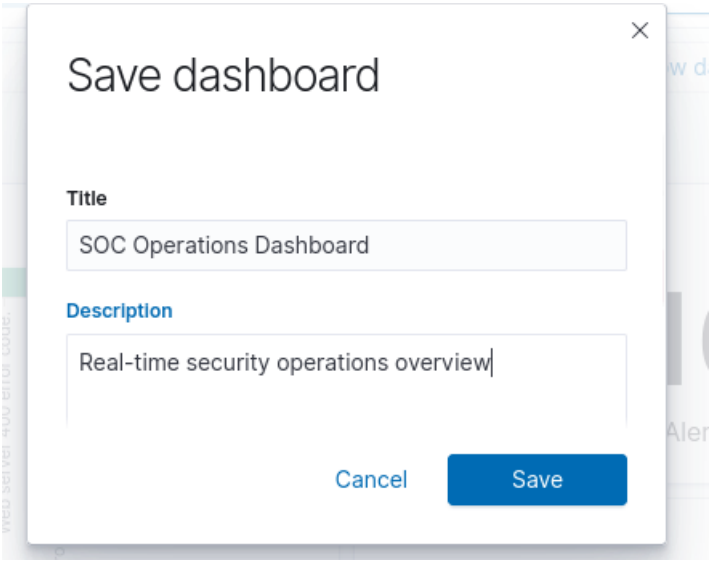

Рисунок 15 – Процес збереження дашборду

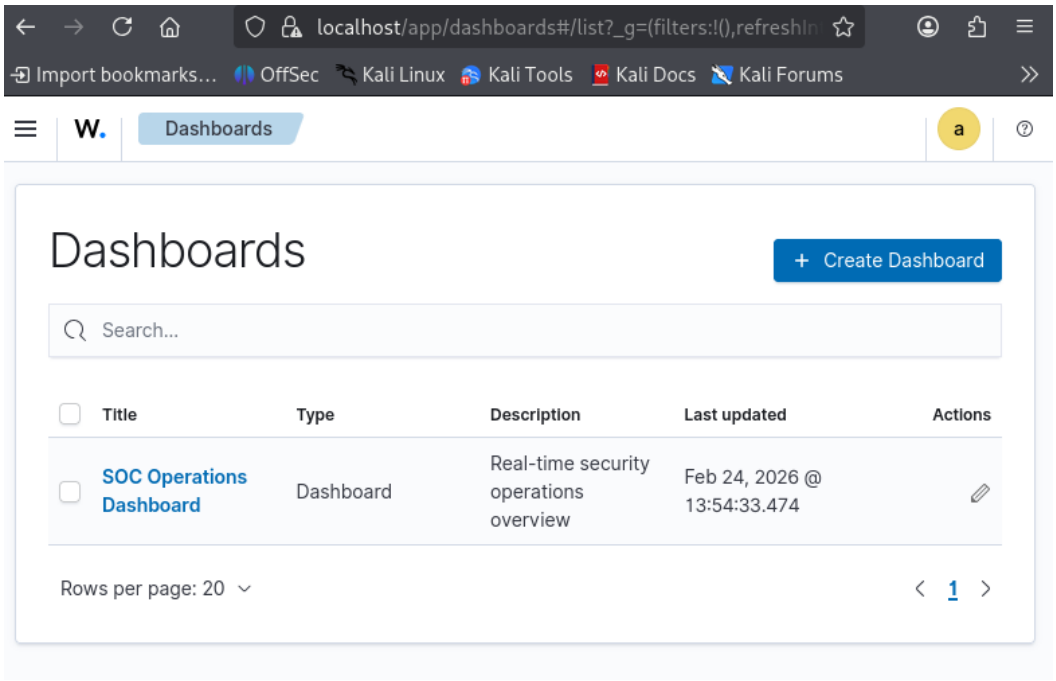

Рисунок 16 – Збережений дашборд

Завдання 4. Налаштування звітів.

1. Експорт вручну.

- Відкрийте дашборд.
- У верхньому меню натисніть **Reporting.**
- Виберіть **Download PDF** або **PNG/CSV.**
- Налаштуйте параметри експорту.
- Збережіть звіт

Завдання 5. Створення спеціалізованого дашборду для FIM.

1. Створіть дашборд "File Integrity Monitoring":
2. Перейдіть до **Dashboards → Create Dashboard**

Процес створення візуалізацій:

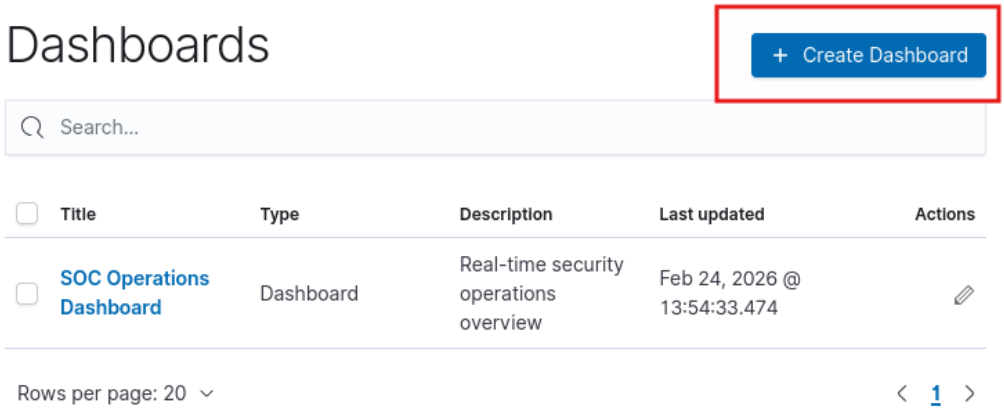

Рисунок 17 – Процес створення візуалізацій

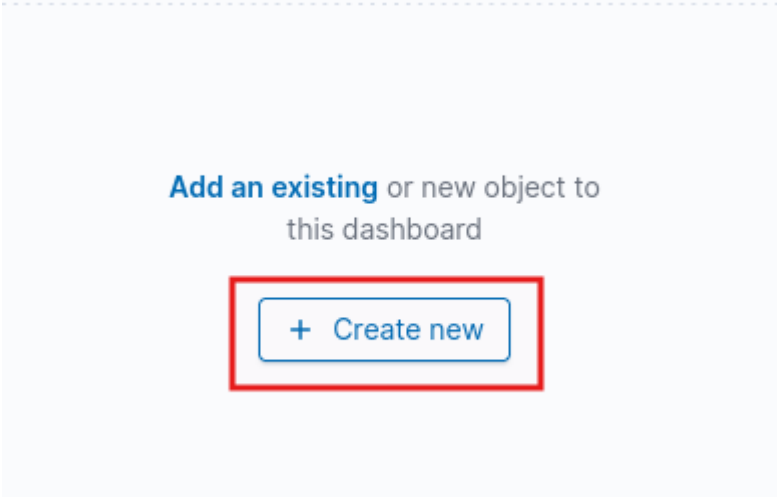

Рисунок 18 – Процес створення візуалізацій

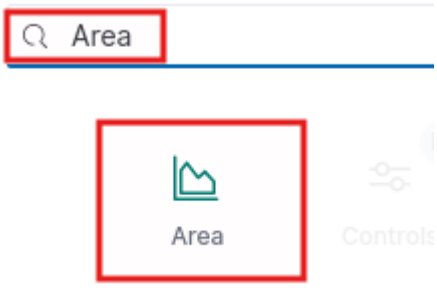

Рисунок 19 – Процес створення візуалізацій

Візуалізація 1: File Changes Over Time

- Тип: Area
- Index: wazuh-alerts-*
- Filter: rule.groups: "syscheck"

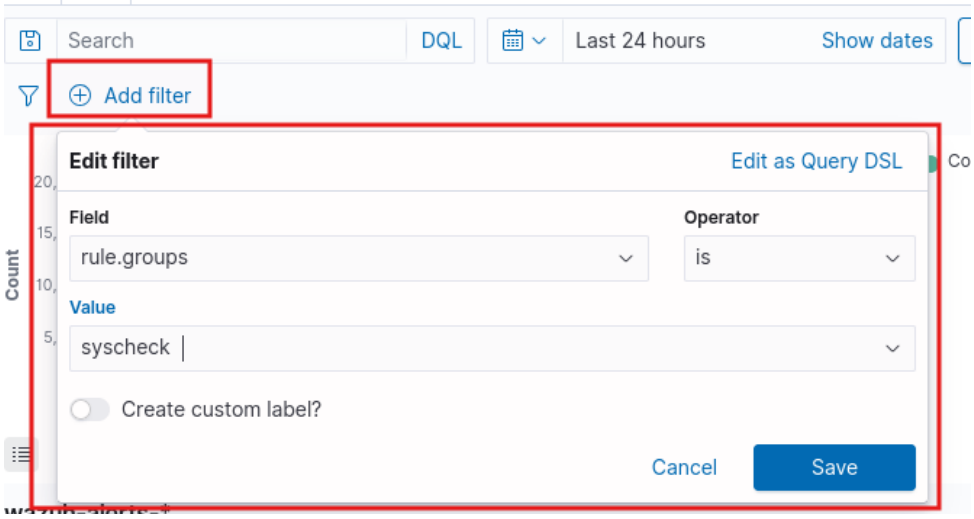

Рисунок 20 – Налаштування фільтру

Візуалізація 2: Top Changed Files

- Тип: Data Table
- Index: wazuh-alerts-*
- Buckets: Split rows.
- Aggregation: Terms.
- Field: syscheck.path
- Показати кількість змін

Візуалізація 3: Changes by Agent

- Тип: Pie
- Index: wazuh-alerts-*

- Buckets: Split slices.

- Aggregation: Terms.

- Field: agent.name

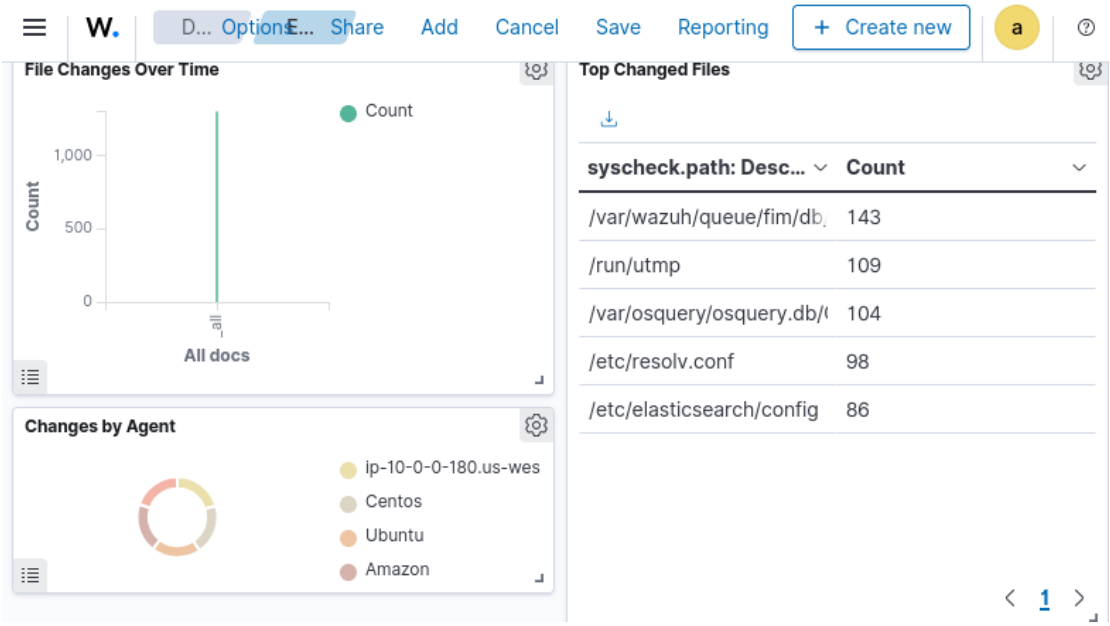

Рисунок 21 – Створені візуалізації

3. Збережіть дашборд.

Завдання 6. Презентація метрик безпеки.

1. Створіть презентаційний режим

- Відкрийте Executive Dashboard.

- Натисніть **Full screen** mode (F11 у браузері) для режиму демонстрації.

2. Створіть PDF-звіт для менеджменту.

- Перейдіть до **Dashboards** та оберіть новостворений дашборд “File Integrity Monitoring”

- Натисніть “**Edit**” у верхній панелі → **Create New**

- Тип візуалізації: Markdown.

- Скопіюйте наступний текст, відредагувавши параметри:

```
# Monthly Security Report
## February 2026

**Prepared by:** SOC Team
**Date:** [дата], 2026
```

```
### Executive Summary
This report provides an overview of the security posture...

### Key Findings
- Total security events: [число]
- Critical incidents: [число]
- Response time (avg): [час]
```

- Збережіть візуалізацію з назвою: Markdown.

- Зручно розташуйте Markdown на дашборді.

- Експортуйте дашборд як PDF

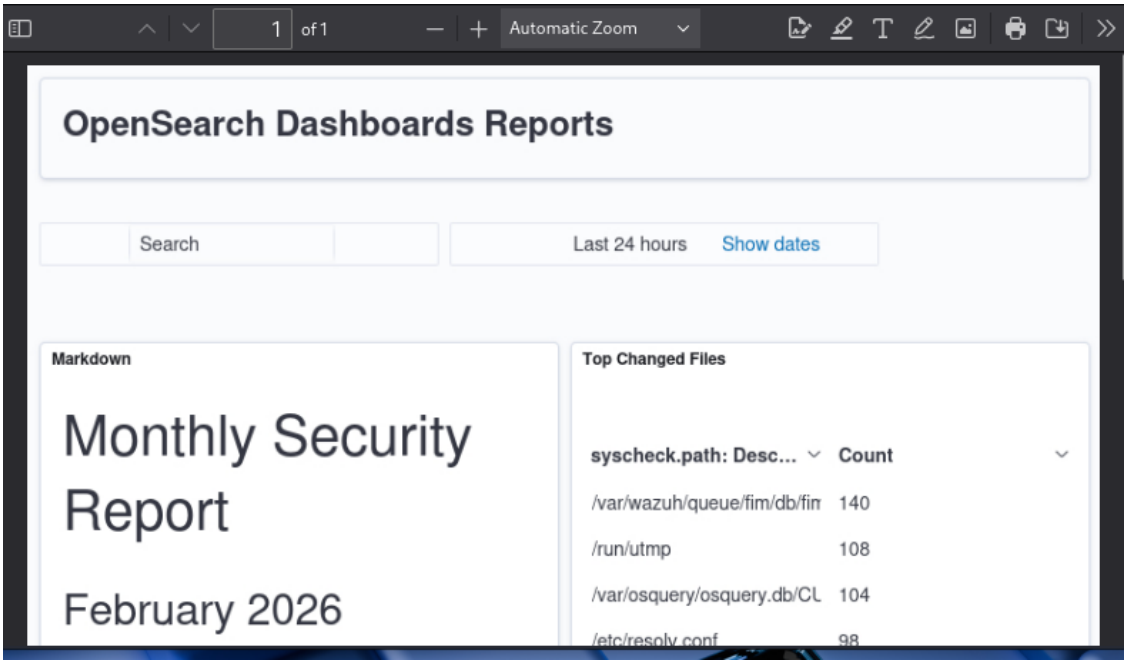

Рисунок 22 – Приклад експортованого дашборду

Контрольні запитання

1. Який тип дашборду використовується для роботи аналітиків SOC у режимі реального часу?

2. Який показник характеризує середній час від виникнення події до її виявлення?

3. Яка агрегація використовується для відображення загальної кількості алертів у типі візуалізації Metric?

4. Яке поле використовується для фільтрації подій File Integrity Monitoring.

5. Який принцип візуалізації передбачає, що користувач має зрозуміти ситуацію за 5 секунд?

6. Який колір у дашбордах зазвичай позначає критичний стан?

7. Яка візуалізація дозволяє представити пропорційний розподіл подій за рівнями критичності?

8. Який інструмент використовується для експорту дашборду у PDF у Wazuh Dashboard?