Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(назва освітнього ступеня)

на тему: Моніторинг стану інформаційної системи на основі Apache Splunk

Виконав(ла): студент(ка) 4 курсу, групи СТс-42
спеціальності 126 Інформаційні системи та технології
(шифр і назва спеціальності)

		Хільчук А.І.
	(підпис)	(прізвище та ініціали)
Керівник		Гром'як Р.С.
	(підпис)	(прізвище та ініціали)
Нормоконтроль		Шимчук Г.В.
	(підпис)	(прізвище та ініціали)
Завідувач кафедри		Боднарчук І.О.
	(підпис)	(прізвище та ініціали)
Рецензент		Золотий Р.З.
	(підпис)	(прізвище та ініціали)

Тернопіль
2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра комп'ютерних наук
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Боднарчук І.О.
(підпис) (прізвище та ініціали)
«25» січня 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр
(назва освітнього ступеня)
за спеціальністю 126 Інформаційні системи та технології
(шифр і назва спеціальності)
студенту Хільчук Андрій Ігорович
(прізвище, ім'я, по батькові)

1. Тема роботи **Моніторинг стану інформаційної системи на основі Apache Splunk**

Керівник роботи **к.ф.-м.н., доц. Гром'як Р.С.**
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
Затверджені наказом ректора від «*16*» *березня* 2022 року № *4/7-162*
2. Термін подання студентом завершеної роботи 17 червня 2022 р.
3. Вихідні дані до роботи Літературні джерела з тематики роботи

4. Зміст роботи (перелік питань, які потрібно розробити)

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Гурик О.Я., к.т.н., доц.		

7. Дата видачі завдання 25 січня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	25.01.22-27.01.22	*Виконано*
2.	Підбір джерел по темі роботи	28.01.22 – 01.04.22	*Виконано*
3.	Оформлення першого розділу	15.04.2022	*Виконано*
4.	Оформлення другого розділу	30.04.2022	*Виконано*
5.	Виконання завдання до підрозділу «Безпека		
	життєдіяльності, основи охорони праці»	10.05.2022	*Виконано*
6.	Оформлення кваліфікаційної роботи	17.02.2022	*Виконано*
7.	Перевірка на плагіат	02.06.2022	*Виконано*
8.	Нормоконтроль	08.06.2022	*Виконано*
9.	Попередній захист кваліфікаційної роботи	09.06.2022	*Виконано*
10.	Захист кваліфікаційної роботи	21.06.2022	

Студент _____ Хільчук А.І.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Гром’як Р.С.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Моніторинг стану інформаційної системи на основі Apache Splunk // Кваліфікаційна робота освітнього рівня "Бакалавр" // Хільчук Андрій Ігорович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра комп'ютерних наук, група СТс-42 // Тернопіль, 2022 // с. – 48, рис. – 18, табл. – 2, кресл. – 10, бібліогр. – 11.

Ключові слова: моніторинг інформаційних систем, машинні дані, файли журналів, big data.

Splunk — це програмне забезпечення, яке використовується для пошуку та аналізу машинних даних. Ці машинні дані можуть надходити з веб-додатків, датчиків, пристроїв або будь-яких даних, створених користувачем. Він відповідає потребам IT-інфраструктури, аналізуючи журнали, створені в різних процесах, але також може аналізувати будь-які структуровані або напівструктуровані дані з належним моделюванням даних. Він має вбудовані функції для розпізнавання типів даних, роздільників полів та оптимізації процесів пошуку. Він також забезпечує візуалізацію даних результатів пошуку.

ABSTRACT

Monitoring the status of the information system based on Apache Splunk // Qualification work of the educational level "Bachelor" // Andrii Khilchuk // Ternopil Ivan Puluj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Computer Science, Group CTc-42 // Ternopil, 2022 // p. – 48, fig. – 18, references – 11, posters – 13.

Key words: information systems monitoring, machine data, log files, big data.

Splunk is a software that is suitable for searching and processing of mashine data. These data can be read from web applications, devices, sensors or these data can be created by system user. So, this application fits for IT infrastructure, particularly for log-files analysis and for any structured or semi structured data, created in different software processes. This service implements onboard functions for data types recognition, fields separators and search optimization. It can be used to visualize results of search operations.

ЗМІСТ

ВСТУП

Splunk використовується для вилучення цінності з даних, згенерованих машиною. Його можна розглядати як інструмент аналізу даних для додатків великих даних. Splunk може ефективно обробляти великі дані без зниження продуктивності. Найкраща частина Splunk полягає в тому, що йому не потрібна база даних для зберігання даних, оскільки він широко використовує свої індекси для зберігання даних.

Splunk – це абсолютно швидкий двигун і забезпечує блискавичні результати. Ви можете усунути будь-яку проблему, вирішивши її з миттєвими результатами та провівши ефективний аналіз першопричин. Splunk можна використовувати як інструмент моніторингу, звітності, аналізу, інформації про безпеку та керування подіями. Splunk бере цінні згенеровані машиною дані та перетворює їх у потужний оперативний інтелект, надаючи статистику за допомогою звітів, діаграм і сповіщень.

Splunk – це програмне забезпечення, яке обробляє та виводить інформацію з машинних даних та інших форм великих даних. Ці дані генеруються центральним процесором, на якому працює, наприклад, веб-сервер, пристроями IoT, журналами мобільних додатків тощо. Ці дані не потрібно надавати кінцевим користувачам і вони не мають жодного бізнесовго сенсу. Однак вони надзвичайно важливі для розуміння, моніторингу та оптимізації роботи машин.

Splunk може читати ці неструктуровані, напівструктуровані або слабо структуровані дані. Після зчитування він дозволяє шукати, позначати, створювати звіти та інформаційні панелі на цих даних. Отже, з простого інструменту для аналізу журналів, Splunk пройшов довгий шлях, щоб стати загальним аналітичним інструментом для неструктурованих машинних даних і різних форм великих даних.

Splunk доступний у трьох різних категоріях продуктів, як показано нижче/

Splunk Enterprise — використовується компаніями, які мають велику IT-інфраструктуру та бізнес, керований IT. Він допомагає збирати та аналізувати дані з веб-сайтів, програм, пристроїв і сенсорів тощо.

Splunk Cloud — це хмарна платформа з тими ж функціями, що й версія для підприємства. Нею можна скористатися з самого Splunk або через хмарну платформу AWS.

Splunk Light — дозволяє шукати, звітувати та сповіщати про всі дані журналу в режимі реального часу з одного місця. Він має обмежені функціональні можливості та функціонал порівняно з двома іншими версіями.

Splunk може читати різноманітні формати даних, як-от JSON, XML, і неструктуровані машинні дані, такі як журнали веб- та програм. Неструктуровані дані можуть бути змодельовані в структуру даних за потребою користувача.

Застосовані дані індексуються Splunk для швидшого пошуку та запитів за різних умов. Пошук у Splunk передбачає використання індексованих даних з метою створення показників, прогнозування майбутніх тенденцій та визначення закономірностей у даних.

Сповіщення Splunk можна використовувати для ініціювання електронних листів або RSS-каналів, коли в даних, що аналізуються, виявлено певні критерії.

Інформаційні панелі Splunk можуть показувати результати пошуку у вигляді діаграм, звітів та зведених даних тощо.

Індексовані дані можна змоделювати в один або кілька наборів даних, які базуються на спеціалізованих знаннях предметної області. Це полегшує навігацію кінцевим користувачам, які аналізують бізнес-кейси, не вивчаючи технічні особливості мови обробки пошуку, яку використовує Splunk.

РОЗДІЛ 1. ОПИС СЕРВІСУ SPLUNK ДЛЯ МОНІТОРИНГУ ІНФОРМАЦІЙНИХ СИСТЕМ

В цьому розділі розглянемо особливості використання сервісу, його установку, інтерфейс, основні функції та їх виклик.

Стосовно установки, то тут ніяких особливостей немає. Існують установочні пакети для Unix та Windows систем, які не потребують установки додаткових компонентів і процес цей традиційний для кожної операційної системи і знайомий їх користувачам. Таким чином після установки сервіс готовий до використання і розкриємо далі основні елементи інтерфейсу користувача та прийоми роботи з сервісом.

Порівняємо сервіс Splunk з аналогом у таблиці 1.1

Таблиця 1.1 – Порівняння сервісу Splunk з ELK

Comparison criteria	Splunk	ELK (ElasticSearch, Logstash, and Kibana)
Технологія індексування	C++ based proprietary	Java-based Apache Lucene
Технологія пошуку	MapReduce based	Apache Lucene based
Мова пошуку	Splunk Processing Language	Query DSL
REST API для інтерфейсу пошуку	Available	Available

Архітектура Splunk складається з трьох основних компонентів:

- Splunk Forwarder;
- Splunk Indexer;
- Search Head.

Тепер розберемо значення всіх цих компонентів.

На наступній схемі (рисунок 1.1) показано, як вищезгадані компоненти працюють разом в архітектурі Splunk:

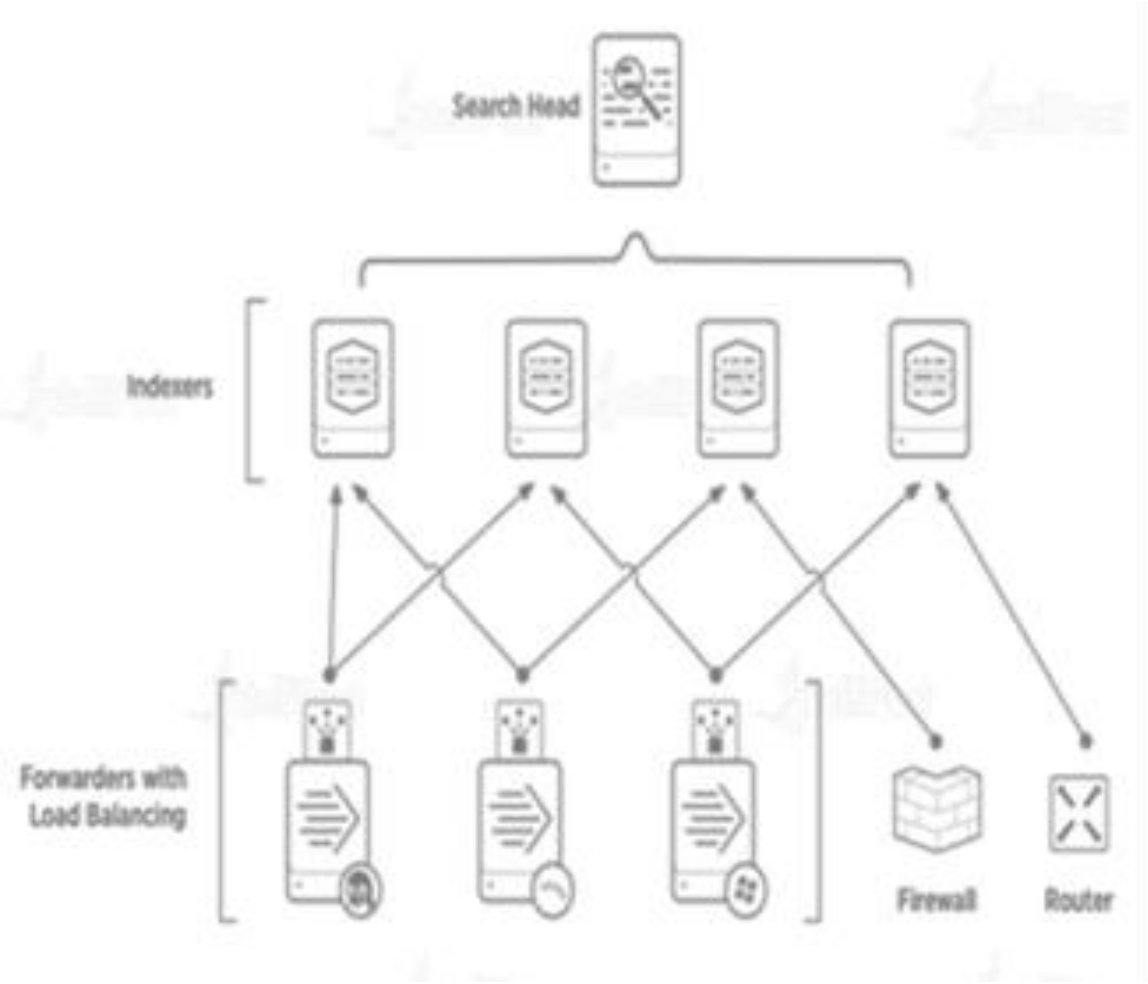

Рисунок 1.1 – Архітектура Splunk

Splunk Forwarder використовується для порівняння даних у реальному часі, щоб уможливити аналіз даних у реальному часі користувачами. Splunk Forwarder збирає всі дані журналу та відправляє їх до індексатора. Виконуючи всі ці дії, Splunk Forwarder споживає менше обчислювальної потужності, ніж інші традиційні інструменти моніторингу. Існує 2 типи Splunk Forwarders. Це:

- Splunk Universal Forwarder
- Splunk Heavy ForwarderІндекс Splunk

Splunk Indexer використовується для індексації та зберігання даних, отриманих від Splunk Forwarder. По суті, він перетворює дані на події, зберігає та додає їх до індексу, що, у свою чергу, покращує можливість пошуку. Дані, отримані від Splunk Forwarder, спочатку аналізуються, щоб видалити всі небажані дані, а потім виконується індексація. У всьому цьому процесі Splunk

Indexer створює такі файли, а потім розбиває їх на різні каталоги, які називаються сегментами:

- Стиснуті вихідні дані
- Індекси, що вказують на необроблені дані (файли .TSIDX)
- Файли метаданих

Splunk Search Head по суті – це графічний інтерфейс користувача, де користувач може виконувати різні операції відповідно до своїх вимог. На цьому етапі користувачі можуть легко взаємодіяти з Splunk і виконувати операції пошуку та запитів щодо даних Splunk. Користувачі можуть вводити ключові слова пошуку та отримувати результат відповідно до своїх вимог.

1.1 Інтерфейс користувач

Веб-інтерфейс Splunk складається з усіх інструментів, необхідних для пошуку, звітування та аналізу даних, які надходять. Той самий веб-інтерфейс надає функції для адміністрування користувачів та їхніх ролей. Він також надає посилання для прийому даних і вбудовані програми, доступні в Splunk. На рисунку 1.2 нижче показано початковий екран після входу в Splunk з обліковими даними адміністратора.

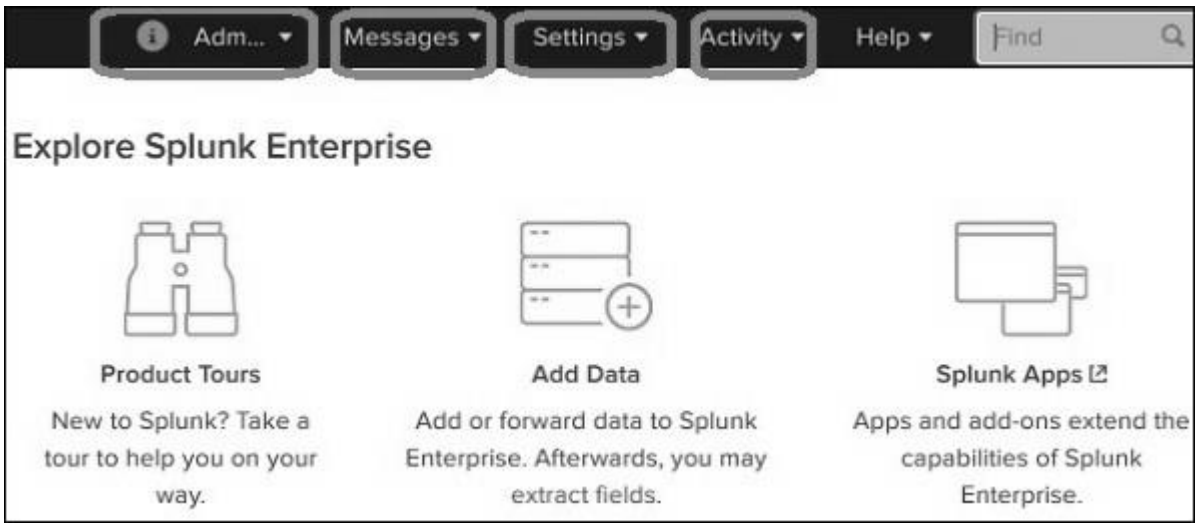

Рисунок 1.2 – Інтерфейс сервісу після входу під профілем адміністратора

Як видно на рисунку, користувачеві доступні посилання для управління (адміністрування) програмою, налаштування, формування звітів.

У спадному меню «Адміністратор» можна встановити та відредагувати дані адміністратора. Ми можемо скинути ідентифікатор електронної пошти адміністратора та пароль тощо.

Далі за посиланням адміністратора ми також можемо перейти до параметра налаштувань, де ми можемо встановити часовий пояс і домашню програму, на якій цільова сторінка буде відкриватися після вашого входу.

Посилання на налаштування програми показує всі основні функції, доступні в Splunk. Наприклад, ви можете додати файли пошуку та визначення пошуку, вибравши посилання пошуку. Ми обговоримо важливі налаштування цих посилань у наступних розділах.

Посилання на пошук і звітування переведе нас до функцій, де ми можемо знайти набори даних, доступні для пошуку звітів і сповіщень, створених для цих пошуків.

Передача даних у Splunk відбувається за допомогою функції «Add data», яка є частиною програми пошуку та звітування. Після входу в систему на головному екрані інтерфейсу Splunk відображається піктограма «Add data», як показано на рис. 1.2.

Натиснувши цю кнопку, ми відкриємо екран для вибору джерела та формату даних, які ми плануємо надіслати до Splunk для аналізу.

Ми можемо отримати дані для аналізу з офіційного сайту Splunk. Збережіть цей файл і розпакуйте його на локальному диску. Відкривши папку, ви можете знайти три файли різних форматів. Це дані журналу, створені деякими веб-програмами. Ми також можемо зібрати інший набір даних, наданих Splunk, який доступний на офіційній веб-сторінці Splunk. Після вибору файлу ми переходимо до наступного кроку за допомогою зеленої кнопки «Далі» у верхньому правому куті.

Splunk має вбудовану функцію для визначення типу даних, які надходять. Він також дає користувачеві можливість вибрати тип даних, відмінний від обраного Splunk. Натиснувши спадне меню типу джерела, ми можемо побачити різні типи даних, які Splunk може приймати та включити для пошуку. У поточному прикладі, наведеному на рис. 1.3, ми вибираємо тип джерела за замовчуванням.

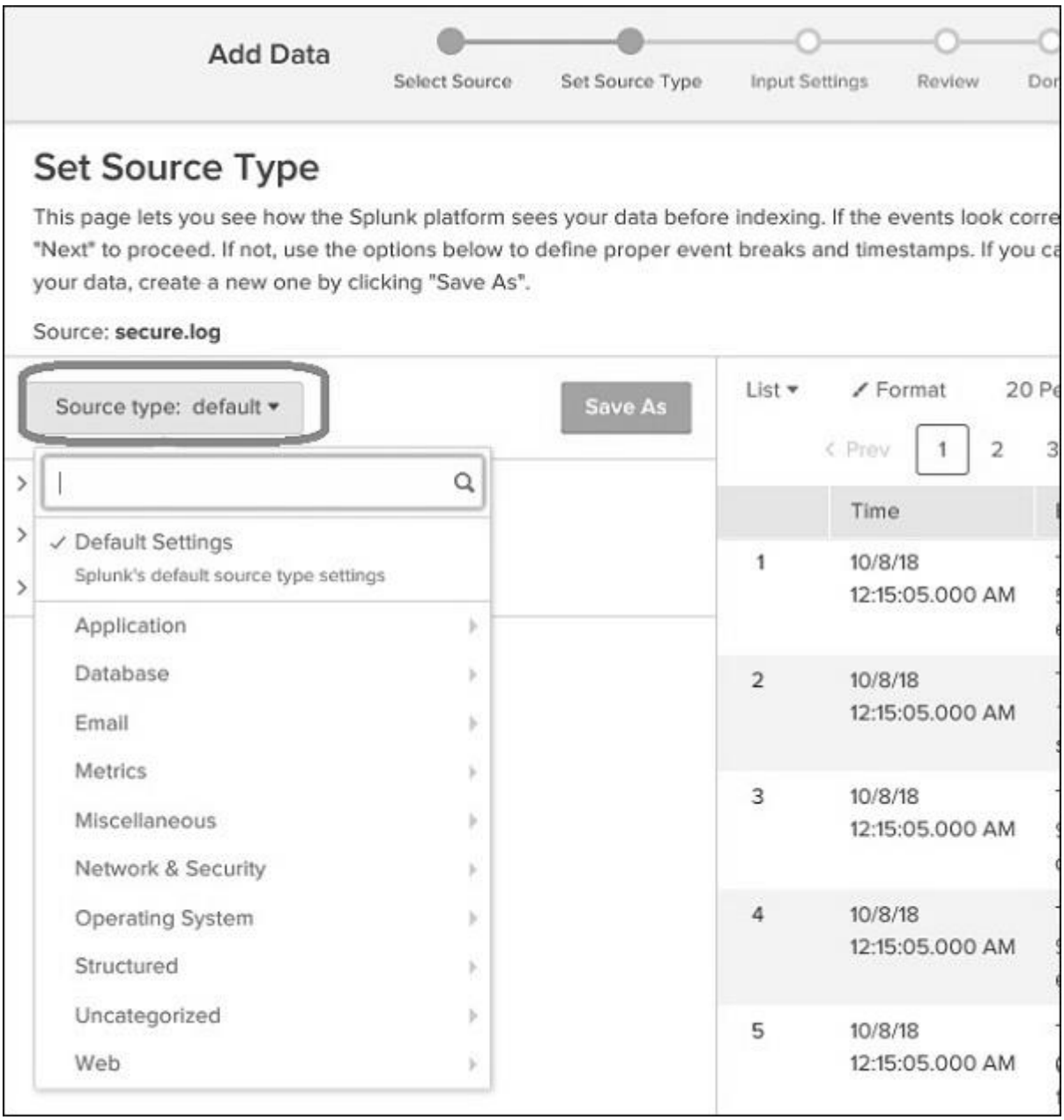

Рисунок 1.3 – Вибір типу джерела даних

Наступним кроком є налаштування вводу. На цьому етапі прийому даних ми налаштовуємо ім’я хоста, з якого надходять дані. Нижче наведено варіанти на вибір для імені хоста:

Constant value. Це повне ім'я хоста, на якому знаходяться вихідні дані.

regex on path. Використовується при потребі витягти ім’я хоста за допомогою регулярного виразу. Потім вводять регулярний вираз для хоста, який потрібно витягти, у поле Регулярний вираз.

segment in path. Якщо ви хочете витягти ім’я хоста з сегмента в шляху вашого джерела даних, введіть номер сегмента в поле Номер сегмента. Наприклад, якщо шлях до джерела є /var/log/ і ви хочете, щоб третій сегмент (ім’я хост-сервера) був значенням хоста, введіть «3».

Далі ми вибираємо тип індексу, який буде створено на вхідних даних для пошуку. Ми вибираємо стратегію індексування за замовчуванням. Зведений індекс створює лише підсумок даних шляхом агрегації та створює для нього індекс, тоді як індекс історії призначений для зберігання історії пошуку. Після натискання на наступну кнопку «Review Settings» ми бачимо підсумок налаштувань, які ми вибрали. Ми переглядаємо його та вибираємо Далі, щоб завершити завантаження даних. Після завершення завантаження з’явиться екран нижче, який показує успішне отримання даних та подальші можливі дії, які ми можемо виконати з ними.

1.2 Підтримувані джерела даних

Усі дані, що надходять до Splunk, спочатку оцінюються вбудованим блоком обробки даних і класифікуються за певними типами та категоріями даних. Наприклад, якщо це журнал з веб-сервера apache, Splunk може розпізнати це та створити відповідні поля із прочитаних даних.

Ця функція в Splunk називається визначенням типу джерела, і для цього використовуються вбудовані типи джерел, відомі як «попередньо навчені» типи

джерел. Це полегшує аналіз, оскільки користувачеві не потрібно вручну класифікувати дані та призначати будь-які типи даних полям вхідних даних.

Підтримувані типи джерел у Splunk можна побачити, завантаживши файл за допомогою функції «Add data», а потім вибравши спадне меню «Source type» як показано вище на рисунку 1.2.

Навіть у цих категоріях ми можемо далі рухатись глибше, щоб побачити всі підкатегорії, які підтримуються. Наприклад, коли ви вибираєте категорію бази даних, ви можете знайти різні типи баз даних та підтримувані файли, які Splunk може розпізнати (див. рис. 1.4).

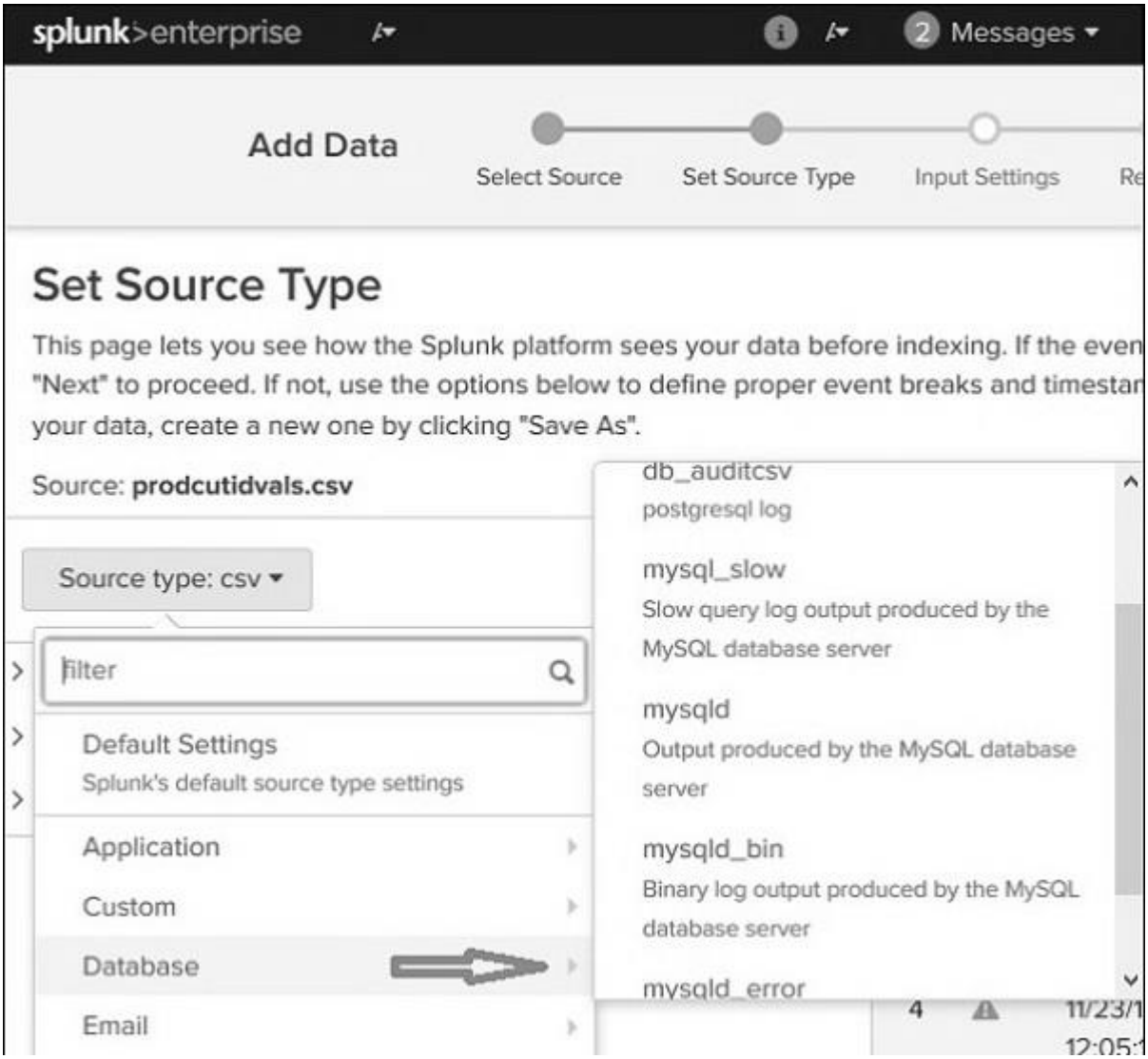

Рисунок 1.4 – Вибір підкатегорії типу джерела даних

В таблиці 1.2 нижче можна побачити перелік наперед визначених типів джерел даних, які Splunk може визначити автоматично.

1.3 Пошук у Splunk

Splunk має надійну функціональність пошуку, яка дозволяє шукати по всьому набору даних, який надходить. Доступ до цієї функції здійснюється через програму під назвою «Search & Reporting», яку можна побачити на панелі зліва після входу у веб-інтерфейс. Натиснувши програму «Search & Reporting», ми відкриємо вікно пошуку, де ми можемо почати пошук за даними журналу, які ми завантажили.

Таблиця 1.2 – Вбудовані типи джерел даних Splunk

Source Type Name	**Походження**
access_combined	Журнали HTTP веб-сервера комбінованого формату NCSA (можуть створюватися Apache або іншими веб-серверами)
access_combined_wcookie	Журнали веб-сервера в комбінованому форматі NCSA (можуть створюватися за допомогою Apache або інших веб-серверів), у кінці якого додано поле cookie
apache_error	Стандартний журнал помилок веб-сервера Apache
linux_messages_syslog	Стандартний системний журнал Linux (/var/log/messages на більшості платформ)
log4j	Стандартний вихід Log4j, створений будь-яким сервером J2EE за допомогою log4j
mysqld_error	Стандартний журнал помилок mysql

Можна, наприклад, ввести ім’я хоста у форматі, як показано нижче (див. рис. 1.5), і натиснути значок пошуку в крайньому правому куті. Це дає нам результат із виділенням пошукового терміну.

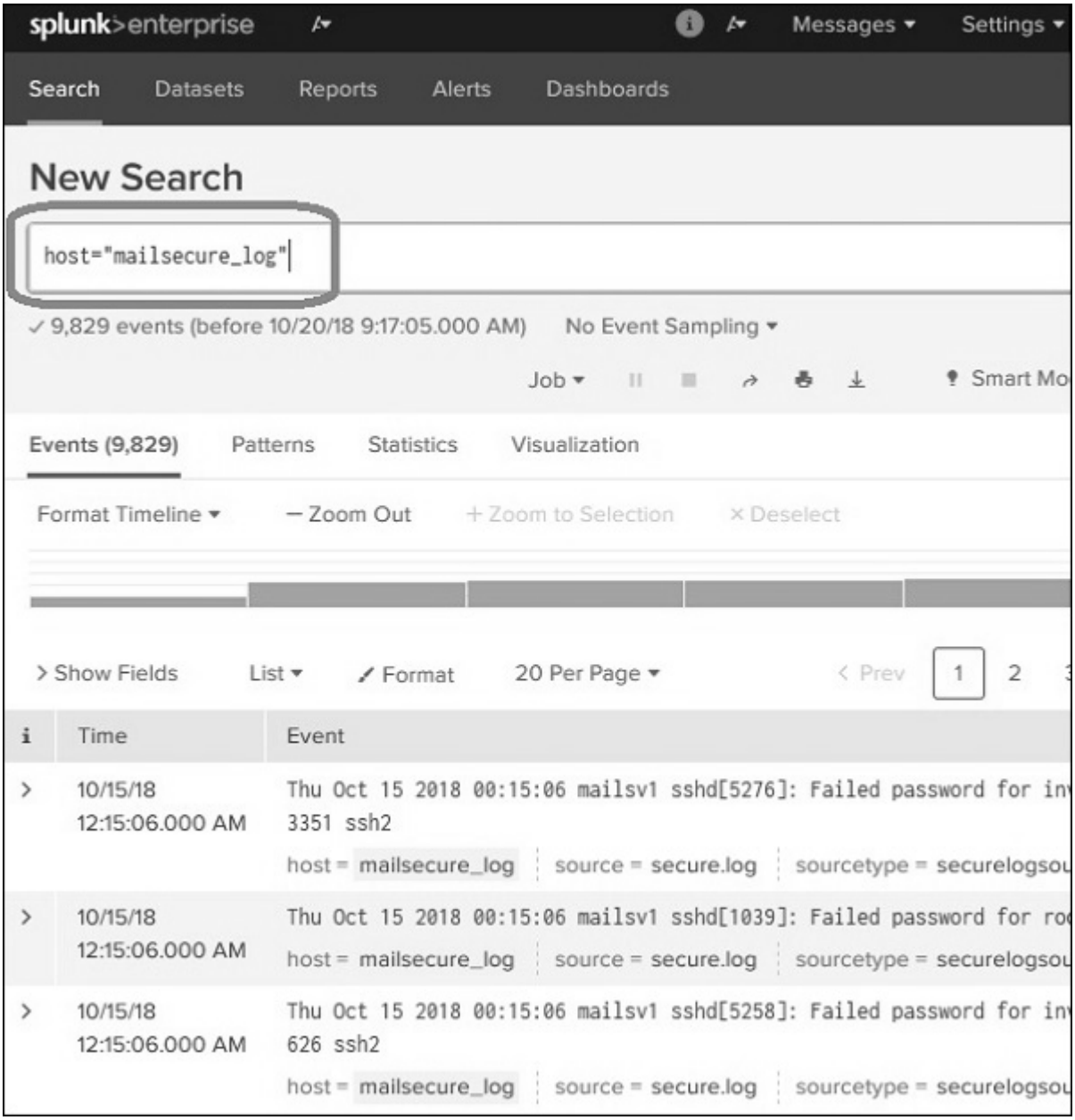

Рисунок 1.5 – Пошук значення у завантаженому файлі

Ми можемо комбінувати терміни, які використовуються для пошуку, записуючи їх один за одним та поміщаючи рядки пошуку користувача в подвійні лапки. Ми можемо використовувати символи підстановки (так звані Wild Card для ОС на основі Unix/Linux) в нашій опції пошуку в поєднанні з операторами І/АБО.

Коли Splunk зчитує завантажені машинні дані, він інтерпретує дані та поділяє їх на багато полів, які представляють єдиний логічний факт про весь запис даних. Наприклад, один запис інформації може містити ім'я сервера,

мітку часу події, тип події, яка реєструється, чи то спроба входу, чи відповідь HTTP тощо.

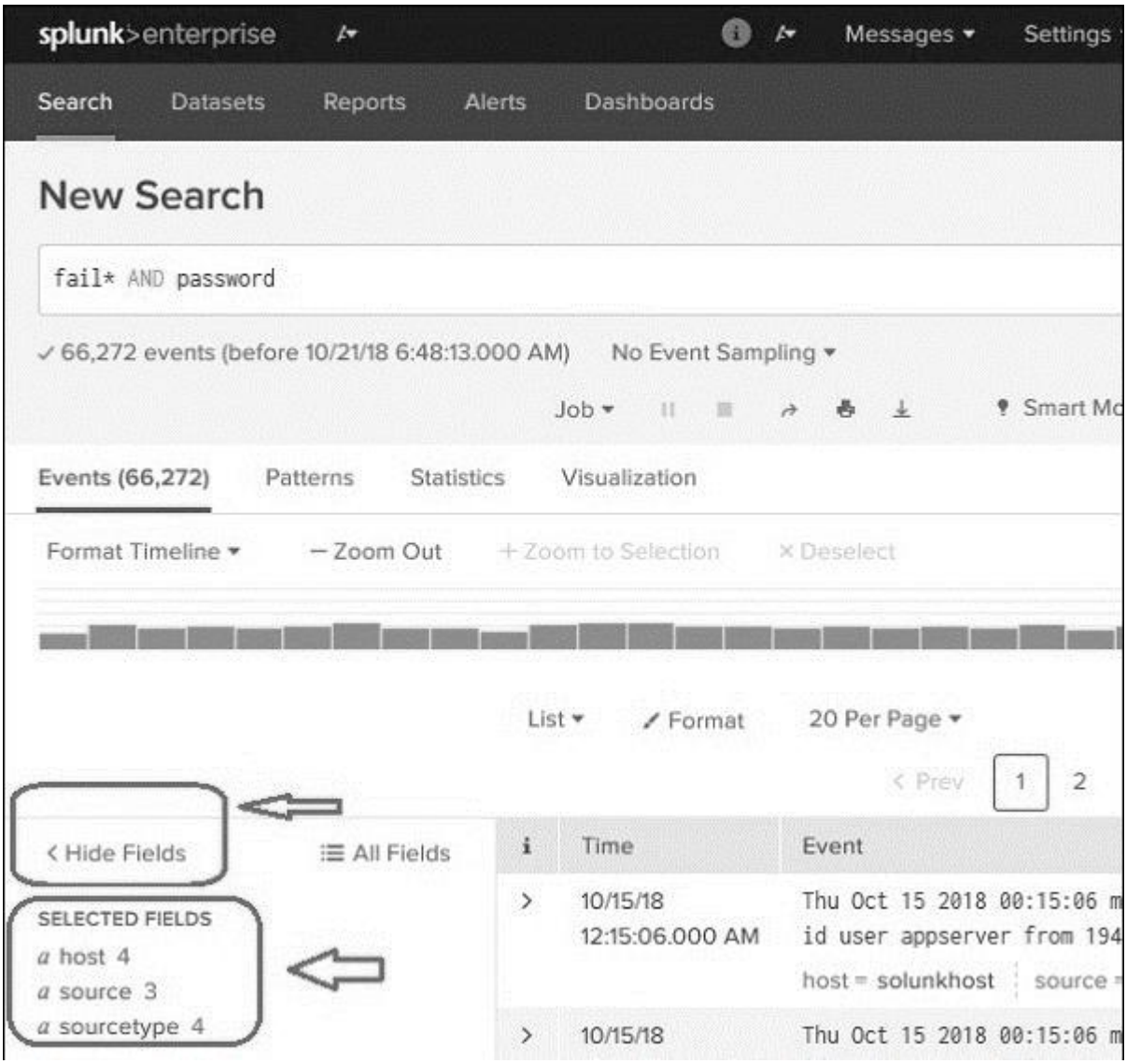

Рисунок 1.6 – Відображення полів даних завантаженого файлу

Навіть у разі неструктурованих даних Splunk намагається розділити поля на значення ключа. об’єднувати або розділяти їх на основі типів даних, які вони мають, числових та стрічкових тощо. Це здійснюється за допомогою елементів керування, показаних на рисунку 1.6.

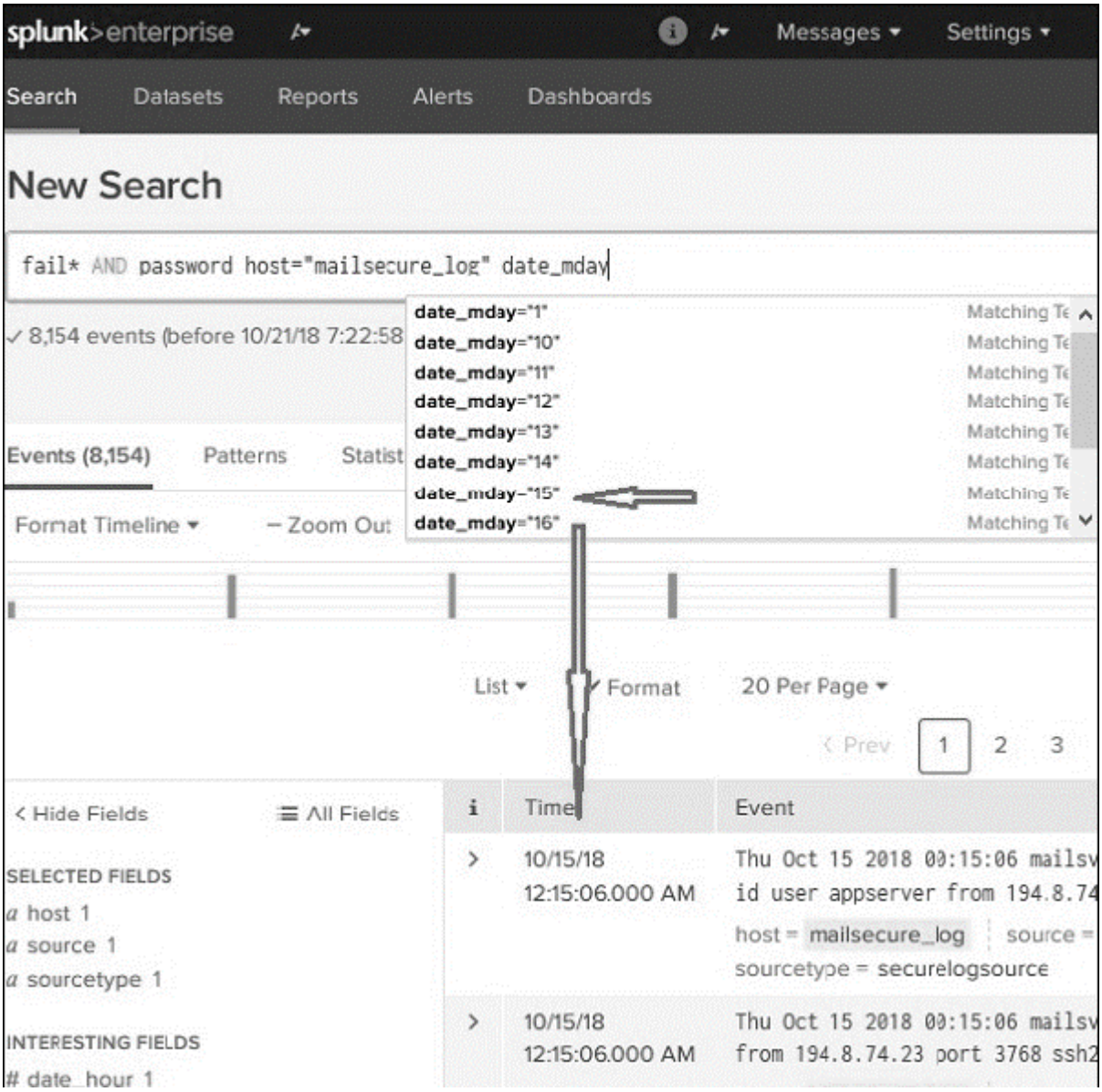

Рисунок 1.7 – Використання назви поля в якості параметра пошуку

Ми можемо вибрати, які поля відображати, вибираючи або знімаючи вибір полів зі списку. При натисканні на всі поля відкривається вікно зі списком усіх полів. Ми можемо використовувати прапорці, щоб вибрати поля для відображення. Окрім назви поля, воно відображає кількість різних значень, які мають поля, тип даних та відсоток подій, у яких це поле міститься. Дуже детальна статистика для кожного вибраного поля стає доступною після натискання по назві поля. Вона показує всі різні значення для поля, їх кількість та їх відсотки.

Назви полів також можна вставити у вікно пошуку разом із конкретними значеннями для пошуку. У наведеному нижче прикладі ми хочемо знайти всі записи для дати 15 жовтня для хоста з ім’ям mailsecure_log. Ми отримуємо результат на цю конкретну дату (див. рис. 1.7).

Веб-інтерфейс Splunk відображає часову шкалу, яка вказує на розподіл подій за певний діапазон часу. Існують попередньо встановлені часові інтервали, з яких ви можете вибрати певний часовий діапазон, або ви можете налаштувати часовий діапазон відповідно до ваших потреб.

Вибір будь-якого з цих параметрів призведе до отримання даних лише за певний період часу, який ви також можете проаналізувати далі, використовуючи доступні спеціальні параметри шкали часу (див. рис. 1.8). Натискаючи та перетягуючи смуги на часовій шкалі, ми можемо вибрати підмножину результату, який уже існує. Це не призводить до повторного виконання запиту. Він фільтрує лише записи з наявного набору.

Дві команди (earliest та latest) можна використовувати в рядку пошуку, щоб вказати діапазон часу, між яким треба відфільтрувати результати. Це подібне до вибору підмножини часу, але здійснюється за допомогою команд, а не натискання на певній панелі стрічки часу. Таким чином, це забезпечує кращий контроль над діапазоном даних, який ви можете вибрати для свого аналізу.

Ми також можемо знайти найближчі події певного часу, вказавши, наскільки ми хочемо, щоб події були відфільтровані. У нас є можливість вибору масштабу інтервалу, наприклад – секунди, хвилини, дні, тиждень тощо.

Під час виконання пошукового запиту результат зберігається як завдання на сервері Splunk. Хоча це завдання було створено одним конкретним користувачем, ним можна поділитися з іншими користувачами, щоб вони могли почати використовувати цей набір результатів без необхідності знову створювати для нього запит. Результати також можна експортувати та зберегти

як файли, якими можна поділитися з користувачами, які не використовують Splunk.

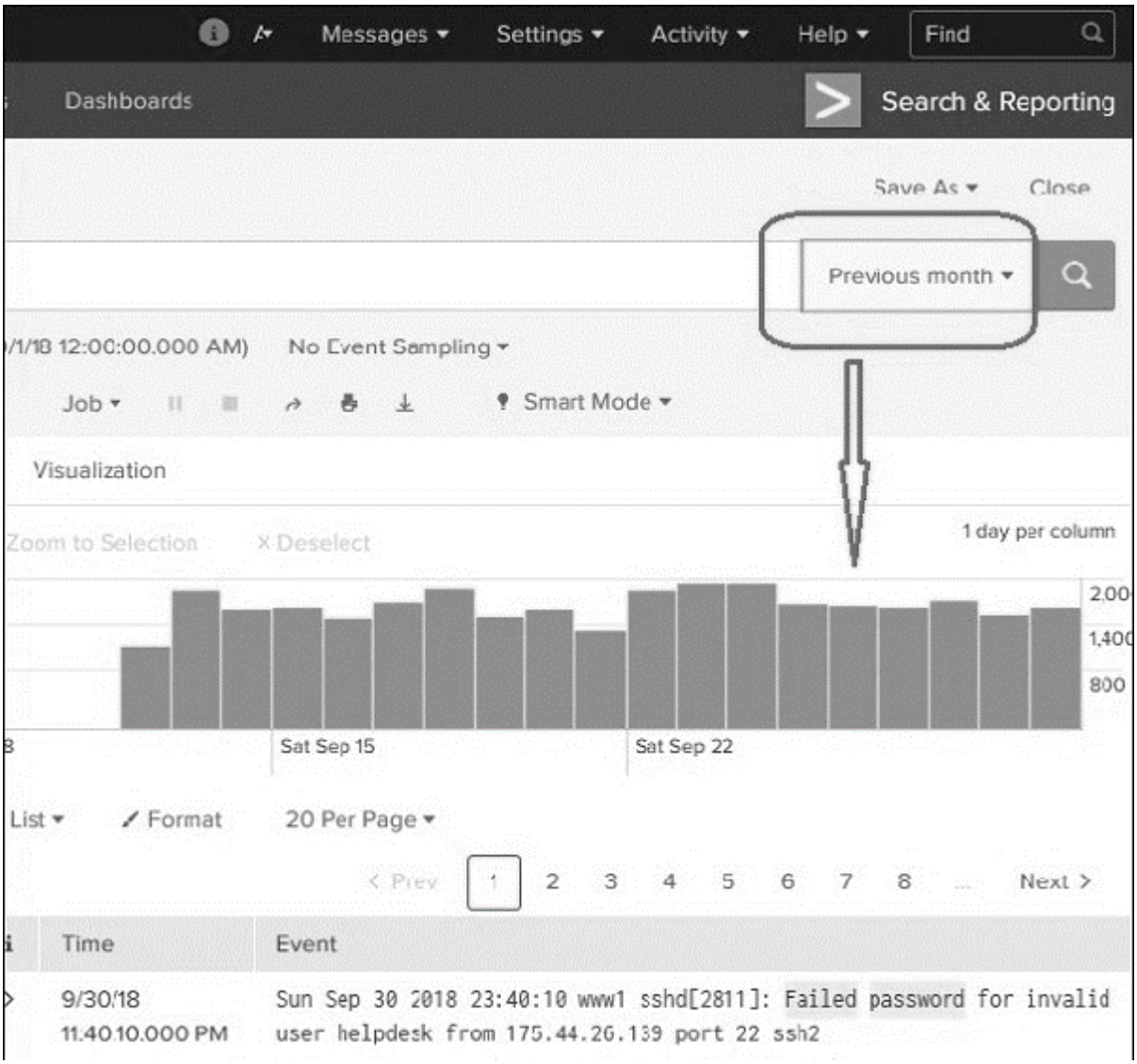

Рисунок 1.8 – Керування часовими діапазонами при пошуку

Поширення результатів пошук у здійснюється через URL-адресу, за якою можна отримати доступ до запиту та результату. Необхідно надати дозвіл користувачам, які будуть використовувати це посилання. Дозвіл надається через інтерфейс адміністрування Splunk. Завдання, збережені для використання всіма користувачами з відповідними дозволами, можна отримати, шукаючи посилання на результати виконання запиту в меню активності у верхньому правому рядку інтерфейсу Splunk. Після натискання вищезгаданого посилання

ми отримаємо список усіх збережених завдань, як показано нижче на рисунку 1.9.

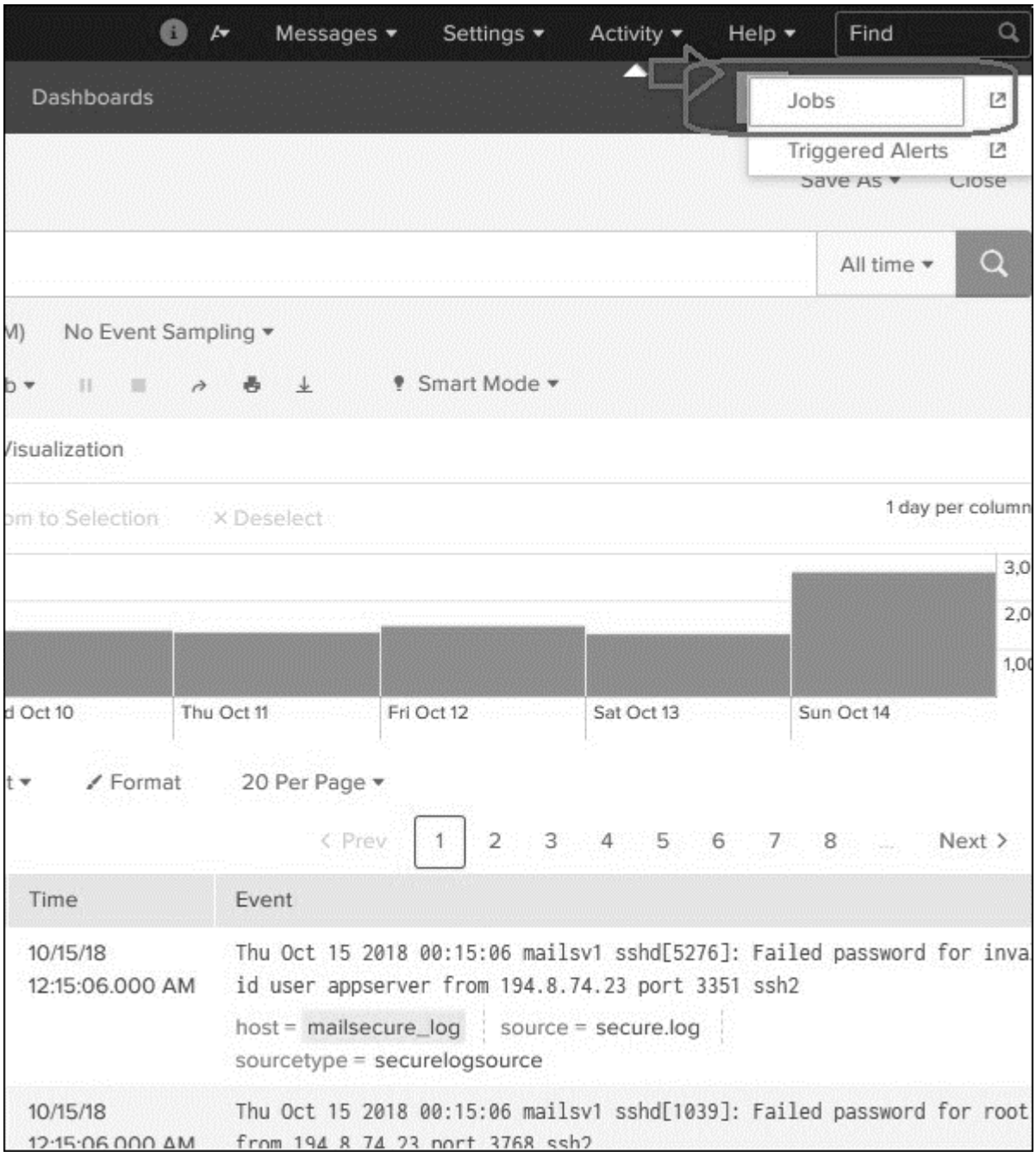

Рисунок 1.9 – Список збережених завдань у Splunk

Він, слід зазначити, містить сповіщення про дату закінчення терміну дії, коли збережена робота буде автоматично видалена зі Splunk. Ви можете змінити цю дату, вибравши роботу та натиснувши «Редагувати вибране», а потім вибравши «Продовжити термін дії».

1.4 Мова обробки пошуку Splunk

Мова обробки пошуку Splunk (SPL – Search Processing Language) – це мова, що містить багато команд, функцій, аргументів тощо для отримання бажаних результатів із наборів даних. Наприклад, коли ви отримуєте набір результатів для пошукового терміну, ви можете додатково відфільтрувати деякі більш конкретні терміни з набору результатів. Для цього вам потрібно додати кілька додаткових команд до наявної команди. Це досягається шляхом вивчення використання SPL.

SPL має наступні компоненти.

– Пошукові терміни – це ключові слова або фрази, які ви шукаєте.

– Команди – дія, яку ви хочете виконати з набором результатів, наприклад форматувати результат або підрахувати їх.

– Функції – які обчислення ви збираєтеся застосувати до результатів. Як сума, середнє тощо.

– Спеціальні опції – як згрупувати або перейменувати поля в наборі результатів.

Обговоримо всі компоненти за допомогою зображень у розділі нижче −

Пошукові терміни – це терміни, які вказуються в рядку пошуку, щоб отримати певні записи з набору даних, які відповідають критеріям пошуку.

Команди SPL використовуються, щоб спростити процес аналізу у наборі даних. У наведеному нижче прикладі (рис. 1.10) ми використовуємо команду head, щоб відфільтрувати лише 3 найпопулярніші результати пошукової операції.

```
host="mailsecure_log" | head 3
```

Рисунок 1.10 – Стрічка пошуку з використанням команди head

Поряд з командами, Splunk також надає багато вбудованих функцій, які можуть приймати вхідні дані з поля, що аналізується, і видавати результат після застосування обчислень до цього поля. Наприклад, функція Stats avg() повертає середнє арифметичне.

Коли ми хочемо отримати результати, згруповані за певним полем, або ми хочемо перейменувати поле у виводі, ми використовуємо спеціальні фрази group by і as відповідно.

1.5 Пошукова оптимізація у Splunk

Splunk вже включає функції оптимізації, аналізує та обробляє пошуки для максимальної ефективності. Ця ефективність в основному досягається завдяки наступним двом цілям оптимізації.

Рання фільтрація – ці оптимізації фільтрують результати дуже рано, щоб кількість оброблюваних даних скоротилася якомога раніше під час процесу пошуку. Цей ранній фільтр дозволяє уникнути непотрібних розрахунків пошуку та оцінки подій, які не є частиною кінцевих результатів пошуку.

Паралельна обробка – вбудовані оптимізації можуть змінювати порядок обробки пошуку, щоб якомога більше команд виконувалося паралельно в індексаторах перед відправкою результатів пошуку в заголовок пошуку для остаточної обробки.

Splunk надає інструменти для аналізу того, як працює пошукова оптимізація. Ці інструменти допомагають зрозуміти, як використовуються умови фільтра та яка послідовність цих кроків оптимізації. Він також дає нам вартість різних кроків, залучених до пошукових операцій.

Розглянемо операцію пошуку, щоб знайти події, які містять слова: fail, failed або password. Коли ми розміщуємо цей пошуковий запит у вікні пошуку, вбудовані оптимізатори діють автоматично, щоб визначити шлях пошуку. Ми можемо перевірити, скільки часу знадобилося на пошук певної кількості

результатів, і, якщо потрібно, можемо перевіряти кожен крок оптимізації разом із пов’язаними з ним накладними затратами.

Ми йдемо пунктами меню Search → Job → Inspect Job, щоб отримати ці деталі, як показано нижче на рисунку 1.11.

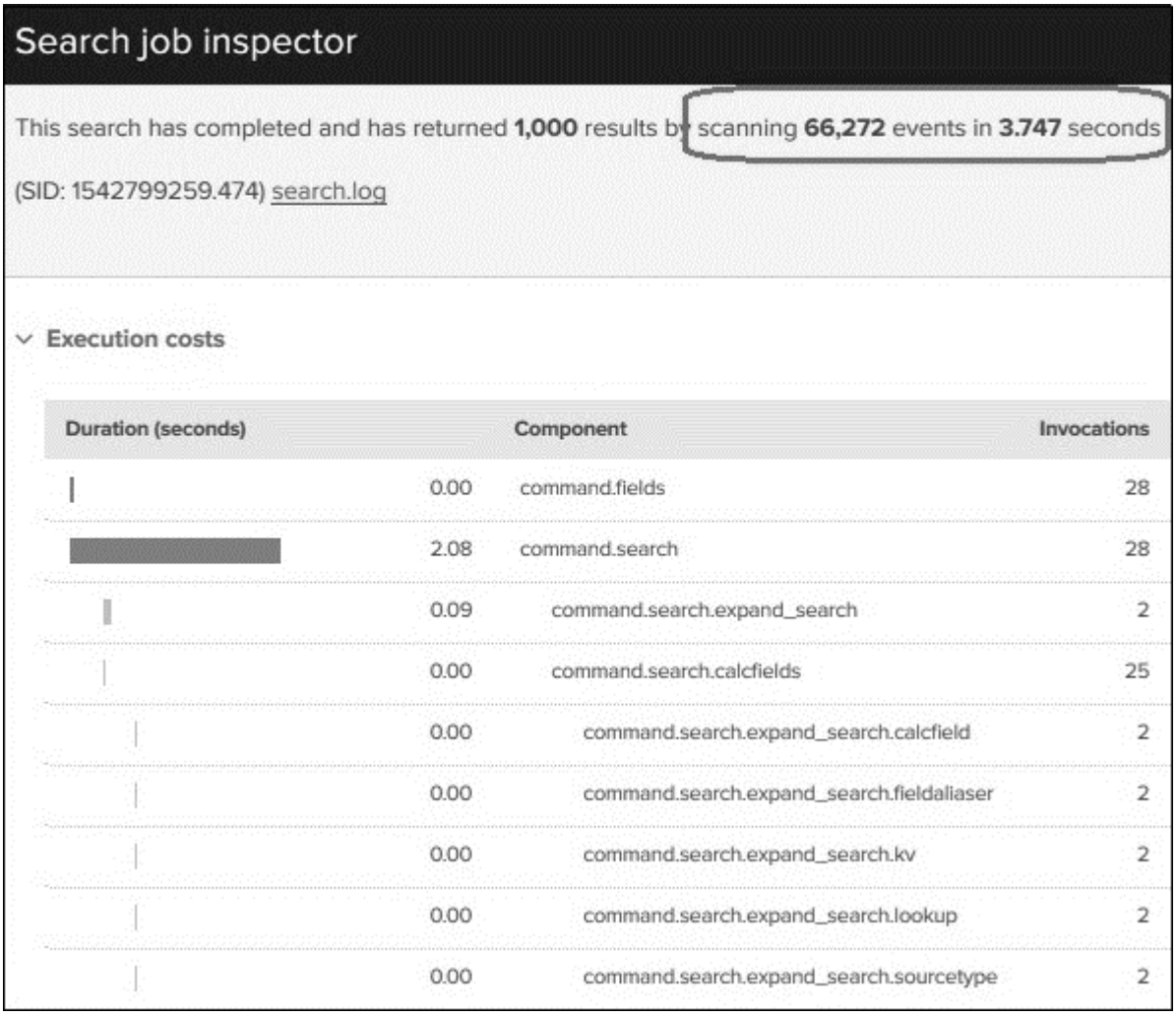

Рисунок 1.11 – Відображення параметрів оптимізації

Ми також можемо вимкнути вбудовану оптимізацію і помітити різницю в часі, необхідному для результату пошуку. Результат може бути кращим, а може і не бути кращим, ніж вбудований пошук. Якщо це краще, ми завжди можемо вибрати цю опцію, щоб вимкнути оптимізацію лише для цього конкретного пошуку.

РОЗДІЛ 2. ОПРАЦЮВАННЯ ДАНИХ В SPLUNK

2.1 Команди перетворення даних в Splunk

в Splunk наявні команди, які використовуються для перетворення результату пошуку в такі структури даних, які будуть корисними для представлення статистики та візуалізації даних.

Нижче наведено кілька прикладів команд перетворення.

Highlight — щоб виділити конкретні терміни в результаті.

Chart — щоб створити діаграму з результатів пошуку.

Stats — для створення статистичних підсумків із результатів пошуку.

Команда Highlight використовується для виділення певних термінів у наборі результатах пошуку. Вона використовується для надання пошукових термінів як аргументів функції виділення. Кілька термінів пошуку вводяться, розділяючи їх комами.

У наведеному нижче прикладі (див. рис. 2.1) ми шукаємо терміни, safari та butter в наборі результатів.

```
host="web_application" | highlight Safari, butter
```

Рисунок 2.1 – Використання команди highlight

Команда chart – це команда перетворення, яка повертає результати у форматі таблиці. Результати можуть бути використані для відображення даних у вигляді діаграми, наприклад стовпчикової діаграми, лінійного графіка, області тощо. У наведеному нижче прикладі (див. рис. 2.2) ми створюємо горизонтальну гістограму, накреслюючи середній розмір байтів для кожного типу файлів.

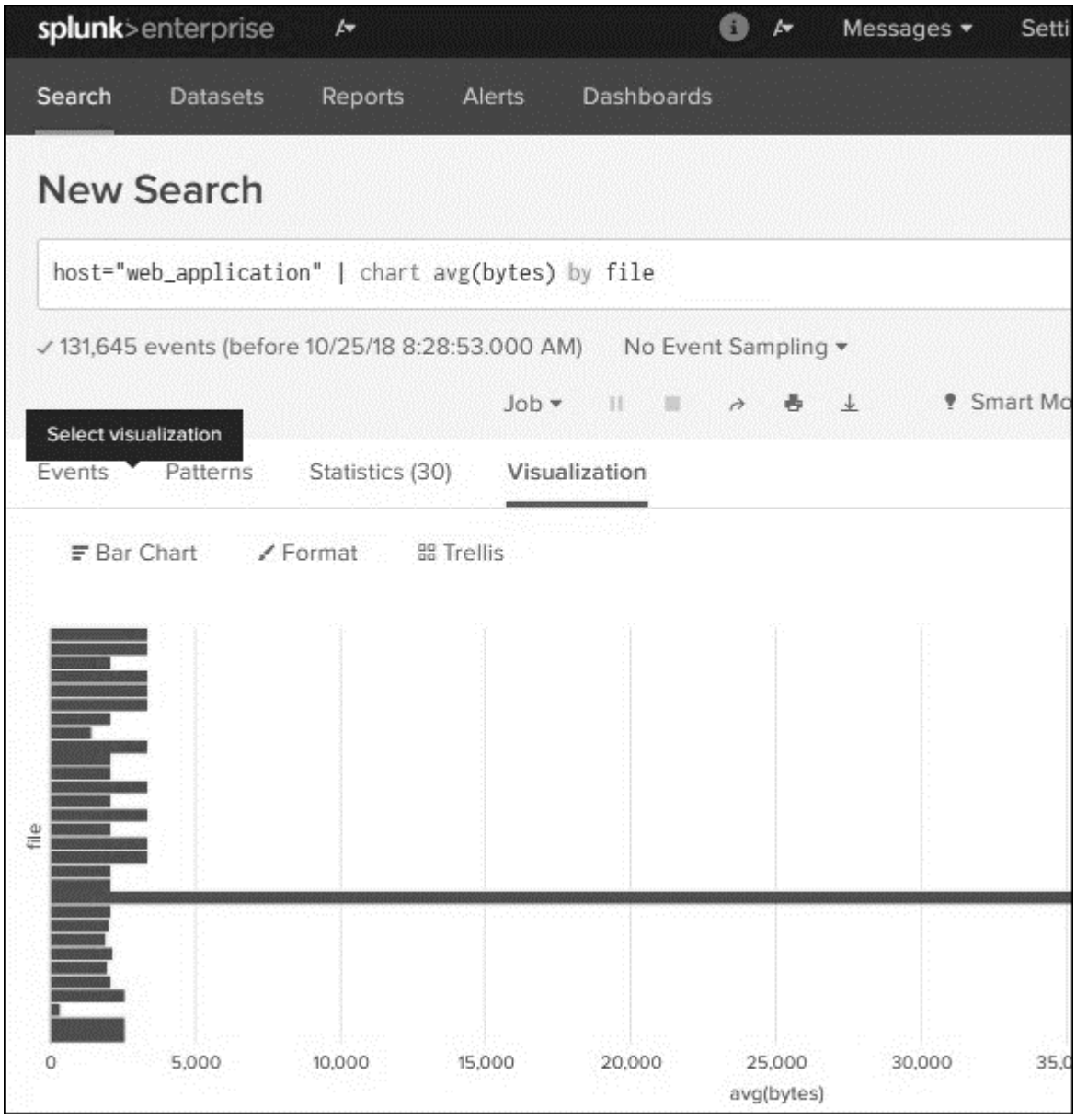

Рисунок 2.2 – Приклад використання команди chart

Команда Stats перетворює набір даних результатів пошуку в різні статистичні представлення залежно від типів аргументів, які ми надаємо для цієї команди.

У наведеному нижче прикладі ми використовуємо команду stats з функцією count, яка потім групується іншим полем (див. рис. 2.3).

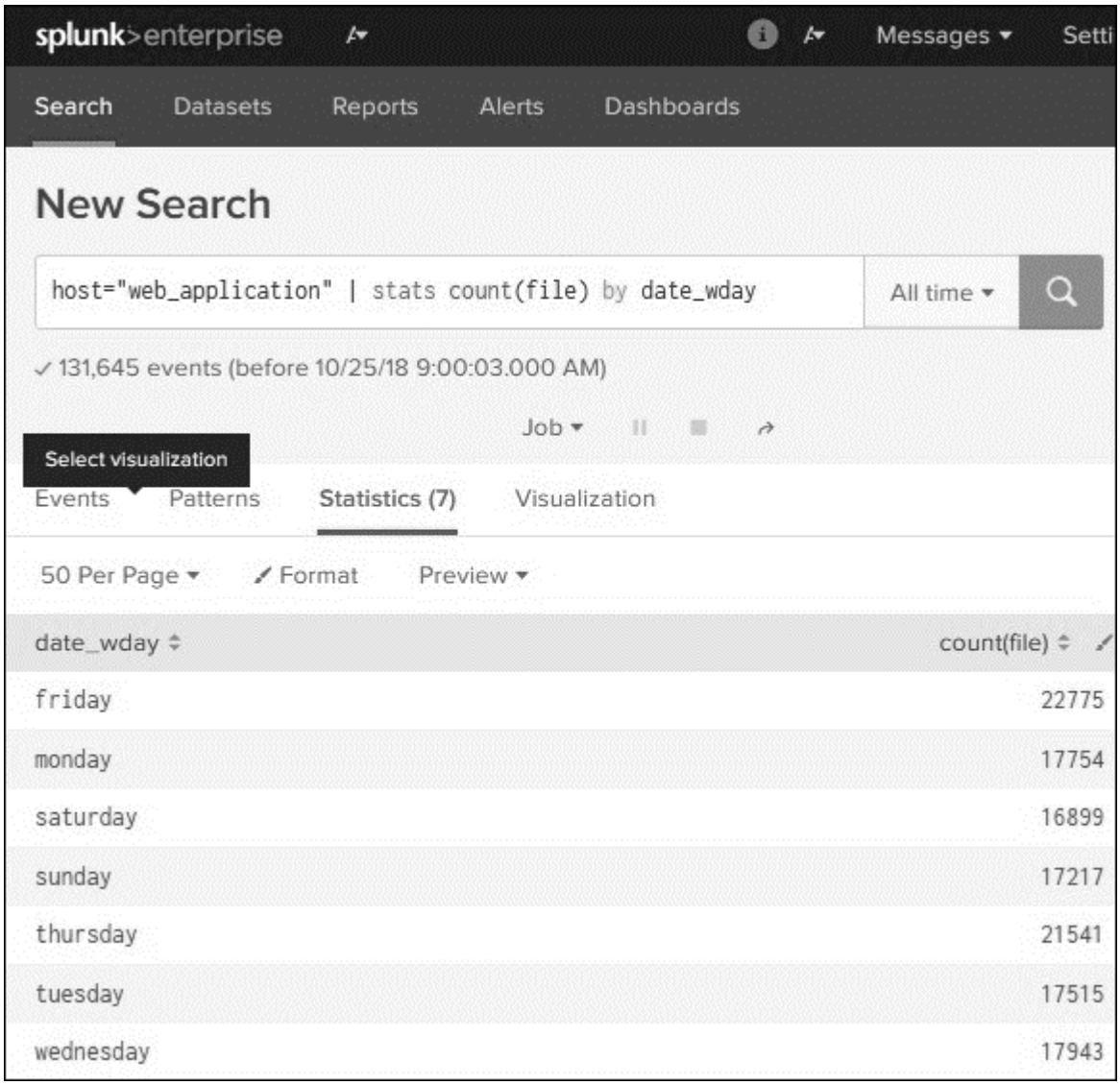

Рисунок 2.3 – Приклад використання команди stats

Тут ми підраховуємо кількість імен файлів, створених у кожен день тижня. Результат рядка пошуку виходить у вигляді таблиці з рядками, створеними для кожного дня.

2.2 Створення звітів у Splunk

Звіти Splunk – це результати, збережені в результаті пошукової дії, яка може показувати статистику та візуалізацію подій. Звіти можна запускати в будь-який час, і вони отримують нові результати кожного разу. Звітами можна ділитися з іншими користувачами та додавати їх на інформаційні панелі. Більш

складні звіти можуть містити функції деталізації, щоби побачити основні події, які створюють остаточну статистику.

У цьому розділі ми побачимо, як створити та відредагувати зразок звіту.

Створення звіту – це простий процес, у якому ми використовуємо параметр «Save as», щоб зберегти результат операції пошуку, вибравши параметр RepSave Asorts. На схемі на рисунку 2.4 показано цей варіант.

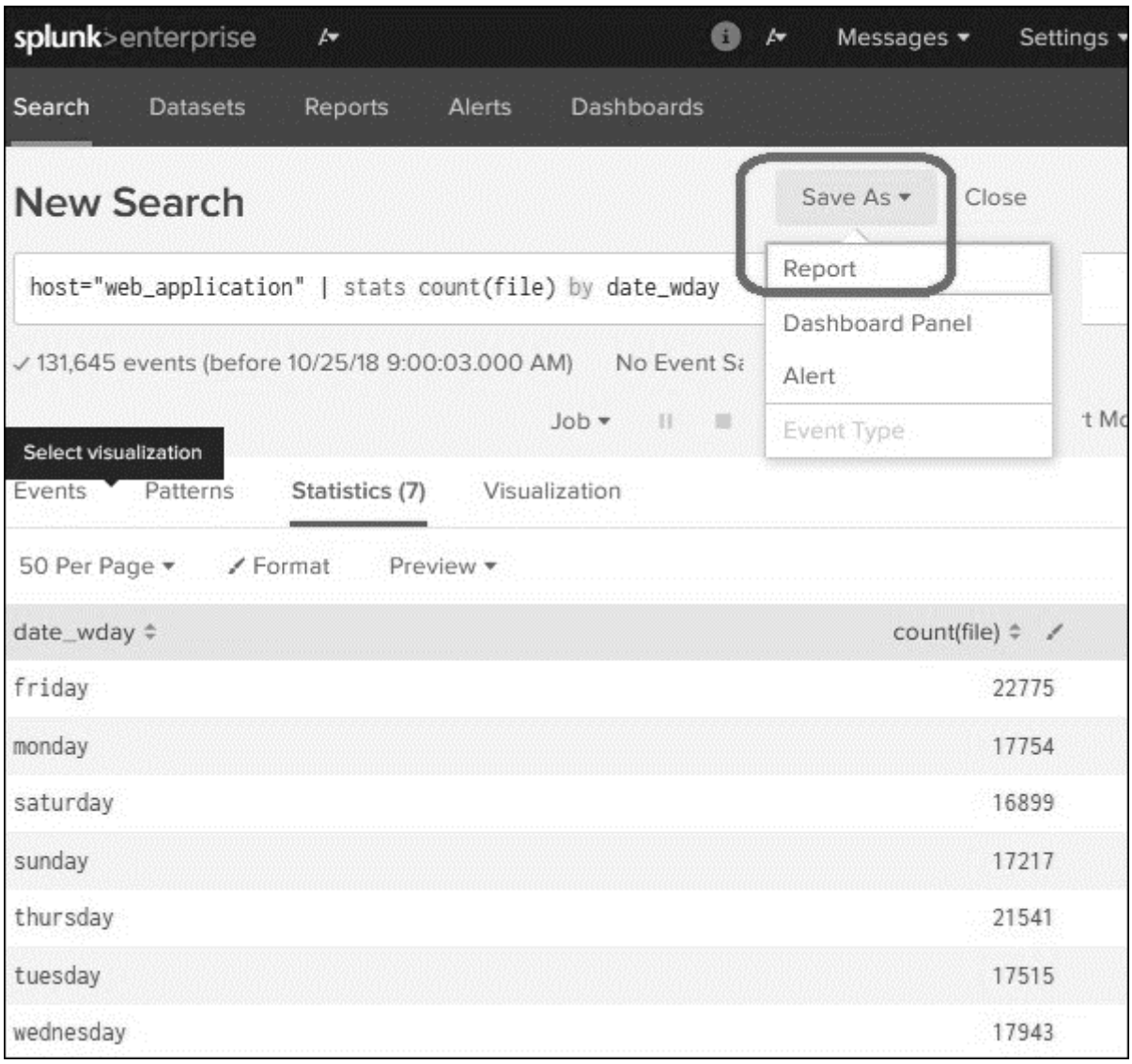

Рисунок 2.4 – Створення звіту

Натиснувши опцію «Reports» у спадному меню, ми отримаємо наступне вікно, яке вимагає ввести додаткові дані, як-от назва звіту, опис та вибір засобу вибору часу. Якщо ми виберемо засіб вибору часу, він дає змогу коригувати

часовий діапазон під час запуску звіту. Після натискання кнопки «Save», щоб створити звіт у наведеному вище кроці, ми отримаємо екран із запитом налаштувати звіт. Тут ми можемо налаштувати дозволи, планувати звіт тощо. Ми також отримуємо можливість перейти до наступного кроку та додати звіт на інформаційну панель. Якщо далі натиснути «View», ми зможемо побачити звіт у вигляді, якого він набуде після створення.

Хоча ми можемо редагувати дозволи, розклад тощо, іноді нам потрібно змінити вихідний рядок пошуку. Це можна зробити, вибравши параметр «Open in Search». Це знову відкриє вихідний варіант пошуку, який ми можемо змінити на новий пошук.

2.3 Інформаційні панелі у Splunk

Інформаційна панель використовується для представлення таблиць або діаграм, які мають цінність для бізнесу. Робиться це за допомогою панелей. Панелі на інформаційній панелі містять діаграму або зведені дані у візуально привабливому вигляді. Ми можемо додати кілька панелей, а отже, і кілька звітів і діаграм на одну інформаційну панель.

Щоб розмістити діаграму на інформаційній панелі, ми можемо вибрати опцію Save As → Dashboard Panel, як показано нижче на рисунку 2.5. Ми можемо додати інші елементи, наприклад, ще одну діаграму на інформаційну панель.

2.4 Набори даних та зведені таблиці

Splunk може приймати різні типи джерел даних і створювати таблиці, подібні до реляційних таблиць. Вони називаються табличними наборами даних або просто таблицями. Вони забезпечують прості способи аналізу та фільтрації даних, пошуку тощо. Ці табличні набори даних також використовуються для виконання аналізу з використанням зведених таблиць.

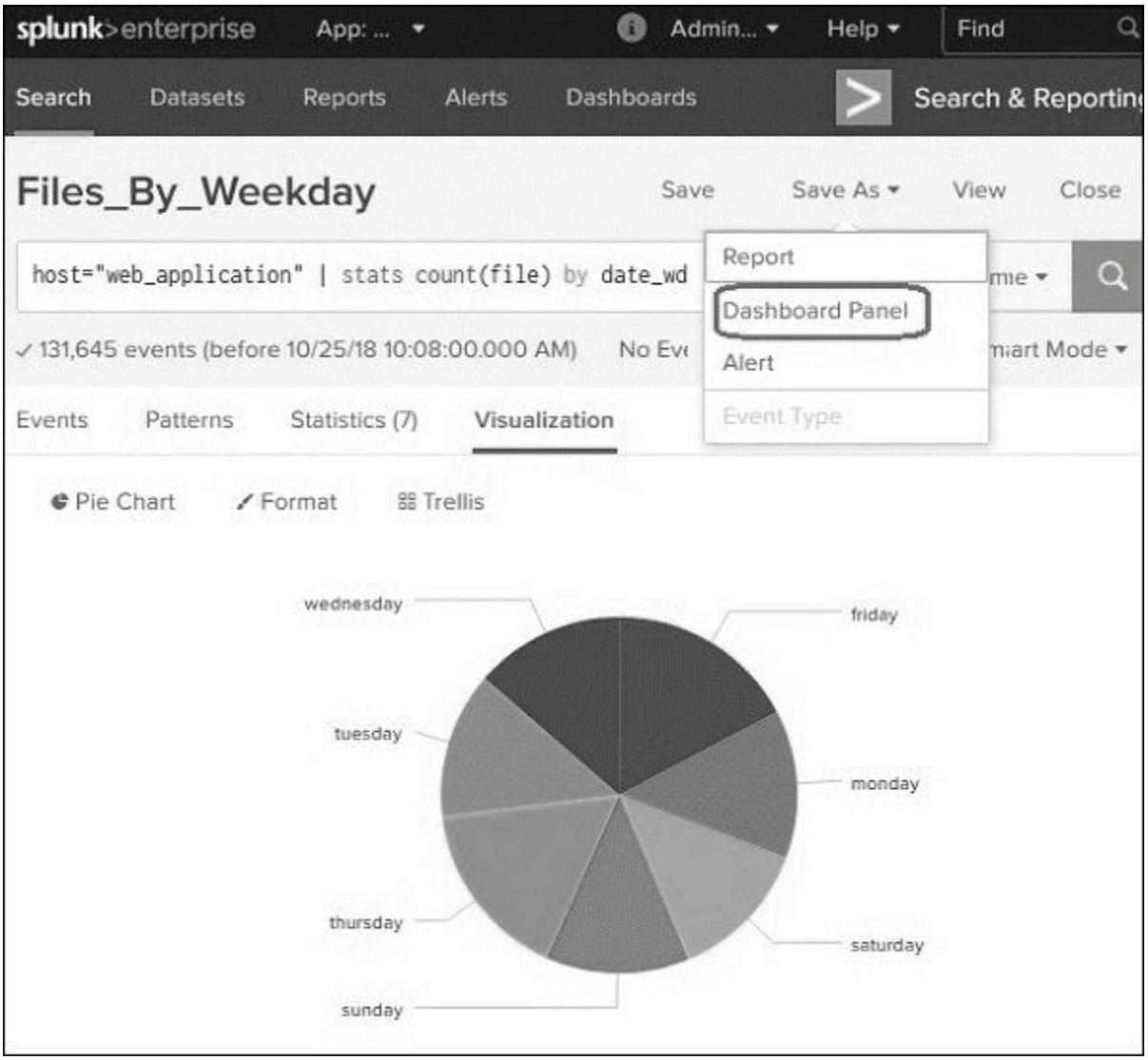

Рисунок 2.5 – Формування інформаційної панелі

Для створення наборів даних і керування ними ми використовуємо надбудову Splunk під назвою Splunk Datasets Add-on. Його можна завантажити з веб-сайту Splunk. Після успішної інсталяції ми бачимо кнопку «Create New Table Dataset» (див. рис. 2.6).

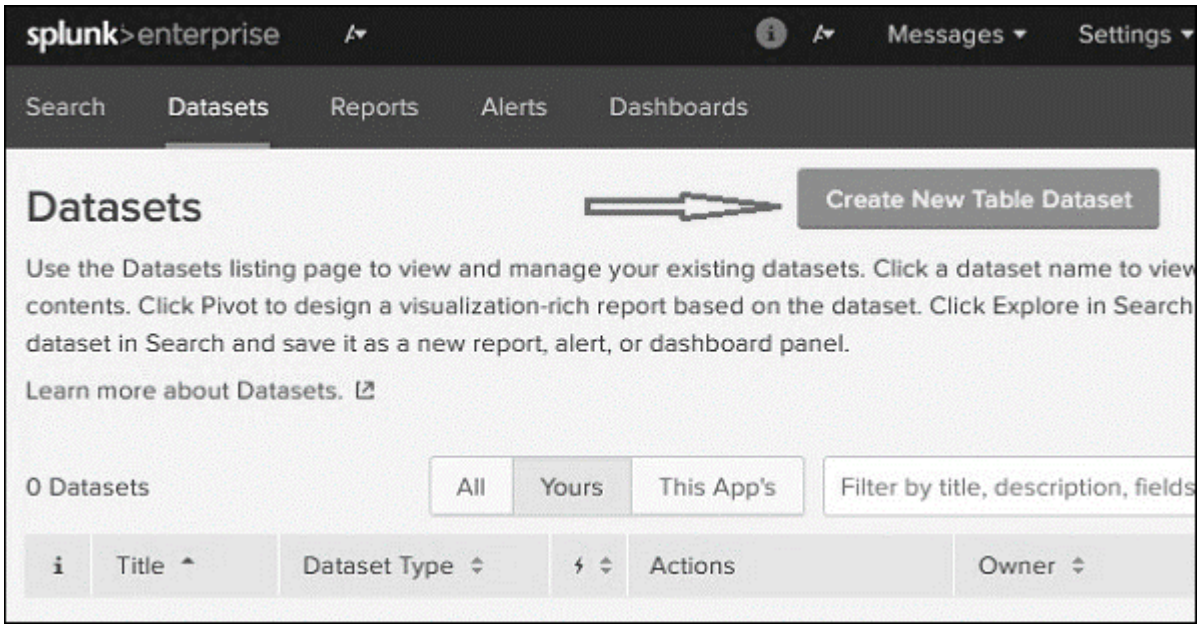

Рисунок 2.6 – Створення табличного набору даних

Далі натисканням кнопки «Create New Table Dataset» отримуємо можливість вибрати один із трьох нижченаведених варіантів.

Indexes and Source Types – виберіть із існуючого індексу або типу джерела, які вже додано до Splunk через інструмент Add data.

Existing Datasets – можливо, вже є створений деякий набір даних раніше, який є потреба змінити, створивши з нього новий набір даних.

Search – потрібно створити пошуковий запит і його результат можна використовувати для створення нового набору даних.

Далі нам надається можливість вибрати різні поля, які ми хочемо помістити в табличний набір даних. Поле _time вибирається за замовчуванням, і це поле не можна скинути. Ми отримуємо остаточний табличний набір даних з усіма вибраними полями. Тепер набір даних став схожим на реляційну таблицю. Зберігаємо набір даних натисканням «Save as».

2.5 Створення зведеної таблиці

Описані вище набори даних використовуються для створення зведеного звіту. Зведений звіт (таблиця) відображає сукупність значень одного стовпця

щодо значень іншого стовпця. Іншими словами, значення одного стовпця перетворюються в рядки, а значення інших стовпців перетворюються на стовпці.

Щоб досягти цього, ми спочатку вибираємо набір даних за допомогою вкладки набору даних, а потім вибираємо параметр «Visualize with Pivot» у стовпці «Actions» для цього набору даних. Далі вибираємо відповідні поля для створення зведеної таблиці. Далі ми можемо зберегти зведену таблицю як звіт або панель на існуючій інформаційній панелі для подальшого використання.

2.6 Створення подій в наборі даних для опрацювання

У пошуку Splunk ми можемо створювати власні події в наборі даних на основі певних критеріїв. Наприклад, ми шукаємо лише події, які мають код статусу http 200. Цю подію тепер можна зберегти як тип події з визначеним користувачем ім’ям як status200 і використовувати це ім’я події як частину майбутніх пошуків.

Інакше кажучи, тип події являє собою пошук, який повертає певний тип події або корисну колекцію подій. Кожна подія, яку може повернути пошук, отримує асоціацію з цим типом події.

Існує два способи створити тип події після того, як ми визначили критерії пошуку. Один із них – запустити пошук, а потім зберегти його як тип події. Іншим є додати новий тип події на вкладці налаштувань. У цьому розділі ми побачимо обидва способи його створення.

Розглянемо пошук подій, для яких критерій успішного http статусу дорівнює 200, а тип події виконується в середу. Після виконання пошукового запиту ми можемо вибрати параметр Save as, щоб зберегти запит як тип події (див. рис. 2.7).

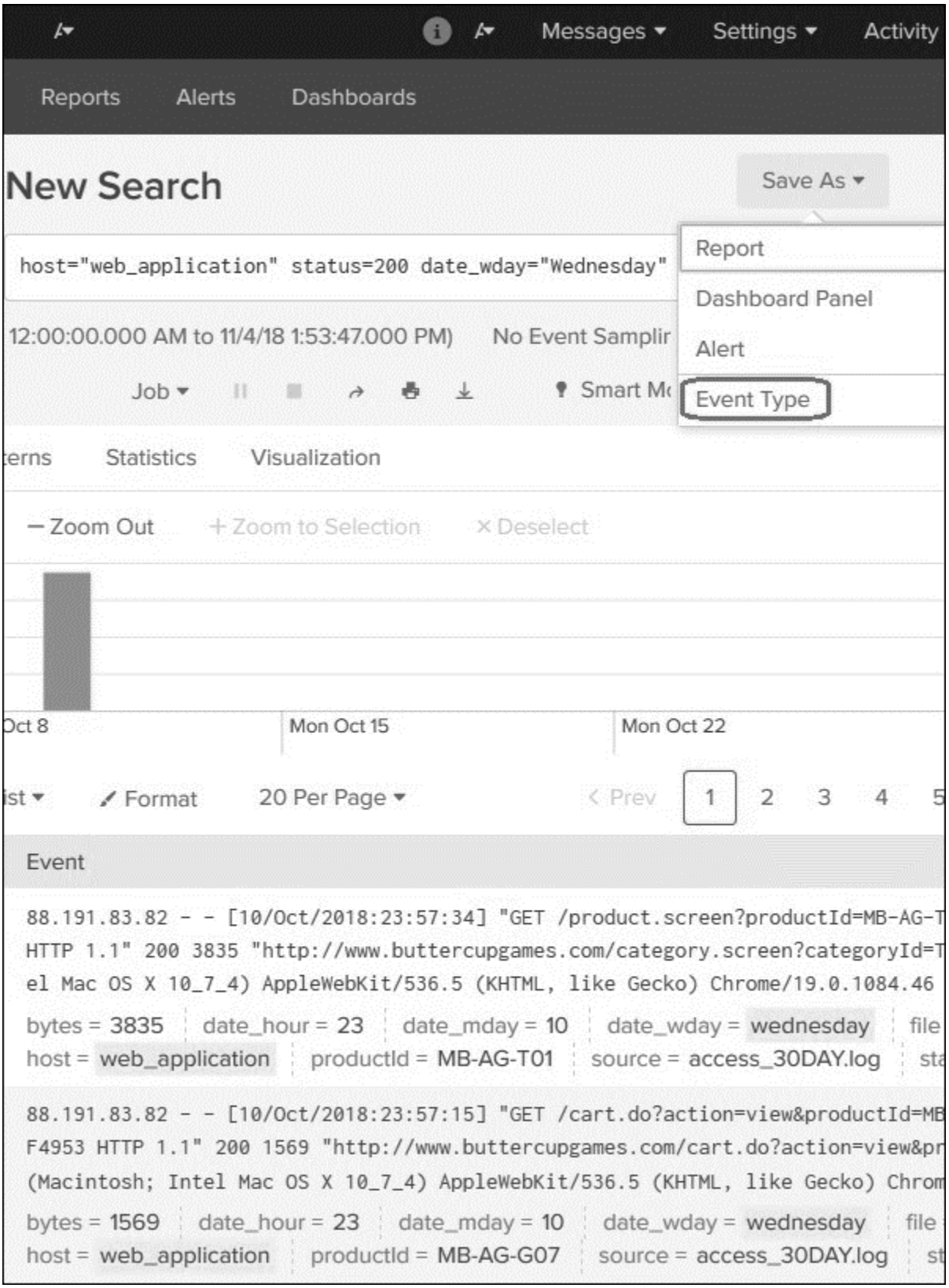

Рисунок 2.7 – Створення типу події на основі результатів пошуку

На наступному екрані буде запропоновано дати назву типу події, вибрати необов’язковий тег, а потім вибрати колір, яким будуть виділені події. Параметр

пріоритету визначає, який тип події буде відображатися першим, якщо два або більше типів подій відповідають одній події. Таким чином усі типи подій будуть доступні через пункт меню Settings → Event Types.

Ще один спосіб створення типу події є використання безпосередньо діалогового вікна для цього, доступного на екрані із списком типів подій. Тут потрібно буде ввести усі реквізити типу події (назва, теги тощо і запит пошуку.

Для використання події з метою отримання результатів пошуку досить створити пошуковий запит, який міститиме ім’я цього типу події.

2.7 Приклади використання запитів Splunk для моніторингу системи

2.7.1 Виявлення атак грубої сили (Brute Force)

Атака Brute Force є фактично набором з кількох спроб входу з використанням багатьох паролів неавторизованого користувача/зловмисника з надією в кінцевому підсумку вгадати правильний пароль. Загальний синтаксис виявлення такого типу атак та конкретні реалізації для ОС Windows та Linux показано на лістингах 2.1 – 2.3

Лістинг 2.1 – Загальний синтаксис виявлення атаки

```
index=__your_sysmon_index__ sourcetype=winxsecurity user=* user!""
| stats count(eval(action="success")) as successes count(eval(action="failure"))
as failures by user, ComputerName
| where successes>0 AND failures>100
```

Лістинг 2.2 – Синтаксис виявлення атаки Brute Force для ОС Windows

```
index=windows source="WinEventLog:Security" EventCode=4625
| bin _time span=5m
| stats count by _time,user,host,src,action
| where count >= 5
```

Лістинг 2.3 – Синтаксис виявлення атаки Brute Force для ОС Linux

```
index=linux source="/var/log/auth.log" "Failed password"
| bin _time span=5m
| stats count by _time,user,host,src,action
| where count >= 5
```

2.7.2 Моніторинг системної папки Windows32

Спроба запису файлу командного пакету batch в системну папку Windows32 може бути виявлена за допомогою запиту, зображеного на лістингу 2.4.

Лістинг 2.4 – Спроба запису файлу командного пакету batch в системну папку Windows32

```
| tstats count min(_time) as firstTime max(_time) as lastTime values
(Filesystem.dest) as dest values (Filesystem.file_name) as file_name values
(Filesystem.user) as user from datamodel=Endpoint.Filesystem by
Filesystem.file_path   | rex field=file_name "(?<file_extension>\.[^\.]+)$" |
search file_path=*system32* AND file_extension=.bat
```

Хоча пакетні файли за своєю суттю не є шкідливими, їх нерідко можна побачити після встановлення ОС, особливо в каталозі Windows. Ця аналітика шукає підозрілу активність пакетного файлу, який створюється в дереві каталогів C:\Windows\System32. Через дії адміністратора помилкові спрацьовування будуть виникати лише іноді.

РОЗДІЛ 3. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ХОРОНИ ПРАЦІ

3.1 Охорона праці та її актуальність в ІТ-сфері

Для підвищення ефективності системи управління охорони праці (СУОП) дуже важлива роль належить формуванню і розвитку інформаційної культури фахівців ІТ-технологій, яка впливає на удосконалення інформаційного контуру сучасних підприємств, дозволяє створювати надійні прогнози щодо стану умов праці, показників здоров'я та працездатності, виробничого травматизму і професійної захворюваності, визначати політику розвитку підприємств, установ та організацій на основі різноманітних стратегій охорони праці (інноваційні, маркетингові, інвестиційні, фінансові, технологічні, диверсифікаційні). Поряд з інформаційною культурою важливо використовувати в рамках СУОП «трикутник» її складових: правову, організаційну, управлінську.

В управлінні охороною праці потрібно реалізувати основні положення, окремі теоретико-методологічні підходи інформаційного менеджменту. Головну роль та відповідальність за стан СУОП мають нести фахівці служби охорони праці сучасного підприємства.

Сучасне суспільство називають постіндустріальним, постекономічним, інформаційним, оскільки йдеться про багатосторонні і кардинальні зміни у розвитку цивілізації.

Інформаційне суспільство передбачає докорінну зміну, яка полягає у перетворенні інформації і знань у головний професійно-виробничий потенціал особистості, соціуму і держави.

На постіндустріальному етапі розвитку суспільства вирішальним фактором стає інформація. Її домінування ініціювала науково-технічна революція, яку ще іменують інформаційною, оскільки нею охоплена будь-яка

інтелектуальна діяльність, починаючи з інформаційних образів штучного інтелекту у нових технологіях, економіки, і продовжуючи інформатизацією суспільства в умова світової глобалізації науки й освіти тощо.

Інформаційні технології розглядаються як потужний важіль економічного зростання України. Для цього необхідні значні стратегічні інвестиції у комп'ютерну та комунікаційну інфраструктуру, програми досліджень і розробок, освітню галузь [7].

Під інформаційною культурою розуміють сукупність, складову НІТ (новітні інформаційні технології), технологічну, правову, психологічну, соціологічну та ергономічну підсистеми, що сприяють спрямованому впливу на протікання соціальних процесів у суспільстві, колективі і вихованню свідомого відношення людини до праці, виконання прав та обов'язків [8].

Поняття інформаційної культури виникло в процесі активізації дослідницької уваги до механізмів інформаційного обміну у зв'язку зі значним підвищення ролі інформації в соціокультурних процесах суспільства, яке розглядають як інформаційне суспільство знань, де в центрі знаходяться інформаційні технології.

Робота з інформацією та інформаційна культура в цілому є одним з найважливіших компонентів спроб компанії управляти змінами. Є три принципові причини, в силу яких сьогодні необхідно дбати про інформаційну культуру компанії.

По-перше, вона все більше і більше стає найважливішою частиною загальної організаційної (корпоративної) культури компанії. Все більше компаній розуміють необхідність перетворень, орієнтованих на задоволення очікувань споживача. Щоб сьогодні впливати на майбутнє, потрібно уявляти собі на що вона буде схожа. А для цього потрібно працювати з різноманітною діловою, професійною, технологічною, соціальною, ринковою та політичною інформацією.

По-друге, інформаційні технології роблять можливим створення в компаніях комп'ютерних мереж, за допомогою яких йде спілкування між менеджерами, але важливо знати, як люди використовують цю інформацію. Саме по собі створення такої мережі з усіма її робочими станціями і мультимедійними можливостями не гарантує того, що інформація буде використовуватися більш розумно і більш ефективно.

По-третє, для різних функціональних служб, підрозділів та робочих груп сучасних підприємств в сфері охорони праці інформаційна культура різна, а це означає відмінність методологічних підходів до процесів усвідомлення, збору, організації, обробки, поширення і використання інформації. Тому багато менеджерів погодяться з тим, що корпоративна інформаційна культура важлива для вироблення різних стратегій охорони праці та запровадження відповідних заходів з її вдосконалення.

Для деяких галузей, таких як розробка програмного забезпечення, інформаційна культура є необхідною умовою виживання, тому що зміна технологій в розробці програмного забезпечення відбувається кожні 6-8 місяців, а інвестиції на підготовку персоналу і освоєння нової технології величезні і у великих компаніях варіюються від 1,5 до 2 млрд. доларів на рік [11].

Аналіз свідчить, що інформатизація та інтеграція комунікаційного простору України сприяє різкому підвищенню інформаційної та професійної компетентності, ділової активності, стимулюванню конкуренції, створенню інноваційних підприємств та організацій, нових робочих місць, зниженню витрат на утримання управлінського апарату [10].

Поряд із задачами і здобутками окреслилися негативи використання інформаційних технологій:

1) надмірне інформаційне навантаження, суть якого полягає у тому, що кількість корисної інформації, яка надходить до мережі, перевищує психофізіологічні можливості її сприйняття людиною;

2) велика кількість інформації, яка сприймається, але не є корисною для фахівців в даний момент;

3) інформаційний голод, причиною якого є саме надлишок інформації, викликаний інформаційним перенавантаженням;

4) «інформоманія» як хвороба людини, яка робить останню знеособленою, залежною від перебування в інформаційному просторі і роботи з комп'ютером і чому вона віддає перевагу, уникаючи «живого» спілкування з людьми;

5) поява «кіберспільнот», що за своїми соціокультурними характеристиками набагато ближчі до представників інших культур у глобальному інформаційному просторі, ніж до своєї етнонаціональної спільноти чи решти населення, не охопленого Інтернетом;

6) індивідуалізм і дегуманізація способу життя «мешканців» Інтернету – відсутність готовності ділитися своїми знаннями.

Слід розуміти, що комп'ютерні технології, а особливо їх мережі істотно впливають на життєдіяльність людини, припускаючи глобалізацію і технократизацію суспільства. Але в ще більшій мірі цей вплив поширюється безпосередньо на центральну нервову систему, яка звикає працювати в дуже інтенсивному режимі багатозадачності, де вже переважають не тривалі логічні роздуми, а інтуїтивно-реактивні ланцюжки розумових формулювань у зв'язку з величезним обсягом оброблюваної щодня інформації, кількість якої зростає за експоненціальною швидкістю. Виникає припущення, що саме збільшення обсягу інформації та прискорення її обробки людиною може згубно вплинути на розвиток розумових здібностей людини.

Аналіз продуктивності розумової праці в найбільших за чисельністю фахівців IT-фірм показав, що велике значення з точки зору впливу на її результати має організаційна (корпоративна) культура. В цьому напрямі влаштовуються різні тімбілдинги, заходи, тренінги для розвитку персоналу. Також кожен керівник повинен добре розуміти свого співробітника, що саме

для нього важливо, що його мотивує. Важливо відвести потрібну роль відповідному співробітнику, щоб він виконував ті завдання, які йому цікаві.

На подібних тренінгах в тому числі повинна розглядатися інформаційна культура працівника, в освоєнні, володінні, мотивуванні, застосуванні, перетворенні інформації із застосуванням сучасних інформаційних технологій і використанням цих умінь в навчанні з охорони праці і в подальшій професійній діяльності. Особливо вони будуть корисні, як доповнення до існуючих інструктажів з охорони праці на підприємстві, або як контроль психологічного стану та взаємовідносин у колективі.

Інформаційна культура як інтегративне утворення абсолютно не зводиться до розрізнених знань, вмінь та навичок роботи за комп'ютером. Вона передбачає інформативну спрямованість цілісної особистості, яка володіє мотивацією до застосування і засвоєння нових даних. Інформаційну культуру можна розглядати, як одну з граней особистісного розвитку промислових робітників. Це шлях універсалізації якостей людини.

Оволодіння інформаційною культурою сприяє реальному розумінню особистістю свого місця, себе і своєї ролі у виробничому колективі. Вона має сприяти формуванню нового покоління фахівців інформаційного суспільства, який повинен володіти наступними навичками: виділення релевантної, значущої інформації, диференціації вихідних даних, розробки інформативних критеріїв її оцінки інформації, вміло використовувати її в рамках СУОП.

Сьогодні продовжує діяти стратегічне правило «Можливості комп’ютерної техніки обмежені тільки нашими уявленнями» [9].

3.2 Шкідлива дія шуту та вібрації і захист від неї

Для запобігання шкідливої дії шуму і вібрації на організм працюючих проводяться технічні, організаційні і медикопрофілактичні заходи.

Одним з основних технічних заходів є зменшення при експлуатації та на стадії проектування, конструювання обладнання причин шуму і вібрації в

самому джерелі утворення. Досягають цього завдяки використанню раціональної конструкції обладнання, заміни ударної дії деталей і машин коливальною, з'єднання елементів гнучкими зв'язками, врівноважування обертових частин механізмів, заміни металевих деталей пластмасовими, забезпечення різних власних частот коливань механізму з частотою збуджуючої сили. Аеродинамічний шум може бути зменшений застосуванням глушників та повітропроводів зі змінним перерізом. Шум трансформаторів (електромагнітний шум) знижується, якщо застосувати листи заліза як складових осердя трансформатора з малою магнітострикцією, серцевини.

Якщо неможливо ізолювати чи знизити шум і вібрацію самого джерела, потрібно:

– ізолювати джерело шуму або вібрації від навколишнього середовища засобами вібро- та звукоізоляції

– раціонально планувати виробничі приміщення, що мають інтенсивні джерела шуму;

– збільшувати звукопоглинання внутрішніх поверхонь приміщення шляхом звукопоглинальних покриттів.

Принцип роботи звукоізоляційних екранів оснований на відбиванні звукової хвилі від різних екранів, стін, кожухів обладнання. Шумливі агрегати слід закривати звукоізоляційними кожухами з виводом назовні органів керування та контрольних приладів. Звукоізоляційні екрани виготовляють з металу, деревини, пластмаси та інших щільних матеріалів. Екрани зсередини покривають звукопоглинаючими матеріалами (скловатою пінополіуретаном), а по периметру кожуха – віброізоляційними підкладками (гума).

Вихідними даними для розрахунку параметрів необхідного екрану є спектр шуму, який необхідно ослабити, кількість екранів, через які проходить шум, їх площа, акустичні характеристики приміщення.

За розрахованими значеннями необхідної звукової ізоляційної здатності екрану підбирається матеріал конструкції й екрану.

Принцип звукопоглинання оснований на явищі трансформації коливальної енергії звуку в теплову через втрати при терті. Найбільші втрати при терті мають пористі, волокнисті і перфоровані матеріали: поролон, пемзолітові і деревоволокнисті плити тощо.

Енергія звукової хвилі переходить у теплову енергію, причому, ефект звукоізоляції збільшується з ростом частоти звукової хвилі. Звукопоглинаючими матеріалами оббивають стелі, стіни. Щоб одержати ефективну звукоізоляцію, найбільш доцільно застосовувати багатошарові огородження з м’якими прошарками (мінеральна вата).

Важливим технічним рішенням у забезпеченні виробничих умов є вдосконалення ручних віброінструментів. Для цього використовують віброгасіння, змінюють ударний вузол, проводять балансування частин, що обертаються.

Послаблення локальної вібрації і передачі вібрації на підлогу і сидіння досягається засобами віброізоляції і вібропоглинання, застосуванням пружинних і гумових амортизаторів, прокладок тощо. Для обмеження поширення вібрацій через ґрунт, між фундаментом і ґрунтом залишають повітряні проміжки, які називаються акустичними розривами.

В останні роки знаходять застосування динамічні віброгасники, в яких створюються вібрації, що співпадають по частоті і протилежні по фазі вібрації машини, коливання якої необхідно зменшити.

До організаційних заходів по боротьбі з шумом та вібрацією на виробництві відносяться: впровадження раціонального режиму праці і відпочинку, обмеження часу роботи при використанні ручного інструменту, який створює вібрацію.

Глушники звуку застосовуються для зменшення шуму аеродинамічних установок (вентиляторів, пневмоінструментів, газотурбінних, дизельних, компресорних установок). Вони поділяються на активні, які поглинають звукову енергію, що на них поступила, і реактивні, які відбивають цю енергію.

Потужні джерела шуму як правило розміщують в окремих приміщеннях, які віддалені від постійних робочих місць.

Ізоляційні кабіни або екрани застосовують як екрани робочих місць для зменшення зовнішніх шумів.

Якщо не вдається зменшити рівень шуму і вібрації на робочому місці до нормативних значень та необхідно використовувати засоби індивідуального захисту: рукавиці, взуття, навушники, м'які шоломи, які зменшують рівень звукового тиску на 40-50 дБ.

У процесі виробництв, експлуатації і зберігання радіоелектронних засобів можуть виникати механічні і динамічні дії, що характеризуються широким діапазоном частот коливань, а також амплітудою, прискоренням і часом дії. Рівень механічних дій визначається умовами транспортування й експлуатації.

Необхідно розрізняти два види механічних дій: удари і вібрації. Удар виникає, коли апаратура отримує швидку зміну прискорення (піддаються удару входи кабелів, джгути, резистори, конденсатори, напівпровідникові діоди і тріоди, силові трансформатори, дроселі тощо). Вібрації – довготривалі знакозмінні процеси, які впливають на роботу апаратури при безпосередньому контакті з джерелом коливань або через повітряне середовище.

У результаті дії вібрацій і удару можуть бути наступні ушкодження апаратури: порушення герметичності через псування паяльних, зварних і клеєних швів і появи тріщин у метало-скляних спаях; повне руйнування корпусів або окремих їх частин через механічний резонанс або циклічну втому; обривання монтажних зв'язків, відшарування багатошарових друкованих плат, руйнування підставок; вихід з ладу електричних контактів; модуляція розмірів хвилеводних трактів; коаксіальних кабелів, конденсаторів змінної ємності, коливальних контурів, електровакуумних приладів, зміщення положення органів настроювання і управління.

Під впливом вібрацій може статись зміна параметрів напівпровідникових приладів, вольт амперних характеристик діодів, транзисторів. Все це призводить до руйнування конструкцій за рахунок явищ втоми.

Радіоелектронна апаратура (РЕА) повинна мати віброміцність, вібростійкість, ударостійкість.

Захист РЕА здійснюється наступними групами методів:

– зменшується інтенсивність джерел вібрації шляхом балансування, зменшення зазорів, віброізоляції джерела вібрацій;

– зменшується величина дій, що передається апаратом шляхом віброізоляції, демпфірування, виключення резонансів, активного віброзахисту за допомогою ексцентриків, маятників, гіроскопів;

– використання найбільш добротні і жорсткі компоненти і вузли;

– застосовуються амортизатори.

Захист часом, захист віддалю, усунення джерела тепловиділення, теплоізоляція, охолодження гарячої поверхні, забезпечення тепловіддачі тіла людини та індивідуальні засоби захисту.

Захист часом передбачає обмеження часу перебування робітника в зоні дії інфрачервоного випромінювання. Потужність випромінювання можна знизити за рахунок конструкторських і технологічних рішень (зміною нагрівання виробів у нагрівальних пічках індукційним нагріванням та ін.) і за рахунок покриття поверхні, яка нагрівається, тепло ізолювальним матеріалом.

Якщо теплоізоляція неможлива, тоді захист від прямої дії інфрачервоного випромінювання здійснюється екрануванням.

Екрани можуть бути прозорими, напівпрозорими і непрозорими.

У свою чергу вони поділяються на тепловідбивальні, тепловідвідні та теплопоглинальні; стаціонарні і нестаціонарні.

Застосовують також прозору водяну завісу у вигляді суцільної тонкої водяної плівки. Вода є активним поглиначем інфрачервоного випромінювання.

Перегрівання людини попереджують раціональним режимом пиття, режимом праці та гідро процедурами. Спецодяг виготовляється з незаймистого, стійкого до інфрачервоного випромінювання, м’якого і повітронепроникного матеріалу (тканина з металевим покриттям відбиває 90 % інфрачервоного випромінювання).

Для захисту очей застосовують світлофільтри зі спеціального жовто-зеленого або синього скла.

Першочергові заходи – це конструкторські і технологічні рішення, які виключають генерацію або понижують інтенсивність випромінювання. Спеціальні засоби захисту (екранування джерел випромінювання, фарбування стін у світлі кольори) попереджують розповсюдження і знижують інтенсивність цих випромінювань у виробничих приміщеннях. Очі захищають окулярами або щитками зі склом – світлофільтром. Для захисту шкіри використовують мазі з речовинами – світлофільтрами для цих променів (салол, саліцилово-метиловий ефір та ін.), а також спецодяг з бавовняних тканин і грубововняного сукна. Руки захищають рукавицями.

ВИСНОВКИ

Splunk – це програмна платформа, яка використовується для моніторингу, пошуку, аналізу та візуалізації даних, створених обчислювальною технікою в реальному часі. Його використання для індексації та збору даних у реальному часі дуже важливе та широко визнане. Крім того, Splunk використовується для створення графіків та діаграм, інформаційних панелей, попереджень та інтерактивних візуалізацій. Використовуючи Splunk, організації можуть легко отримати доступ до даних і знайти рішення для складних бізнес-проблем.

Однією з найбільших переваг Splunk є обробка даних в режимі реального часу. Вхідні дані для Splunk можуть бути в будь-якому форматі, наприклад CSV, JSON тощо. Можна легко шукати та досліджувати конкретний результат за допомогою Splunk. Це дозволяє усунути будь-які несправності системи для підвищення її продуктивності. Можна відстежувати будь-які бізнес-показники та приймати зважене рішення. Можна візуалізувати результати за допомогою потужних інформаційних панелей.

Таким чином можна аналізувати продуктивність будь-якої IT-системи за допомогою інструмента Splunk. Splunk дозволяє також включити штучний інтелект для опрацювання даних.

Типовими задачами для застосування сервісу Splunk є:

– для веб-аналітики, щоб зрозуміти KPI та підвищити продуктивність;

– в IT-операціях для виявлення вторгнень, зловживань і зловмисників мережі;

– відстеження та аналіз цифрового маркетингу;

– робота в поєднанні з Інтернетом речей;

– в системах промислової автоматизації з метою моніторингу їх роботи;

– консультування персоналу з кібербезпеки щодо прийняття рішень стосовно захисту IT-систем.

ПЕРЕЛІК ПОСИЛАНЬ

1. Splunk Use Cases. CyberY [електронний ресурс] https://0xcybery.github.io/blog/Splunk+Use+Cases (квітень, 2022).

2. David Taylor. Splunk Tutorial for Beginners: What is Splunk Tool? How to Use? [електронний ресурс] https://www.guru99.com/splunk-tutorial.html (травень, 2022).

3. Splunk Cloud Platform. Search Tutorial 8.2.2203. Splunk inc. [електронний ресурс] https://docs.splunk.com/ Documentation/SplunkCloud/ 8.2.2203/ SearchTutorial/WelcometotheSearchTutorial (травень, 2022).

4. Splunk Tutorial. Java Point. [електронний ресурс] https://www.javatpoint.com/splunk (квітень, 2022).

5. Splunk Tutorial For Beginners: Explore Machine Data With Splunk. edureca! [електронний ресурс] https://www.edureka.co/blog/splunk-tutorial (квітень, 2022).

6. Splunk online tutorial. Geek University. [електронний ресурс] https://geek-university.com/splunk-online-tutorial/ (квітень, 2022).

7. Конспект лекцій з курсу «Охорона праці в галузі» / Укладачі: Яскілка В.Я., Олійник М.З. – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 56 с.

8. Шконда В.В., Кальянов А.В. Культорологічні засади становлення майбутніх фахівців: Монографія. – Донецьк, 2012. – 262 с.

9. Шконда В.В., Кальянов А.В., Давыдов П.Г. Феномен синергетики: наука – общество – образование: Монография / Ред. Шконда В.В. – Донецк: Норд-Пресс, 2009. – 156 с.

10. Информационная культура предприятий, виды информационной культуры, информационное поведение [Електронний ресурс]: [Веб-сайт]. – Електронні дані (Лекції). – Режим доступу: https://lektsii.com/1-78900.html – відкритий.

11. Пивоваров М.Г., Медко Д.А. Перспективы создания и развития информационно-коммуникационной системы Украины // Економіка: проблеми теорії та практики: Зб. наук. праць. – Вип. 49. – Дніпропетровськ: Дніпропетр. Нац. Ун-т, 2000. – С.56-61.