|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ** | | | | | | | | | | | | | | | | | | | | | | | | | |
| **НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ** | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
| **КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ** | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
| **КВАЛІФІКАЦІЙНА РОБОТА** | | | | | | | | | | | | | | | | | | | | | | | | | |
| на тему: | | | | | | | | | | | | | | | | | | | | | | | | | |
| **«Методи проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack»** | | | | | | | | | | | | | | | | | | | | | | | | | |
| зі спеціальності | | | | *125 Кібербезпека* | | | | | | | | | | | | | | | | |  | | | | |
| *(код, найменування спеціальності)* | | | | | | | | | | | | | | | | | | | | | | | | | |
| освітньо-професійної програми | | | | | | | | | *Інформаційна та кібернетична безпека* | | | | | | | | | | | | | | | |  |
| *(назва програми)* | | | | | | | | | | | | | | | | | | | | | | | | | |
| *Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело*  \_\_\_\_\_\_\_\_\_\_\_\_ Богдан ТАРАСЕНКО  *(підпис)* | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | Виконав: здобувач вищої освіти групи БСД-44 | | | | | | | | | | | | | | | | | |
|  | |  | | | | | | | | ТАРАСЕНКО Богдан | | | | | | | | | | | | | | | |
|  | |  | | | | | | | | *(прізвище, ім’я)* | | | | | | | | | | | | | | | |
|  | |  | | | | | | Керівник | | | | | | Ст. викладач, ДМІТРІЄВ В.Є. | | | | | | | | | | | |
|  | |  | | | | | | *(науковий ступінь, вчене звання, прізвище, ім’я)* | | | | | | | | | | | | | | | | | |
|  | |  | | | | | | Рецензент | | | | | | |  | | | | | | | | | | |
|  | |  | | | | | | *(науковий ступінь, вчене звання, прізвище, ім’я)* | | | | | | | | | | | | | | | | | |
|  | |  | | | | | |
|  | |  | | | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | | Київ 2025 | | | | | | | | | | | | | | | | | | | |  | | | |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**  **НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ** | | | | | | | | | | | | | | | | | | | | | | | | | |
| Кафедра | | Систем та технологій кібербезпеки | | | | | | | | | | | | | | | | | | | | | | | |
| Ступінь вищої освіти | | | | | Бакалавр | | | | | | | | | | | |  | | | | |  | | | |
| Спеціальність | | | 125 Кібербезпека | | | | | | | | | | | | | |  | | | | |  | | | |
| Освітньо-професійна програма | | | | | | | | | | Інформаційна та кібернетична безпека | | | | | | | | | | | | | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | | ЗАТВЕРДЖУЮ | | | | | | | | |
|  | |  | | | | | | | |  | | | | | | | Завідувач кафедри СТКБ | | | | | | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | | Галина ГАЙДУР | | | |
|  | |  | | | | | | | |  | | | | | | | “\_\_\_” 2025 року | | | | | | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | | **З А В Д А Н Н Я** | | | | | | | | | | | | | | | | | | | |  | | | |
|  | | **НА КВАЛІФІКАЦІЙНУ РОБОТУ** | | | | | | | | | | | | | | | | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
| Тарасенку Богдану Тарасовичу | | | | | | | | | | | | | | | | | | | | | | | | | |
| *(прізвище, ім’я)* | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. Тема кваліфікаційної роботи: | | | | | | | | | | |  | | | | | | | | | | | | | | |
| **«**Методи проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack» | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | | | | | |
| керівник кваліфікаційної роботи | | | | | | | | | | | | Дмітрієв В'ячеслав, Ст. викладач | | | | | | | | | | | | | |
|  | |  | | | | | | | | *(прізвище, ім’я, науковий ступінь, вчене звання)* | | | | | | | | | | | | | | | |
| затверджені наказом Державного університету інформаційно-комунікаційних  технологій від « » \_\_\_\_\_\_\_\_\_ 2025 року № \_\_\_\_. | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
| 2. Строк подання здобувачем вищої освіти кваліфікаційної роботи | | | | | | | | | | | | | | | | | | | | | | | 06.06.2024 р. | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
| 3. Вихідні дані до кваліфікаційної роботи | | | | | | | | | | | | |  | | | | | | | | |  | | | |
| інформаційна система організації (умовна або реальна); | | | | | | | | | | | | | | | | |  | | | | |  | | | |
| рішення ELK Stack; | | | | | | | | | | | | | | | | | | | | | | | | | |
| наукова та технічна література, експлуатаційна документація, нормативні | | | | | | | | | | | | | | | | | | | | | | | | | |
| документи, міжнародні стандарти. | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1. Дослідження проблеми розслідувань з кібербезпеки в інформаційній системі організації. | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. Аналіз методів проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack. | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. Розроблення рекомендацій щодо розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack. | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4. Перелік графічного матеріалу | | | | | | | | | | | | | | | | |  | | | | |  | | | |
| Презентація PowerPoint. | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5. Дата видачі завдання | | | | | | 28.02.2025 р. | | | | | | | | | | | | | | | | | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
|  | | **КАЛЕНДАРНИЙ ПЛАН** | | | | | | | | | | | | | | | | | | | |  | | | |
|  | |  | | | | | | | |  | | | | | | |  | | | | |  | | | |
| №  зп | Назва етапів  кваліфікаційної роботи | | | | | | | | | | | | | | | | | Строк виконання етапів роботи | | | | | | Примітка | |
| 1. | Визначення актуальності проблеми методів проведення розслідувань з кібербезпеки в інформаційній системі організації | | | | | | | | | | | | | | | | | 03.03.2025 р. | | | | | |  | |
| 2. | Аналіз наукової та технічної літератури з питань теми кваліфікаційної роботи. | | | | | | | | | | | | | | | | | 18.03.2025 р. | | | | | |  | |
| 3. | Аналіз методів проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack | | | | | | | | | | | | | | | | | 29.03.2025 р. | | | | | |  | |
| 4. | Практична реалізація варіанту проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack | | | | | | | | | | | | | | | | | 14.04.2025 р. | | | | | |  | |
| 5. | Розроблення рекомендацій щодо розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack. | | | | | | | | | | | | | | | | | 01.05.2025 р. | | | | | |  | |
| 6. | Оформлення результатів дослідження. | | | | | | | | | | | | | | | | | 06.05.2025. р. | | | | | |  | |
| 7. | Підготовка доповіді до захисту. | | | | | | | | | | | | | | | | | 06.06.2025 р. | | | | | |  | |
|  | | | | | | | | | | | | | | | | | |  | | | | | |  | |
| Здобувач вищої освіти | | | | | | |  | | | | | | | | | | |  | | Богдан ТАРАСЕНКО | | | | | | |
|  | | | | | | | *(підпис)* | | | | | | | | | | |  | | *(ім’я, прізвище)* | | | | | | |
|  | |  | | | | | | | |  | | | | | |  | | | | | |  | | | |
| Керівник кваліфікаційної роботи | | | | | | | | | | | |  | | | | | |  | | В'ячеслав ДМІТРІЄВ | | | | | | | |
|  | | | | | | | | | | *(підпис)* | | | | | | | | | *(ім’я, прізвище)* | | | | | | |

**ВІДГУК РЕЦЕНЗЕНТА**

на кваліфікаційну роботу

здобувачаТАРАСЕНКА Богдана

на тему: «Методи проведення розслідувань з кібербезпеки в інформаційній системі організації»

**Актуальність:** У сучасних умовах стрімкого розвитку цифрових технологій та зростання кількості кіберзагроз питання забезпечення кібербезпеки в інформаційних системах організацій набуває особливої важливості. Проведення якісних розслідувань кіберінцидентів є ключовим етапом у запобіганні повторним порушенням безпеки та мінімізації можливих збитків.

Тема кваліфікаційної роботи є надзвичайно актуальною, відповідає сучасним вимогам сфери інформаційної безпеки та спрямована на практичне застосування сучасних методів цифрової криміналістики.

**Позитивні сторони:**

1. Робота має чітку структуру, логічно побудовані розділи та послідовне викладення матеріалу.
2. Автор демонструє глибоке розуміння предметної області, використовуючи сучасні підходи до розслідування інцидентів кібербезпеки.
3. Описані методи розслідувань підкріплюються прикладами їх практичного застосування, що свідчить про практичну цінність роботи.
4. Здобувач у роботі виявив аналітичні здібності, здатність до критичного мислення та самостійного вирішення фахових завдань.
5. У роботі використані актуальні джерела, зокрема міжнародні стандарти та практики в галузі кібербезпеки.

**Недоліки:**

1. У деяких місцях слід було б розширити порівняльний аналіз обраних методів розслідувань.
2. Відчувається певна недостатність візуалізацій, можна було б показати наприкладі реальної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

**Висновок:** Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **ТАРАСЕНКО Богдан** – присвоєння кваліфікації бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Рецензент: |  |  |  |  |  |  |  |
|  |  |  | *(науковий ступінь,*  *вчене звання)* |  | *(підпис)* |  | *(ім’я, прізвище)* |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**  **НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ** | | | | | | | | | |
| **ПОДАННЯ**  **ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**  **ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**  **на здобуття освітнього ступеня бакалавра** | | | | | | | | | |
| Направляється здобувач | | | ТАРАСЕНКО Богдан | | до захисту кваліфікаційної роботи | | | | |
|  | | | *(прізвище, ім’я)* | |  | | | | |
| спеціальності 125 Кібербезпека | | | |  | |  | | |  |
| освітньо-професійної програми | | | | Інформаційна та кібернетична безпека | | | | | |
|  | |  | | *(шифр і назва спеціальності)* | | | | | |
| на тему: | «Методи проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack». | | | | | | | | |
| Кваліфікаційна робота і рецензія додаються. | | | | | |  | | |  |
| Директор інституту | | | |  | | Євгенія ІВАНЧЕНКО | | | |
| *(підпис) (ім’я, прізвище)* | | | | | | | | | |
|  | |  | |  | |  | | |  |
|  | |  | | | | | | |  |
|  | |  | |  | |  | | |  |
|  | | **Висновок керівника кваліфікаційної роботи** | | | | | | |  |
| Здобувач **ТАРАСЕНКО Богдан**обрав тему роботи, метою якої було дослідити методи проведення розслідувань з кібербезпеки в інформаційній системі організаціїта розробка рекомендацій щодо її реалізації. Перелік використаних джерел свідчить про вміння здобувачем розбиратись в наукових питаннях та застосовувати їх при дослідженнях. Під час виконання кваліфікаційної роботи **ТАРАСЕНКО Богдан**показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати питання і робити висновки. Роботу виконував сумлінно, акуратно та вчасно за планом.  Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача **ТАРАСЕНКА Богдана**на оцінку **“добре”** та присвоїти йому кваліфікацію бакалавр з кібербезпеки за освітньою програмою Інформаційна та кібернетична безпека. | | | | | | | | | |
| Керівник кваліфікаційної роботи | | | | | |  | | В’ячеслав ДМІТРІЄВ | |
|  | |  | |  | | *(підпис)* | | | *(ім’я, прізвище)* |
|  | |  | |  | | “\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_ 2025 року | | | |
|  | | **Висновок кафедри про кваліфікаційну роботу** | | | | | | |  |
| Кваліфікаційна робота розглянута. Здобувач **ТАРАСЕНКО Богдан**допускається до захисту | | | | | | | | | |
| даної кваліфікаційної роботи в Екзаменаційній комісії. | | | | | | | | | |
| Завідувач кафедри Систем та технологій кібербезпеки | | | | | | |  | |  |
| *(назва*) | | | | | | | | | | |
|  | |  | |  | |  | | | Галина ГАЙДУР |
|  | |  | | *(підпис)* | | *(ім’я, прізвище)* | | | |
|  | | | |  | |  | | |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **РЕФЕРАТ** | | | | |
|  |  |  |  |  |
|  |  |  |  |  |
| Текстова частина кваліфікаційної роботи: 55 сторінок, 20 рисунків, 18 джерел.  *Об’єкт дослідження* – проведення розслідувань з кібербезпеки в інформаційній системі організації.  *Предмет дослідження* – методи та засоби проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack *.*  *Мета роботи р*озробити та реалізувати варіант проведення розслідувань інцидентів кібербезпеки в інформаційній системі організації з використанням інструментів платформи ELK Stack, з метою підвищення ефективності виявлення, аналізу та реагування на кіберзагрози.  *Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.  Проведення розслідувань з кібербезпеки є критично важливою складовою захисту інформаційної системи організації, оскільки це не лише реакція на інцидент, а й стратегічний процес, що дозволяє зміцнити стійкість інформаційної системи та зберегти довіру до організації. ELK Stack відіграє ключову роль у побудові процесу DFIR, забезпечуючи повний цикл: збір → аналіз → візуалізація → реагування. Тому ця система має все необхідно, що дозволяє організаціям швидко реагувати на інциденти безпеки.  В роботі досліджено проблему проведення розслідувань з кібербезпеки в інформаційній системі організації, зокрема розглянуто методи виявлення, аналізу та документування інцидентів за допомогою інструментів платформи ELK Stack. Також досліджено особливості інтеграції ELK Stack з іншими засобами інформаційної безпеки, проаналізовано приклади практичного застосування та розроблено рекомендації щодо впровадження системи моніторингу в реальному середовищі.  На основі досліджень, проведених у роботі, запропоновано варіант побудови системи розслідування інцидентів кібербезпеки на базі платформи ELK Stack, Розроблено рекомендації фахівцям з кібербезпеки щодо реалізації методів та засобів проведення розслідування.  Галузь використання – кібербезпека інформаційних ресурсів організації.  ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ, ПРОВЕДЕННЯ РОЗСЛІДУВАНЬ, МЕТОДИ ТА ЗАСОБИ ПРОВЕДЕННЯ РОЗСЛІДУВАНЬ З КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ | | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ЗМІСТ** | | | | | |
|  |  | | |  | Стор. |
|  | **ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ** ……………………………… | | | | 9 |
|  |  | | |  |  |
|  | **ВСТУП** …………………………………………………..……………… | | | | 10 |
|  |  | |  | |  |
| 1 | **ДОСЛІДЖЕННЯ ПРОБЛЕМИ ПРОВЕДЕННЯ РОЗСЛІДУВАНЬ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ**….………...…………………………………………...…. | | | | 13 |
|  |  |  | | |  |
|  | 1.1 | Аналіз проблеми проведення розслідувань з кібербезпеки в інформаційній системі організації ……………………......……….... | | | 13 |
|  | 1.2 | Аналіз підходів до проведення розслідувань з кібербезпеки в інформаційній системі організації ………......………......………...... | | | 16 |
|  | 1.3 | Аналіз існуючих рішень із проведення розслідувань з кібербезпеки в інформаційній системі організації …………......………......……… | | | 25 |
|  |  |  | | |  |
| 2 | **АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РОЗСЛІДУВАНЬ З КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ НА БАЗІ ELK STACK**…...……………...……………...…………….. | | | | 32 |
|  |  |  | | |  |
|  | 2.1 | Архітектура та компоненти рішення ELK Stack …………………... | | | 32 |
|  | 2.2 | Призначення та основні функції компонентів ELK Stack ………… | | | 35 |
|  | 2.3 | Процеси функціонування рішення ELK Stack …………………….. | | | 40 |
|  |  |  | | |  |
| 3 | **РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПРОВЕДЕННЯ РОЗСЛІДУВАНЬ З КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ** ……………………………………………… | | | | 43 |
|  |  |  | | |  |
|  | 3.1 | Варіант розгортання системи проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack ……………………………………………………....................... | | | 43 |
|  | 3.2 | Порядок проведення розслідувань з кібербезпеки в рішенні ELK Stack……………………………………………………...…...…...…... | | | 48 |
|  | 3.3 | Рекомендації щодо проведення розслідувань з кібербезпеки в інформаційній системі організації ………………………………………..……..……..……..……..…….. | | | 55 |
|  |  |  | | |  |
|  | **ВИСНОВКИ** …………………………………………………………….. | | | | 58 |
|  |  | | | |  |
|  | **ПЕРЕЛІК ПОСИЛАНЬ** ............................................................................ | | | | 60 |
|  |  | | | |  |
|  | **ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)** ............................ | | | | 62 |

**ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ**

API – Application Programming Interface

ATM – Asynchronous Transfer Mode

AWS – Amazon Web Services

C2 – Command and Control

CSV – Comma-Separated Values

DFIR – Digital Forensics and Incident Response

DDoS – Distributed Denial of Service

DNS – Domain Name System

DSL – Domain Specific Language

ELK – Elasticsearch, Logstash, Kibana

ESI – Electronically Stored Information

FDDI – Fiber Distributed Data Interface

GDPR – General Data Protection Regulation

IDS/IPS – Intrusion Detection System / Intrusion Prevention System

IEEE – Institute of Electrical and Electronics Engineers

IoCs – Indicators of Compromise

ISAC – Information Sharing and Analysis Center

ISAKMP – Internet Security Association and Key Management Protocol

ISO – International Organization for Standardization

JSON – JavaScript Object Notation

NIST – National Institute of Standards and Technology

NRT – Near Real-Time

PPP/HDLC – Point-to-Point Protocol / High-Level Data Link Control

RAM – Random Access Memory

SANS – SysAdmin, Audit, Network, and Security Institute

SIEM – Security Information and Event Management

SP – Service Provider

SQL – Structured Query Language

SSL/TLS – Secure Sockets Layer / Transport Layer Security

TSK – The Sleuth Kit

TTPs – Tactics, Techniques, and Procedures

US CERT – United States Computer Emergency Readiness Team

VPN – Virtual Private Network

WEP – Wired Equivalent Privacy

WPA/WPA2 – Wi-Fi Protected Access / Wi-Fi Protected Access 2

**ВСТУП**

*Актуальність дослідження.* У сучасному цифровому середовищі зростання кількості та складності кіберзагроз стало одним з головних викликів для організацій будь-якого масштабу. Щодня відбуваються сотні тисяч атак на інформаційні системи, спрямованих на викрадення конфіденційної інформації, виведення систем з ладу, порушення бізнес-процесів або завдання економічної шкоди. У цьому контексті надзвичайно важливо не лише запобігати інцидентам інформаційної безпеки, а й уміти оперативно реагувати на них та розслідувати вже здійснені порушення.

Одна з головних проблем полягає в тому, що сучасні організації часто не мають ефективних механізмів внутрішнього моніторингу, централізованого збирання логів та аналітики, що унеможливлює повноцінне розслідування інцидентів. У багатьох випадках логи не збираються в одному місці, мають різні формати або не зберігаються достатньо довго. Це ускладнює ідентифікацію джерел загроз, їх аналіз і, найголовніше, — побудову повної картини атаки у часовому вимірі.

На цьому фоні все більшого значення набувають технології централізованого збору та обробки журналів подій (логів), які дозволяють здійснювати глибокий аналіз діяльності користувачів, систем і мереж. Однією з найбільш ефективних і водночас доступних рішень у цій сфері є ELK Stack — стек з відкритим вихідним кодом, що включає Elasticsearch, Logstash, Kibana та додаткові агенти Beats. Цей інструмент дозволяє організації побудувати власну внутрішню систему виявлення та розслідування інцидентів безпеки без значних фінансових витрат.

Використання ELK Stack забезпечує:

централізацію журналів подій з багатьох джерел (Windows, Linux, мережеві пристрої, веб-сервери тощо);

нормалізацію та структуризацію логів, що дає змогу уніфікувати процес аналізу;

побудову гнучких візуалізацій (дашбордів) і сповіщень про інциденти;

швидкий пошук по мільйонах подій для встановлення причин і наслідків порушень;

підтримку методів цифрової криміналістики (forensics) шляхом аналізу історичних даних.

Актуальність теми дослідження зумовлена також відсутністю стандартизованих підходів до побудови системи кіберрозслідувань у більшості організацій України, особливо в державному та комунальному секторах. Це робить запропоновану методику побудови рішення на базі ELK Stack не лише корисною, але й потенційно широко застосовуваною на практиці.

Крім того, сучасна стратегія Zero Trust, рекомендації NIST (SP 800-92, SP 800-137) та вимоги ISO/IEC 27001:2022 особливу увагу приділяють обов’язковому моніторингу подій безпеки та здатності організації реагувати на інциденти. Тобто впровадження систем розслідувань на базі ELK Stack сприятиме також і відповідності організації міжнародним стандартам у сфері кібербезпеки.

Підсумовуючи, можна зробити висновок, що дослідження методів розслідувань кіберінцидентів на базі ELK Stack є актуальним, практично значущим та своєчасним. Воно відповідає як нагальним вимогам ІТ-ринку, так і сучасним викликам кіберзахисту, та може бути інтегроване у реальну ІТ-інфраструктуру з метою підвищення рівня безпеки, прозорості та контролю за подіями.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження методів та засобів проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack.

*Об’єкт дослідження* – проведення розслідувань з кібербезпеки в інформаційній системі організації.

*Предмет дослідження* – методи та засоби проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack *.*

*Мета роботи р*озробити та реалізувати варіант проведення розслідувань інцидентів кібербезпеки в інформаційній системі організації з використанням інструментів платформи ELK Stack, з метою підвищення ефективності виявлення, аналізу та реагування на кіберзагрози.

*Наукові завдання:*

дослідити сутність проблеми проведення розслідувань з кібербезпеки в інформаційній системі організації;

проаналізувати основні підходи до проведення розслідувань з кібербезпеки в інформаційній системі організації;

проаналізувати існуючі рішення із проведення розслідувань з кібербезпеки в інформаційній системі організації;

проаналізувати методи та засоби проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack;

запропонувати варіант системи проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack;

розробити рекомендацій щодо застосування методів та засобів проведення розслідувань з кібербезпеки в інформаційній системі організації.

*Методи дослідження* – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

*Практичне значення одержаних результатів:* розроблено рекомендації щодо застосування методів та засобів проведення розслідувань з кібербезпеки в інформаційній системі організації, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науково-практичній конференції «Цифрова трансформація кібербезпеки», яка відбулася 24 квітня2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

**1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ПРОВЕДЕННЯ РОЗСЛІДУВАНЬ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ**

**1.1. Аналіз проблеми проведення розслідувань з кібербезпеки в інформаційній системі організації**

У сучасному цифровому середовищі організації постійно піддаються кіберзагрозам, які можуть спричинити витік конфіденційної інформації, порушення бізнес-процесів, зупинку критичних сервісів або репутаційні втрати. У зв’язку з цим, важливого значення набуває своєчасне й ефективне проведення кіберрозслідувань, метою яких є виявлення джерел загроз, визначення масштабів інциденту, збереження цифрових доказів та формування заходів для недопущення повторення аналогічних ситуацій у майбутньому.

Хоча безпеку організації зазвичай забезпечує внутрішня команда захисту, кожен співробітник відіграє роль у кібербезпеці. Річ у тім, що 80% атак щороку припадає на фішинг, шкідливе ПЗ та атаки через веб-додатки. Це доводить, що підвищення рівня кіберосвіти серед працівників є одним із найефективніших заходів захисту. Постійні тренінги та програми підвищення обізнаності допомагають співробітникам ставати першою лінією оборони проти зловмисників.  
Згідно фахівців з Verizon Data Breach Investigations Report (DBIR), маємо звіт, який підтверджує результати відповідних досліджень, які підкреслюють зростаючу загрозу (рисунок 1.1) [1].

Изображение выглядит как текст, снимок экрана, Шрифт, круг

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 1.1. Статистика та висновки цьогорічного звіту від Verizon [1]

Однак практика реалізації процесу кіберрозслідування виявляє низку суттєвих проблем.

*Відсутність уніфікованих підходів та політик* у більшості організацій немає чітко формалізованих внутрішніх політик реагування на інциденти або протоколів розслідувань. Це ускладнює координацію дій між ІТ-відділом, службами безпеки, юристами та керівництвом. За даними NIST SP 800-61 Rev. 2, інцидент-менеджмент має здійснюватися на основі циклу: підготовка → виявлення та аналіз → реагування → відновлення → постінцидентний аналіз, однак на практиці ці етапи часто реалізуються фрагментарно (рисунок 1.2) [2].

Изображение выглядит как текст, флэш-память, логотип, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 1.2. Життєвий цикл реагування на інциденти за версією NIST SP 800-61 Rev. 2 [2]

*Дефіцит кваліфікованих кадрів* за оцінками ENISA, однією з найгостріших проблем є відсутність фахівців з цифрової криміналістики та аналізу кіберінцидентів. Багато організацій не мають у штаті аналітиків безпеки, що володіють необхідними знаннями щодо обробки логів, аналізу трафіку, відновлення даних та формалізації цифрових доказів. Це призводить до втрати або пошкодження важливої інформації вже на ранньому етапі розслідування.

*Обмеженість технічної інфраструктури* у ряді випадків розслідування унеможливлюється через відсутність необхідних засобів логування, моніторингу подій, збереження історії доступів, журналів аудиту тощо. Це стосується як малого, так і середнього бізнесу. Наприклад, SANS Institute у своїх курсах із DFIR підкреслює необхідність впровадження SIEM-систем (Security Information and Event Management) для збору й кореляції подій, однак такі системи залишаються недоступними для багатьох підприємств через високу вартість або складність налаштування.

*Юридичні та процесуальні бар’єри* проведення кіберрозслідувань часто наштовхується на неврегульованість правових питань: відсутність чітких норм щодо збору, зберігання та передачі цифрових доказів, складність притягнення до відповідальності у випадку міждержавних атак, а також необхідність дотримання регуляторних вимог (наприклад, GDPR). Цифрові докази мають бути зібрані згідно з процесуальними нормами, щоб мати юридичну силу у суді, однак далеко не всі організації дотримуються відповідних стандартів.

Таким чином, проблема проведення розслідувань з кібербезпеки в інформаційних системах є багатогранною і включає як технічні, так і організаційно-правові аспекти. Для її вирішення необхідна побудова цілісної стратегії реагування на інциденти, інвестування в кадровий потенціал, модернізація засобів безпеки, а також тісна взаємодія з правоохоронними органами й регуляторами.

**1.2 Аналіз підходів до проведення розслідувань з кібербезпеки в інформаційній система організації**

Проведення розслідувань кіберінцидентів є комплексною діяльністю, що потребує чіткої організації, методологічної бази та використання технічних і правових інструментів. Станом на сьогодні, сформувалось декілька усталених підходів до розслідувань у сфері кібербезпеки, які застосовуються в залежності від специфіки інциденту, ресурсів організації та її регуляторного середовища.

*Стандартизований підхід за NIST (США)* один із найавторитетніших підходів викладено у документі NIST SP 800-61 Rev. 2 — "Computer Security Incident Handling Guide". У ньому розслідування організовується у вигляді життєвого циклу з чотирьох етапів [1]:

Підготовка (Preparation) — створення політик, навчання персоналу, налаштування моніторингу.

Виявлення та аналіз (Detection and Analysis) — збір логів, виявлення аномалій, початковий тріаж.

Стримування, усунення, відновлення (Containment, Eradication, Recovery) — блокування загроз, відновлення роботи.

Післяінцидентний аналіз (Post-Incident Activity) — уроки з інциденту, оновлення процедур.

Цей підхід особливо ефективний для організацій, що прагнуть дотримання принципів зрілості процесів кіберзахисту.

*Ключові рекомендації* щодо організації можливостей реагування на комп’ютерні інциденти наведені нижче:

Створити офіційну здатність до реагування на інциденти. Організації повинні бути готовими швидко й ефективно реагувати на порушення комп’ютерної безпеки. Закон FISMA вимагає від федеральних агентств створення можливостей реагування на інциденти.

Розробити політику реагування на інциденти. Політика є основою програми реагування на інциденти. Вона визначає, які події вважаються інцидентами, встановлює організаційну структуру реагування, ролі та обов’язки, а також вимоги до звітування про інциденти й інші аспекти.

Розробити план реагування на інциденти на основі політики. План реагування забезпечує дорожню карту для впровадження програми реагування відповідно до політики організації. Він визначає як коротко-, так і довгострокові цілі програми, включаючи метрики для оцінювання ефективності. У плані також слід зазначити, як часто потрібно проводити навчання фахівців з реагування та вимоги до їх кваліфікації.

Розробити процедури реагування на інциденти. Процедури мають містити детальні кроки реагування на інциденти, охоплюючи всі фази процесу реагування. Вони повинні ґрунтуватися на політиці та плані реагування на інциденти.

Встановити політики та процедури щодо обміну інформацією, пов’язаною з інцидентами. Організація повинна передавати відповідну інформацію зовнішнім сторонам, таким як ЗМІ, правоохоронні органи та організації для звітування про інциденти. Команда з реагування має обговорити це з пресслужбою, юридичним відділом та керівництвом для створення відповідних політик і процедур. Вона також має дотримуватись чинної політики організації щодо взаємодії із зовнішніми сторонами.

Надати відповідну інформацію про інциденти уповноваженим організаціям. Федеральні цивільні агентства зобов’язані повідомляти про інциденти в US-CERT; інші організації також можуть звертатися до US-CERT та/або свого ISAC. Повідомлення є корисним, оскільки US-CERT і ISAC використовують ці дані для інформування учасників про нові загрози та тенденції інцидентів.

Ураховувати відповідні чинники при виборі моделі команди з реагування. Організації мають ретельно зважити переваги та недоліки кожної можливої моделі структури та кадрового складу, враховуючи свої потреби й доступні ресурси.

Відібрати людей із відповідними навичками для команди. Авторитет і ефективність команди великою мірою залежать від технічних навичок і критичного мислення її членів. Важливими є такі навички, як адміністрування систем і мереж, програмування, технічна підтримка та виявлення вторгнень. Також необхідні навички командної роботи та комунікації. Усі члени команди мають проходити відповідне навчання.

Визначити інші підрозділи організації, які можуть бути залучені до реагування. Команда з реагування покладається на експертизу, досвід і здібності інших підрозділів, включаючи керівництво, службу інформаційної безпеки, ІТ-підтримку, юридичний відділ, пресслужбу та адміністрацію об’єктів.

Визначити перелік послуг, які повинна надавати команда. Хоча основна мета команди — реагування на інциденти, більшість команд виконує додаткові функції. Прикладами є моніторинг систем виявлення вторгнень, розповсюдження інформаційних бюлетенів з безпеки та навчання користувачів з питань безпеки [1].

*Підхід цифрової криміналістики*. Озираючись назад на історію цифрової криміналістики, можна сказати, що правоохоронні органи того часу мали мінімальне розуміння застосування методів цифрової криміналістики. Однак протягом 1970-х і 1980-х років група криміналістів в основному складалася з представників федеральних правоохоронних органів з комп'ютерною освітою. Першою сферою, яка викликала занепокоєння у правоохоронців, було зберігання даних, оскільки більшість документації відбувалася в цифровому форматі. Безперечно, вилучення, зберігання та аналіз документації були тривалим завданням для влади. У цій ситуації ФБР у 1984 році запустило програму Magnet Media, яка була першою офіційною програмою цифрової криміналістики. Слідом за цим були розроблені інші методи виявлення кіберзлочинців при їх проникненні в комп'ютерні системи. У 1986 році Кліфф Столл, системний адміністратор Unix в Національній лабораторії Лоуренса в Берклі, створив першу пастку для ханіпоту. Згодом цифрова криміналістика набула професійного піднесення у зв'язку з поширенням дитячої порнографії в Інтернеті. Війна між Іраком та Афганістаном також призвела до того, що з'явився попит на цифрове криміналістичне розслідування. Водночас цифрова криміналістика відіграла важливу роль у вилученні доказових даних із цифрових активів, зібраних американськими військами під час війни. У 2006 році США впровадили обов'язковий режим електронного витребування у свої Правила цивільного процесу.

Цифровий слід – це інформація про людину в системі, наприклад, веб-сторінки, які вона відвідувала, коли вона була активною та який пристрій використовувала. Слідуючи за цифровими слідами, слідчий отримає дані, критично важливі для розкриття справи про злочин. Наприклад, Метт Бейкер у 2010 році, Кренар Луша у 2009 році, і ще більше справ було розкрито за допомогою цифрової криміналістики.

Слідчі з кіберкриміналістики є експертами у розслідуванні зашифрованих даних з використанням різних типів програмного забезпечення та інструментів. Існує багато майбутніх методів, які використовують слідчі залежно від типу кіберзлочинів, з якими вони мають справу. Завдання кіберслідчих включають відновлення видалених файлів, злом паролів і пошук джерела порушення безпеки. Після збору докази потім зберігаються та перекладаються, щоб зробити їх презентаційними перед судом або для подальшого вивчення поліцією. Роль кіберкриміналістики у кримінальних правопорушеннях можна зрозуміти на прикладі конкретного прикладу: холодні кейси та кіберкриміналістика

*Модель цифрової криміналістики (Digital Forensics Approach)* цей підхід передбачає проведення детального аналізу цифрових слідів злочину або атаки. Його основні етапи (рисунок 1.3)[4]:

Фаза I – Перше реагування. Дія, виконана відразу після виникнення інциденту безпеки, називається першим реагуванням. Це сильно залежить від характеру події.

Фаза II – Обшук і виїмка. На цьому етапі професіонали шукають пристрої, задіяні у скоєнні злочину. Потім ці пристрої обережно вилучалися, щоб витягнути з них інформацію.

Фаза III – Збір доказів. Після етапу обшуку та вилучення професіонали використовують придбані пристрої для збору даних. Вони мають чітко визначені криміналістичні методи поводження з доказами.

Фаза IV - Захист доказів. Судово-медичний персонал повинен мати доступ до безпечного середовища, де вони можуть зберегти докази. Вони визначають, чи є зібрані дані точними, автентичними та доступними.

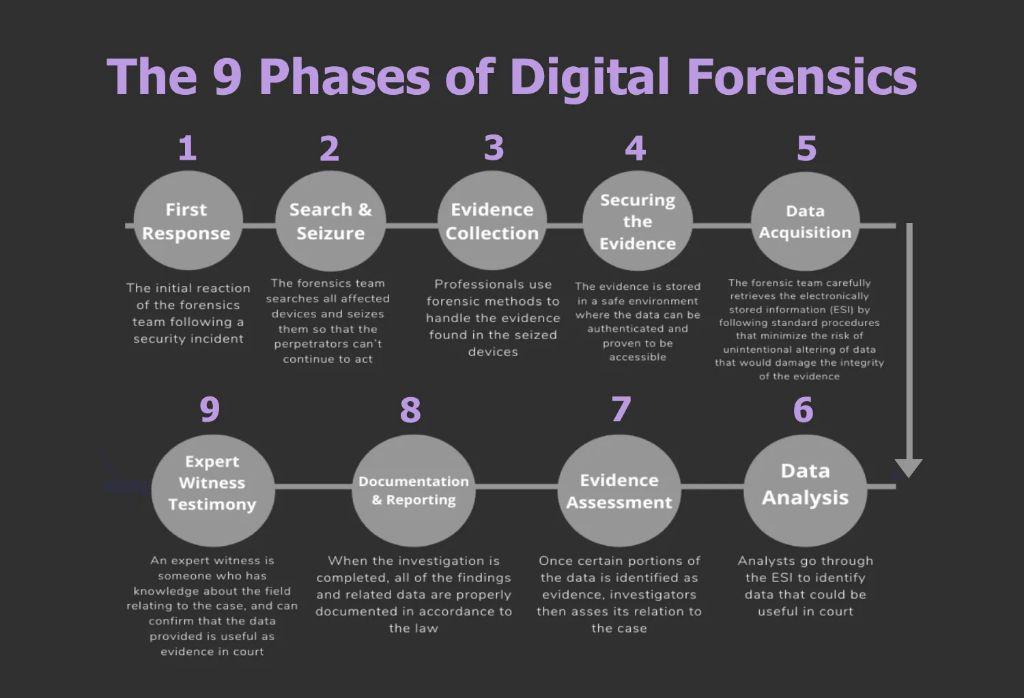
Фаза V – Збір даних. збір даних – це процес отримання інформації, що зберігається в електронному вигляді (ESI) з підозрюваних цифрових активів. Це допомагає отримати уявлення про інцидент, тоді як неналежний процес може змінити дані, тим самим пожертвувавши цілісністю доказів.

Фаза VI – Аналіз даних. Під час аналізу даних підзвітний персонал сканує отримані дані, щоб виявити доказову інформацію, яка може бути представлена суду. Цей етап полягає у вивченні, виявленні, розділенні, перетворенні та моделюванні даних для перетворення їх на корисну інформацію.

Фаза VII – Оцінка доказів. Процес оцінки доказів пов'язує доказові дані з інцидентом безпеки. Повинна бути ретельна оцінка, заснована на масштабах справи.

Фаза VIII – Документація та звітність. Це етап після розслідування, який охоплює звітування та документування всіх висновків. Крім того, звіт повинен мати достатні та прийнятні докази відповідно до суду.

Фаза IX – Надання свідчень як свідок-експерт. Судово-медичний експерт повинен підійти до свідка-експерта для підтвердження точності доказів. Свідок-експерт – це фахівець, який розслідує злочин з метою отримання доказів [4].

  
Рис 1.3. Фази цифрової криміналістики.[4]

*Підхід Cyber Kill Chain*, розроблений Lockheed Martin (2022), пояснює, як зловмисники переміщуються мережами, щоб виявити вразливості, якими вони потім можуть скористатися. Зловмисники використовують кроки в ланцюжку кібервбивств під час проведення наступальних операцій у кіберпросторі проти своїх цілей. Якщо ви відповідаєте за захист мережі, ця модель може допомогти вам зрозуміти етапи кібератаки та заходи, які ви можете вжити для запобігання або перехоплення кожного кроку.

*Cyber Kill Chain* поділяється на сім етапів (рисунок 1.4): розвідка, використання зброї, доставка, експлуатація, встановлення, командування та управління (C2) та дії на цілях [5].

*Розвідка*є першим етапом у ланцюжку кібератак і передбачає дослідження потенційних цілей перед проведенням будь-яких тестів на проникнення. Етап розвідки може включати виявлення потенційних цілей, знаходження їх вразливостей, виявлення того, які треті сторони з ними пов'язані (і до яких даних вони можуть отримати доступ), а також вивчення існуючих точок входу, а також пошук нових. Розвідка може проходити як онлайн, так і офлайн.

*Використання зброї* це етап використання Cyber Kill Chain як зброї відбувається після того, як відбулася розвідка і зловмисник виявив всю необхідну інформацію про потенційні цілі, такі як вразливості. На етапі перетворення на зброю вся підготовча робота зловмисника завершується створенням шкідливого програмного забезпечення для використання проти визначеної цілі. Використання зброї може включати створення нових типів зловмисного програмного забезпечення або модифікацію існуючих інструментів для використання в кібератаці. Наприклад, кіберзлочинці можуть вносити незначні зміни в існуючий варіант програми-вимагача, щоб створити новий інструмент Cyber Kill Chain.

*Доставка* важлива, адже на етапі доставки кіберзброя та інші інструменти Cyber Kill Chain використовуються для проникнення в мережу цілі та охоплення користувачів. Доставка може включати надсилання фішингових електронних листів із вкладеннями зловмисного програмного забезпечення з темами, які пропонують користувачам перейти за посиланням. Доставка також може набувати форми злому мережі організації та використання вразливості апаратного або програмного забезпечення для проникнення в неї.

*Експлуатація* – це етап, який слідує за доставкою та використанням зброї. На етапі експлуатації Cyber Kill Chain зловмисники використовують вразливості, які вони виявили на попередніх етапах, щоб ще більше проникнути в мережу цілі та досягти своїх цілей. У цьому процесі кіберзлочинці часто переміщуються бічно по мережі, щоб дістатися до своїх цілей. Експлуатація іноді може привести зловмисників до їхніх цілей, якщо особи, відповідальні за мережу, не вжили заходів обману.

*Встановлення* після того, як кіберзлочинці скористалися вразливостями своєї цілі, щоб отримати доступ до мережі, вони починають етап встановлення Cyber Kill Chain: спроба встановити шкідливе програмне забезпечення та іншу кіберзброю на цільову мережу, щоб взяти під контроль її системи та викрасти цінні дані. На цьому етапі кіберзлочинці можуть встановити кіберзброю та зловмисне програмне забезпечення за допомогою троянських коней, бекдорів або інтерфейсів командного рядка.

*Командування та управління* на етапі C2 Cyber Kill Chain кіберзлочинці спілкуються зі шкідливим програмним забезпеченням, яке вони встановили в мережу цілі, щоб дати вказівки кіберзброї або інструментам для виконання своїх цілей. Наприклад, зловмисники можуть використовувати канали зв'язку, щоб спрямувати комп'ютери, заражені шкідливим програмним забезпеченням ботнету Mirai, перевантажити веб-сайт трафіком, або сервери C2, щоб дати вказівку комп'ютерам виконувати цілі кіберзлочинності.

Дії щодо цілей після того, як кіберзлочинці розробили кіберзброю, встановили її в мережу цілі та взяли під контроль мережу своєї цілі, вони починають завершальний етап Cyber Kill Chain: виконання своїх цілей кібератаки. Хоча цілі кіберзлочинців різняться залежно від типу кібератаки, деякі приклади включають використання ботнету як зброї для переривання послуг за допомогою розподіленої атаки типу «відмова в обслуговуванні » (DDoS), розповсюдження шкідливого програмного забезпечення для викрадення конфіденційних даних цільової організації та використання програм-вимагачів як інструменту кібервимагання [5].

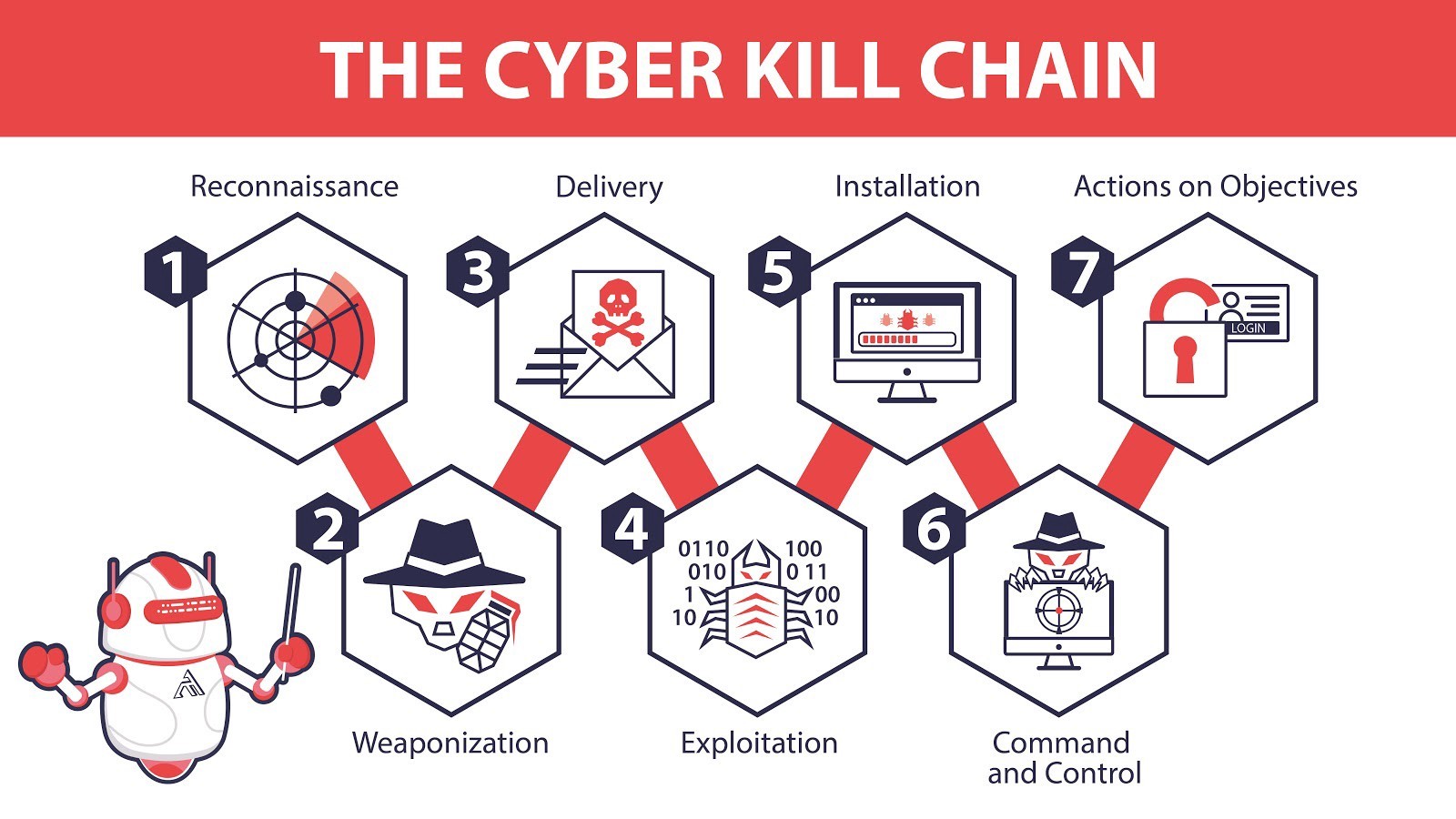


Рис. 1.4. Модель Kill Chain [5]

*Підхід MITRE ATT&CK* — це база знань з тактик, технік та процедур (TTPs), які використовують зловмисники. Вона дозволяє: класифікувати дії зловмисника впродовж атаки, корелювати індикатори компрометації (IoCs) з поведінковими ознаками, автоматизувати виявлення інцидентів у SIEM-системах.

MITRE ATT&CK все частіше використовується у поєднанні з іншими підходами для побудови більш детальної картини атаки.

За результатами аналізу показує (таблиця 1.1), що ефективне розслідування кіберінцидентів вимагає поєднання різних методологій. Універсального підходу не існує, однак більшість провідних компаній комбінують стандарти NIST, інструменти цифрової криміналістики та поведінкові моделі на основі MITRE ATT&CK. Успішне впровадження цих підходів забезпечує як швидке реагування на інциденти, так і якісний аналіз для підвищення рівня кіберстійкості організації.

Таблиця 1.1

**Порівняльна таблиця підходів до кіберрозслідувань**

|  |  |  |  |
| --- | --- | --- | --- |
| Підхід | Фокус | Призначення | Сфера застосування |
| NIST SP 800-61 | Цикл реагування на інциденти | Управління та реагування | Організації з політикою безпеки |
| Digital Forensics | Збір і аналіз цифрових доказів | Юридично значимий аналіз | Правоохоронні, великі корпорації |
| Kill Chain Model | Етапи кібератаки | Виявлення та зупинка атаки | Аналітика SOC, Threat Hunting |
| MITRE ATT&CK | Тактики, техніки, процедури атак | Аналіз поведінки атакуючого | SIEM, Red Teaming, Blue Teaming |

|  |  |
| --- | --- |
| **1.3** | **Аналіз існуючих рішень із проведення розслідувань з кібербезпеки в інформаційній системі організації** |

Сучасні інформаційні системи організацій є об'єктами постійного ризику у зв’язку з високою активністю кіберзлочинців, що вимагає наявності ефективних рішень для розслідування інцидентів інформаційної безпеки. Існуючі рішення можна умовно поділити на три категорії: автоматизовані інструменти, програмні комплекси для цифрової криміналістики, а також інтегровані системи моніторингу та реагування на інциденти.

1.3.1 Автоматизовані засоби збору і фіксації цифрових слідів

Ці інструменти здатні забезпечувати швидке виявлення та документування слідів кіберінцидентів. Прикладами є:

*Volatility Framework* — платформа для аналізу вмісту оперативної пам’яті, яка дозволяє виявляти підозрілі процеси, відкриті сокети, обробники API тощо.

У 2007 році перша версія The Volatility Framework була випущена публічно на Black Hat DC. Програмне забезпечення було засноване на багаторічних опублікованих академічних дослідженнях у галузі передового аналізу пам'яті та криміналістики. До цього моменту цифрові розслідування були зосереджені в основному на пошуку контрабанди в зображеннях жорстких дисків. Волатильність познайомила людей з можливостями аналізу стану системи під час виконання за допомогою даних, знайдених у енергонезалежних сховищах (RAM). Він також надав кросплатформну, модульну та розширювану платформу для заохочення подальшої роботи в цій захоплюючій галузі досліджень. Іншою важливою метою було заохочення співпраці, інновацій та доступу до знань, які були поширені в спільнотах наступального програмного забезпечення.

З того часу аналіз пам'яті став однією з найважливіших тем для майбутнього цифрових досліджень. Зараз Volatility є найбільш широко використовуваною у світі платформою для криміналістики пам'яті (рисунок 1.5.)[7], яка підтримується однією з найбільших та найактивніших спільнот у криміналістичній галузі. Volatility також надає унікальну платформу, яка дозволяє негайно передавати передові дослідження в руки цифрових слідчих. В результаті, дослідження, побудовані на основі волатильності, з'явилися на провідних академічних конференціях, а волатильність використовувалася в деяких з найбільш критичних досліджень останнього десятиліття. Він став незамінним інструментом цифрових розслідувань, на який покладаються правоохоронні органи, військові, наукові та комерційні слідчі по всьому світу.

Фонд Volatility Foundation був створений для сприяння використанню аналізу волатильності та пам'яті в криміналістичному співтоваристві; захищати інтелектуальну власність проекту (торгові марки, ліцензії тощо) та довговічність його життя; і сприяти просуванню інноваційних досліджень з аналізу пам'яті. У цьому напрямку також було створено Volatility Foundation, щоб допомогти захистити права розробників, які жертвують своїм часом і ресурсами, щоб зберегти найдосконалішу у світі платформу криміналістики пам'яті з вільним і відкритим вихідним кодом.

Изображение выглядит как текст, снимок экрана, линия, диаграмма

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 1.5. Графік популярності інструментів для криміналістики пам'яті.

*Autopsy* є одним із найбільш популярних безкоштовних інструментів для проведення цифрових розслідувань. Це зручне графічне середовище, побудоване на базі інструменту командного рядка The Sleuth Kit (TSK), яке дозволяє швидко та ефективно проводити аналіз цифрових носіїв, включаючи жорсткі диски, флеш-накопичувачі та образи дисків.

Autopsy підтримується активною спільнотою розробників та широко застосовується в правоохоронних структурах, кібербезпеці, корпоративному секторі та освітніх установах. Основною перевагою інструменту є поєднання широких можливостей аналізу з інтуїтивно зрозумілим графічним інтерфейсом, що значно спрощує роботу експерта з цифрової криміналістики.

Простота у використанні. Autopsy був розроблений таким чином, щоб бути інтуїтивно зрозумілим з коробки. Установка проста, а інструкції проведуть вас через кожен крок. Всі результати знаходяться в одному дереві.

Розширюваний. Autopsy була розроблена як наскрізна платформа з модулями, які постачаються з нею з коробки, та іншими, доступними від третіх сторін.

Швидкий. Всі хочуть результату ще раз, навіть в цю ж секунду. Autopsy виконує фонові завдання паралельно з використанням кількох ядер і надає вам результати, як тільки вони будуть знайдені. Повний пошук на диску може зайняти кілька годин, але ви дізнаєтесь за кілька хвилин, чи були знайдені ваші ключові слова в домашній папці користувача.

Економічно вигідний. Autopsy безкоштовний. Оскільки бюджети зменшуються, економічно ефективні рішення для цифрової криміналістики є важливими. Autopsy пропонує ті ж основні функції, що й інші інструменти цифрової криміналістики, і пропонує інші важливі функції, такі як веб-аналіз артефактів та аналіз реєстру, яких не надають інші комерційні інструменти [8].

1.3.2 Інструменти аналізу мережевого трафіку

Виявлення та відслідковування активності зловмисників у мережі організації здійснюється за допомогою таких систем:

*Wireshark* — безкоштовний аналізатор мережевого трафіку, що дозволяє проводити глибокий аналіз пакетів і визначати підозрілу активність. Wireshark є провідним у світі аналізатором мережевих протоколів. Це дає змогу бачити, що відбувається у вашій мережі на мікроскопічному рівні. Це стандарт де-факто (і часто де-юре) у багатьох галузях і навчальних закладах.

Розробка Wireshark процвітає завдяки внеску експертів з нетворкінгу з усього світу. Він є продовженням проекту, який стартував у 1998 році.

Мультиплатформенність: працює на Windows, Linux, macOS, FreeBSD, NetBSD та багатьох інших.

Дані в реальному часі можна зчитувати з Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI та інших (залежно від вашої платформи).

Підтримка дешифрування для багатьох протоколів, включаючи IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP і WPA/WPA2.

Глибока перевірка сотень протоколів, які постійно додаються [9].

*Suricata* — це високопродуктивне програмне забезпечення для аналізу мережі та виявлення загроз з відкритим вихідним кодом, яке використовується більшістю приватних і державних організацій і вбудовується великими постачальниками для захисту своїх активів. Система виявлення вторгнень (IDS), яка дозволяє в режимі реального часу виявляти підозрілі шаблони в трафіку.

Suricata розпочала свій шлях до допомоги командам безпеки та синього кольору 14 років тому як рідна багатопотокова система виявлення/запобігання вторгнень (IDS/IPS) і з тих пір постійно розвивається та вдосконалюється завдяки щедрій, активній спільноті та зусиллям колишніх і нинішніх членів консорціуму [10].

В даний час Suricata використовується різними комерційними постачальниками та проектами з відкритим вихідним кодом, від локальних розгортань до хмарних провайдерів, таких як AWS та інші.

Основні можливості Suricata:

Глибокий аналіз мережевого трафіку (Deep Packet Inspection)  
Suricata підтримує аналіз не лише заголовків, а й вмісту пакетів. Це дозволяє виявляти як відомі сигнатури атак, так і аномальну поведінку.

Підтримка сигнатур Snort  
Suricata сумісна зі сигнатурами, розробленими для Snort, що дозволяє швидко інтегрувати наявні бази правил без потреби створювати нові з нуля.

Модулі виявлення аномалій  
Окрім сигнатурного аналізу, Suricata підтримує поведінкове виявлення та модулі статистичного аналізу, що дає змогу ідентифікувати нові або змінені атаки.

Журналювання та логування  
Suricata генерує повні журнали подій, включно з HTTP-запитами, TLS-метаданими, DNS-запитами, потоками та алертами, які можна обробляти за допомогою SIEM-систем (наприклад, ELK Stack, Splunk).

Мультипотоковість та висока продуктивність  
Завдяки підтримці багатоядерності Suricata може обробляти великий обсяг трафіку, що робить її придатною для використання у середніх і великих мережах.

Suricata забезпечує реальний час виявлення загроз, що дозволяє аналітикам SOC (Security Operations Center) оперативно реагувати на потенційні інциденти. Зібрані дані (наприклад, повні HTTP-запити або метадані TLS-сесій) є надзвичайно корисними під час пост-інцидентного аналізу та цифрової криміналістики.

Особливо ефективною є інтеграція Suricata з інструментами:

ELK Stack (Elasticsearch, Logstash, Kibana) — для зберігання, фільтрації та візуалізації алертів та подій.

1.3.3Інтегровані рішення SIEM (Security Information and Event Management)

Системи SIEM надають можливості для централізованого збору, кореляції та аналізу подій безпеки з усіх компонентів ІТ-інфраструктури:

*ELK Stack* — це потужний інструментарій із відкритим вихідним кодом, що складається з трьох основних компонентів: Elasticsearch, Logstash та Kibana. Разом вони формують універсальну платформу для збирання, обробки, зберігання та візуалізації журналів подій. ELK Stack є однією з найпоширеніших реалізацій SIEM-системи у середовищі open-source і активно використовується для виявлення, моніторингу та розслідування кіберінцидентів в інформаційних системах організацій [11].

Складається с трьох компонентів:

Elasticsearch це високопродуктивна система зберігання та пошуку даних, побудована на основі Apache Lucene. Вона дозволяє ефективно індексувати великі обсяги журналів (логів) і забезпечує швидкий пошук та фільтрацію інформації. У контексті кібербезпеки Elasticsearch виконує функцію центрального сховища подій, з яких формується аналітика безпеки.

Logstash компонент для збору, парсингу, обробки та переспрямування журналів із різних джерел. Logstash підтримує десятки плагінів і дозволяє підключати системні логи серверів, журнали брандмауерів, IDS/IPS-систем, проксі-серверів, а також інструменти на зразок Suricata, Zeek, Wazuh тощо. Logstash стандартизує дані та готує їх до подальшого аналізу.

Kibana веб-інтерфейс для візуалізації даних, отриманих з Elasticsearch. За допомогою Kibana фахівці з безпеки можуть створювати дашборди, графіки, часові шкали та фільтри, що дозволяють швидко ідентифікувати інциденти, підозрілу активність, сканування мережі, аномалії тощо.

Застосування ELK Stack у кіберрозслідуваннях:

Централізований збір логів: з усіх хостів, мережевих пристроїв, додатків та систем безпеки;

Кореляція подій: можливість виявляти зв’язки між, здавалося б, розрізненими подіями, наприклад між логіном користувача, запуском процесу та передачею даних;

Інтеграція з IDS/IPS: як-от Suricata чи Zeek, для глибшого аналізу мережевого трафіку;

Побудова тимчасових ліній інцидентів (timeline): критично важливо для реконструкції дій атакувальника;

Алертинг: можливість налаштування правил для генерації попереджень у реальному часі [11].

Проведений аналіз сучасних інструментів та платформ для кіберрозслідувань дозволяє зробити висновок, що сьогодні існує широкий спектр рішень, які орієнтовані на різні аспекти цифрової криміналістики та реагування на інциденти.

Таким чином, вибір інструментів для проведення кіберрозслідувань має базуватись на конкретних потребах організації, рівні загроз, а також ресурсах, доступних для впровадження, налаштування та обслуговування відповідних рішень. Оптимальною є побудова гібридної архітектури, яка поєднує інструменти збору, аналізу пам’яті, мережевих інцидентів і централізованого моніторингу.

1. **АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ РОЗСЛІДУВАНЬ З КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ НА БАЗІ ELK STACK**

|  |  |
| --- | --- |
| **2.1** | **Архітектура та компоненти рішення ELK Stack** |

Перш ніж розглянемо архітектуру та компоненти рішення, необхідно мати базове поняття, що саме с себе представляє рішення ELK Stack.

ELK Stack — це комплексне open-source рішення для збору, обробки, зберігання та візуалізації логів. Назва утворена від перших літер основних компонентів: Elasticsearch, Logstash і Kibana, а також розширюється за рахунок Beats — легких агентів збору даних. Разом ці компоненти створюють потужну екосистему для аналізу логів, моніторингу інформаційної інфраструктури та виявлення кіберінцидентів.

Якщо поглянути на просту архітектуру самого ELK, то вона має в основі лише 3 компонента (рисунок 2.1)[12].

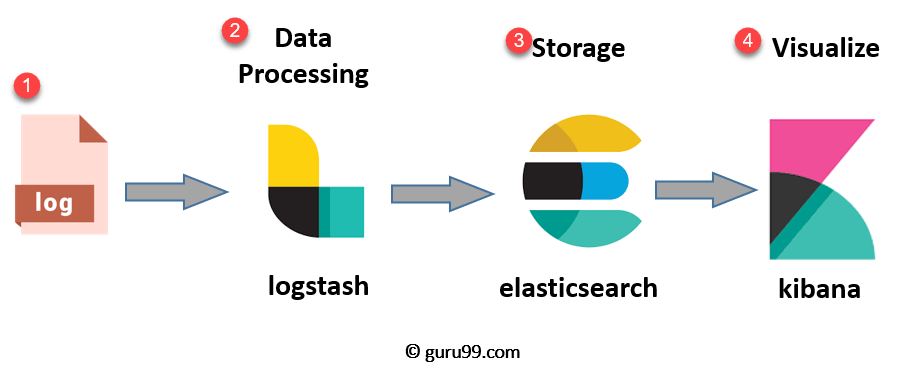


Рис. 2.1. Проста архітектура стеку ELK [12].

Для кращого розуміння принципів функціонування ELK Stack проаналізуємо послідовність взаємодії ключових компонентів системи під час обробки журналів подій:

Журнали: Визначаються серверні журнали, які потрібно проаналізувати;

Logstash: Збирайте журнали та дані про події. Він навіть аналізує та перетворює дані;

ElasticSearch: Перетворені дані з Logstash is Зберігати, шукати та індексувати.;

Кібана: Kibana використовує Elasticsearch DB для дослідження, візуалізації та спільного використання [12].

Однак потрібен ще один компонент або збір даних під назвою Beats. Це змусило Elastic перейменувати ELK на Elastic Stack (рисунок 2.2.)[12].

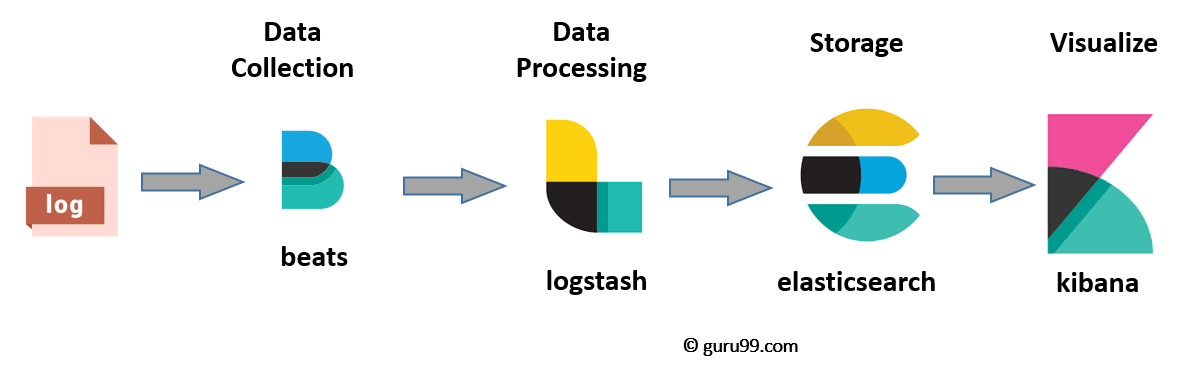


Рис. 2.2. Архітектура ELK Stack [12].

Під час роботи з дуже великими обсягами даних вам може знадобитися Kafka, RabbitMQ для буферизації та стійкості. Для безпеки можна використовувати nginx.

Таким чином, доповнення ELK Stack такими рішеннями, як Kafka, RabbitMQ та Nginx, дозволяє побудувати високодоступну, безпечну та масштабовану систему, придатну для корпоративного моніторингу безпеки та реагування на кіберінциденти в режимі реального часу (рисунок 2.3.)[12].

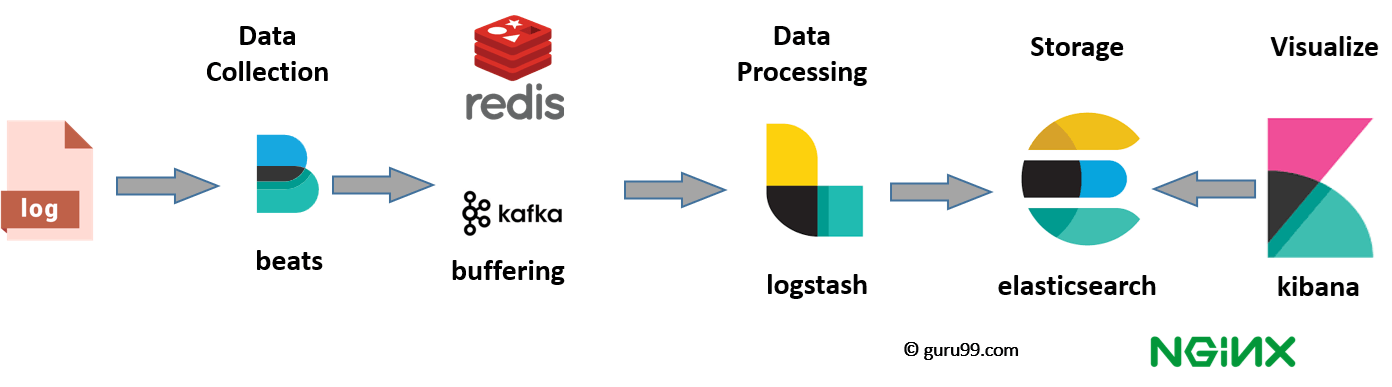


Рис. 2.3. Архітектура ELK Stack разом з Kafka, RabbitMQ та nginx [12].

Основна архітектура ELK Stack передбачає наступні рівні (рисунок 2.4.):

Рівень збору даних (Data Shipping)  
Цей рівень реалізується за допомогою Beats або зовнішніх засобів, які передають логи або метрики до Logstash чи Elasticsearch.

Рівень обробки (Data Processing)  
Logstash відповідає за прийом, обробку та маршрутизацію подій. Він трансформує неструктуровані дані у формат, придатний для аналізу.

Рівень зберігання (Data Indexing & Storage)  
Elasticsearch зберігає оброблені дані, індексує їх та забезпечує високошвидкісний пошук і аналітику.

Рівень візуалізації (Data Visualization)  
Kibana надає графічний інтерфейс для аналізу та моніторингу даних. Через Kibana здійснюється побудова дашбордів, аналітика та керування системою.

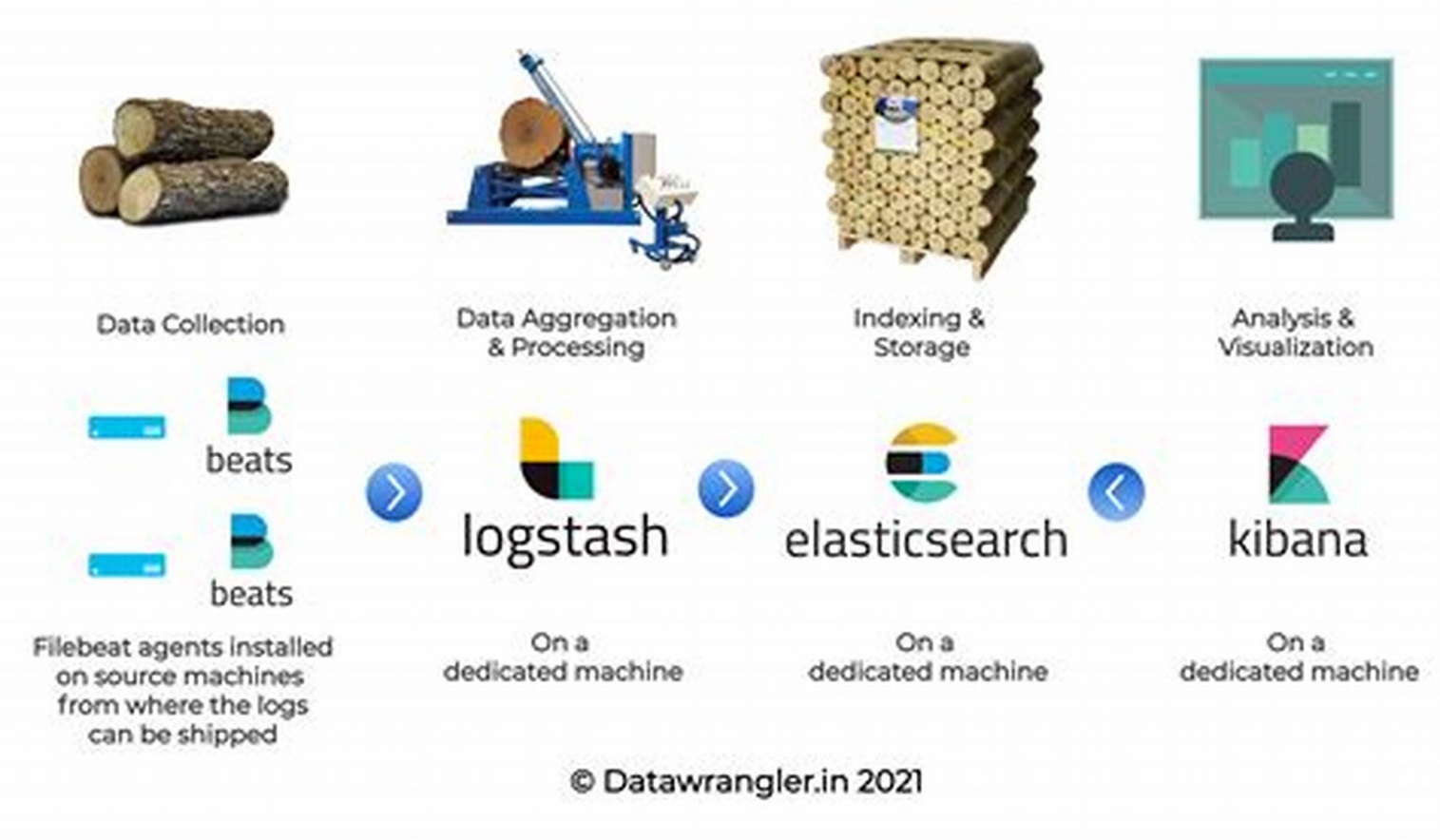


Рис. 2.4. Рівні ELK Stack

Архітектура рішення ELK Stack вирізняється модульністю, гнучкістю та здатністю обробляти великі обсяги даних у реальному часі. Компоненти системи — Elasticsearch, Logstash та Kibana — інтегруються у єдину аналітичну платформу, яка забезпечує повний цикл обробки подій: від збору логів до їх візуалізації. Завдяки масштабованості та розширюваності, ELK Stack може бути адаптований до потреб як малого бізнесу, так і великих корпоративних середовищ.

Додаткове включення таких компонентів, як Beats, Kafka або Nginx, дозволяє суттєво підвищити надійність, продуктивність і безпеку платформи. Це робить ELK Stack одним із провідних рішень для моніторингу, аналізу та кіберрозслідувань в інформаційних системах організацій.

|  |  |
| --- | --- |
| **2.2** | **Призначення та основні функції компонентів ELK Stack** |

ELK Stack розроблений, щоб дозволити користувачам отримувати дані з будь-якого джерела в будь-якому форматі, а також шукати, аналізувати та візуалізувати ці дані в режимі реального часу [12].

*Elasticsearch* – це справжнє «серце» ELK Stack. Мова йде про потужний пошуковий й аналітичний двигун. Він розроблений на базі Apache Lucene — відомої бібліотеки для повнотекстового пошуку, і спеціально призначений для роботи з великими обсягами структурованих і неструктурованих даних.

Основні характеристики:

Elasticsearch надає потужні можливості для швидкого та ефективного повнотекстового пошуку. Він може знаходити відповідність між запитами користувача та документами, навіть якщо вони містять велику кількість даних;

інструмент проводить аналіз даних, включаючи агрегацію, фільтрацію, групування та підрахунки, щоб зрештою отримати цінні інсайти;

Elasticsearch розроблений з урахуванням розподіленої архітектури, що дозволяє легко масштабувати систему на багато вузлів для обробки великих обсягів даних та забезпечує високу доступність;

інструмент спроектований для роботи в реальному часі, щоб оперативно оновлювати дані та отримувати результати запитів без значних затримок;

Elasticsearch — це база даних NoSQL, а також відкрите програмне забезпечення. Його можна безкоштовно використовувати та адаптувати під свої потреби. Крім того, він підтримує багато розширень і плагінів для різноманітних завдань. Він має вбудовані можливості для обробки текстових даних, включаючи пошук по аналогії, токенізацію, стемінг та багато інших операцій для точного та розширеного пошуку [13].

*Особливості еластичного пошуку:*

Сервер пошуку з відкритим кодом написаний за допомогою Java;

Використовується для індексування різнорідних даних будь-якого типу;

Має веб-інтерфейс REST API з виведенням JSON;

Повнотекстовий пошук;

Пошук у майже реальному часі (NRT);

Сховище документів у форматі JSON із можливістю реплікації та пошуку;

Розподілене сховище документів на основі REST і JSON без схем;

Підтримка кількох мов і геолокації [12].

*Переваги Elasticsearch*

Зберігайте дані без схеми, а також створюйте схему для ваших даних;

Керуйте своїми записами даних за записами за допомогою багатодокументних API;

Виконуйте фільтрацію та надсилайте запити на дані, щоб отримати статистику;

Базується на Apache Lucene та надає RESTful API;

Забезпечує горизонтальну масштабованість, надійність і багатокористувацький потенціал для використання індексування в реальному часі для пришвидшення пошуку;

Допомагає масштабувати по вертикалі та горизонталі.

Logstash – це інструмент для збирання, перетворення та обробки даних з різних джерел. Його часто використовують разом з Elasticsearch та Kibana в ELK stack для аналізу та візуалізації даних.

Основні характеристики:

Logstash збирає дані з різних джерел: лог-файли, потоки даних, бази даних, метрики системи, системні події та багато інших. Він підтримує багато вхідних плагінів для різних джерел;

після збирання даних Logstash може виконувати різні операції над ними. Зокрема, це фільтрація, структурування, нормалізація та збагачення для подальшого аналізу;

Logstash підтримує велику кількість вихідних плагінів для відправлення оброблених даних до різних систем та сховищ, включаючи Elasticsearch, Apache Kafka, Amazon S3 і багато інших;

інструмент надає розширені можливості обробки даних: парсинг регулярних виразів, геопросторовий аналіз та обробку структурованих форматів даних JSON і CSV.

Logstash надає гнучкі можливості конфігурації. Користувачі можуть визначити, як дані треба зібрати та обробити [13].

Logstash може уніфікувати дані з різних джерел і нормалізувати дані у бажаних місцях призначення. Він складається з трьох компонентів:

вхід: передача журналів для їх обробки у зрозумілий машині формат;

фільтри: це набір умов для виконання певної дії чи події;

вихід: засіб прийняття рішень щодо обробленої події або журналу.

*Особливості Logstash.* Щоб отримати результат потрібно знати про функціонал кожного компоненту, тому дізнаємося про функції LogStash:

Події проходять через кожну фазу за допомогою внутрішніх черг;

Дозволяє різні входи для ваших журналів;

Фільтрування/розбір ваших журналів.

*Переваги Logstash* мають не меншу цінність, аніж його особливості, розглянемо основні:

Пропозиції централізують обробку даних;

Він аналізує велику різноманітність структурованих/неструктурованих даних і подій;

ELK LogStash пропонує плагіни для підключення до різних типів джерел введення та платформ [12].

**Kibana -** це інструмент для візуалізації та аналізу даних. Він використовується для створення графіків, дашбордів та звітів на основі даних, які зберігаються в Elasticsearch. Kibana дозволяє користувачам інтерактивно візуалізувати та аналізувати дані, робити запити та отримувати візуальні інсайти.

Основні функції та характеристики:

Kibana надає можливість створювати різноманітні типи візуалізацій: лінійні графіки, стовпчасті діаграми, колеса підписів, графіки розсіювання та інші;

користувачі можуть об'єднувати різні візуальні компоненти (графіки, таблиці, метрики) на дашбордах з метою створення комплексних інтерактивних панелей для моніторингу та аналізу даних;

дає можливість користувачам фільтрувати дані за різними параметрами, щоб досліджувати конкретні аспекти даних або подій;

доступні інструменти для аналізу даних, включаючи відображення та відстеження змін в часі, розрахунок агрегатів, фільтрація та сортування;

Kibana підтримує створення карт і географічних візуалізацій для аналізу інформації, яка містить геодані.

Інструмент підтримує систему ролей, що дозволяє адміністраторам контролювати доступ до функціональності та даних [13].

*Особливості Kinbana:*

Потужна інтерфейсна інформаційна панель, яка здатна візуалізувати індексовану інформацію з еластичного кластера;

Вмикає пошук індексованої інформації в реальному часі;

Ви можете шукати, переглядати та взаємодіяти з даними, що зберігаються в Elasticsearch;

Виконуйте запити до даних і візуалізуйте результати в діаграмах, таблицях і картах;

Інформаційна панель, що налаштовується, дозволяє розділяти журнали logstash у elasticsearch;

Здатність надавати історичні дані у вигляді графіків, діаграм тощо;

Інформаційні панелі в реальному часі, які легко налаштовуються;

Kibana ElasticSearch забезпечує пошук проіндексованої інформації в режимі реального часу.

*Переваги та недоліки Кінбана:*

Легка візуалізація;

Повністю інтегрований з Elasticsearch;

Інструмент візуалізації;

Пропонує аналіз у реальному часі, діаграми, узагальнення та можливості налагодження;

Забезпечує інтуїтивний і зручний інтерфейс;

Дозволяє обмінюватися знімками журналів, у яких проводився пошук;

Дозволяє зберігати інформаційну панель і керувати кількома інформаційними панелями [12].

Дослідивши всі компоненти нашого рішення, можемо зробити висновок, що саме плюси ELK Stack:

всі компоненти стека — відкриті програми, тож можна безкоштовно використовувати їх і адаптувати під свої потреби;

ELK стек легко масштабується, що дає можливість додавати нові вузли для обробки більшого обсягу даних;

ELK stack підтримує обробку даних в реальному часі, що дозволяє виявляти проблеми та аналізувати події негайно;

стек можна масштабувати горизонтально, щоб відповідати зростаючим обсягам даних і вимогам користувачів;

ELK stack можна налаштувати відповідно до різних випадків використання, від ІТ-операцій і аналітики безпеки до маркетингових досліджень.

Тобто саме рішення функціоную чудово і полегшую проведення розслідування в інформаційних системах в організаціях, але в кожній системі і кожному рішенні бувають і недоліки, саме в цьому питанні зустрілись такі мінуси:

налаштування і розгортання ELK stack достатньо складне;

набір програмних продуктів вимагає значних обсягів обчислювальних ресурсів та пам’яті для ефективної роботи з великими обсягами даних;

для максимальної користі від ELK стеку потрібно мати навички в аналізі даних та розробці дашбордів;

система вимагає постійного моніторингу й обслуговування.

Спочатку ELK stack використовували лише для аналізу логів і моніторингу систем. Протягом років він став популярним інструментом для різноманітних завдань, включаючи вебаналітику, обробку подій, безпеку, аналітику застосунків та багато іншого. Elastic також надала комерційні рішення та підтримку для організацій, які шукають розширені можливості та підтримку.

Загалом, ELK stack — це потужний і гнучкий інструмент для збору, аналізу та візуалізації даних, який знаходить застосування в багатьох галузях. Він має активну спільноту користувачів і багато ресурсів для навчання та підтримки.

* 1. **Процеси функціонування рішення ELK Stack**

ELK Stack функціонує як єдина система збору, обробки, зберігання та візуалізації логів, що дозволяє реалізувати повний цикл реагування на інциденти та підтримувати безперервний моніторинг інформаційної інфраструктури. Робота рішення базується на послідовній обробці подій через інтегровані компоненти системи.

*Збір даних.* На початковому етапі агенти Beats або зовнішні джерела (системи, сервери, мережеві пристрої) генерують логи, метрики або події. Beats, як найпоширеніший інструмент збору, забезпечує:

безперервну доставку логів у реальному часі;

легкість розгортання на клієнтських машинах;

підтримку багатьох типів логів (системні, мережеві, користувацькі).

Іноді джерела надсилають події напряму у Logstash, особливо якщо дані потребують обробки.

*Обробка та трансформація даних.* На цьому етапі Logstash або Ingest pipelines в Elasticsearch виконують наступні функції:

Нормалізація: перетворення логів у структурований формат (наприклад, JSON);

Фільтрація: вилучення зайвих полів, перетворення часових міток, уніфікація IP-адрес тощо;

Збагачення: додавання метаінформації, геолокації, інформації про користувача або пристрій;

Виявлення подій: визначення шаблонів, що свідчать про потенційні інциденти.

*Індексація та зберігання.* Оброблені дані надходять до Elasticsearch, де вони зберігаються у вигляді індексів. Основні процеси тут:

Індексація кожного документа з повнотекстовим пошуком;

Розподіл навантаження між нодами кластера (якщо є кілька серверів);

Виконання запитів і агрегацій для подальшого аналізу.

Elasticsearch забезпечує масштабованість, надійне зберігання даних і швидкий доступ до великого обсягу логів.

Візуалізація та аналіз. Kibana слугує інтерфейсом користувача для:

пошуку подій за часовими мітками, користувачами, IP-адресами тощо;

побудови дашбордів для виявлення аномалій;

використання визначених правил безпеки, які реагують на підозрілу активність;

створення звітів і графіків для аналітичної роботи;

інтеграції з інструментами сповіщення (email, Slack, Webhook тощо).

Автоматичне реагування (опціонально). У поєднанні з модулем Elastic Security або зовнішніми системами можна реалізувати:

виявлення індикаторів компрометації (IoC);

автоматичну генерацію інцидентів;

інтеграцію з SIEM-рішеннями або SOAR-системами для реагування.

Слідуючи всім вище перечисленими підрахунками, можна зробити висновок, що процеси функціонування ELK Stack охоплюють усі ключові етапи роботи з логами — від збору до аналізу. Такий підхід забезпечує прозорість, гнучкість і оперативність в управлінні інформаційною безпекою організації. ELK Stack не лише допомагає виявляти інциденти, але й створює умови для побудови комплексної системи кіберрозслідувань.

1. **РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПРОВЕДЕННЯ РОЗСЛІДУВАНЬ З КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ**

**3.1** **Варіант розгортання системи проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK STACK**

Архітектура рішення ELK Stack насамперед передбачає кілька взаємопов’язаних рівнів:  
 Рівень збору даних: джерела логів — сервери, мережеве обладнання, системи безпеки (наприклад, файрволи, IDS/IPS), а також кінцеві точки;  
 Рівень обробки: Logstash або Beats збирає дані з джерел, виконує фільтрацію, нормалізацію, обробку;  
 Рівень зберігання та пошуку: Elasticsearch зберігає індексовані дані для подальшого аналізу;  
 Рівень візуалізації: Kibana надає зручний інтерфейс для створення дашбордів, побудови аналітики та розслідувань.

Також слід зазначити основні компоненти системи:

Filebeat/Winlogbeat — агенти, які встановлюються на клієнтські машини або сервери для збору логів;  
 Logstash — відповідає за фільтрацію, парсинг і маршрутизацію логів;  
 Elasticsearch — високопродуктивний рушій для зберігання, пошуку й аналітики;  
 Kibana — веб-інтерфейс для візуального аналізу логів і побудови панелей моніторингу;  
 Wazuh (опціонально) — розширення для моніторингу безпеки, інтегрується з ELK.

Стосовно етапів впровадження, розглянемо таку послідовність подій та поступово розберемо кожну з них:

Оцінка потреб та визначення джерел логів (сервери, програми, мережа);

Розгортання Filebeat/Winlogbeat на джерелах логів;

Конфігурація Logstash для обробки подій;

Налаштування Elasticsearch для зберігання індексованих логів;  
Розгортання Kibana для побудови візуалізацій та розслідувань;  
Створення шаблонів дашбордів та правила кореляції для виявлення аномалій;

Налаштування резервного копіювання, ролей доступу та аудиту дій користувачів.

Самим головним в етапах впровадження, буде саме конфігурація та налаштування основних компонентів по типу Logstash, Elasticsearch, Kibana.

*Logstash* – утиліта для обробки подій журналу з різних джерел, за допомогою якої можна виділити поля та їх значення у повідомленні, також можна налаштувати фільтрацію та редагування даних. Після всіх маніпуляцій Logstash перенаправляє події в сховище даних призначення. Утиліта налаштовується тільки через конфігураційні файли [14].

Типова конфігурація журналу — це файл(и), що складається з кількох вхідних потоків, кількох фільтрів для цієї інформації та кількох вихідних потоків. Виглядає він як один або кілька конфігураційних файлів, що в найпростішому варіанті (який взагалі нічого не робить) виглядає так (рисунок 3.1)[14]:



Рис. 3.1. Типова конфігурація журналу [14].

У INPUT ми налаштовуємо, в які журнали портів будуть відправлятися і за яким протоколом, або з якої папки читати нові або постійно додаються файли.

У FILTER ми налаштували парсер логів: парсинг полів, редагування значень, додавання нових параметрів або їх видалення. FILTER — це поле керування повідомленнями, яке приходить до Logstash із безліччю опцій редагування.

У OUTPUT налаштовуємо куди відправляти вже розібраний лог, в разі, якщо відправляється еластичний пошуковий JSON-запит, в якому відправляються поля зі значеннями, або в рамках налагодження, можна вивести його в stdout або записати в файл (рисунок 3.2)[14].

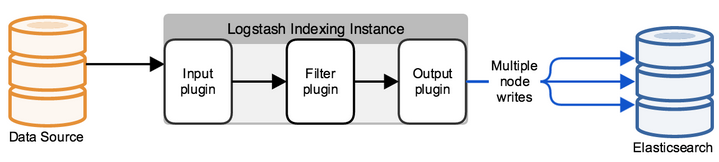


Рис. 3.2. Приклад правильного налаштування конфігурації [14].

Настав час до другої конфігурації, а саме еластичний пошук.

Спочатку *Elasticsearch* — це рішення для повнотекстового пошуку, але з додатковими зручностями, такими як легке масштабування, реплікація та інші речі, що зробило продукт дуже зручним і хорошим рішенням для високонавантажених проектів з великими обсягами даних. Elasticsearch — це нереляційне (NoSQL) сховище документів у форматі JSON, а також пошукова система, заснована на повнотекстовому пошуку Lucene. Апаратною платформою є Java Virtual Machine, тому для роботи системи потрібна велика кількість ресурсів процесора та оперативної пам'яті [14].

Кожне вхідне повідомлення, як і у випадку з Logstash або за допомогою API запиту, індексується як «документ» – аналогічно таблиці в реляційному SQL. Всі документи зберігаються в індексі, аналогічно базі даних в SQL. Це можна побачити саме на цьому рисунку, куди і яким чином ідуть записи та який візуал має (рисунок 3.3)[14]:  
Изображение выглядит как текст, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 3.3. Приклад документа в базі даних [14].

Вся робота з базою даних базується на JSON-запитах з використанням REST API, які або видають документи по індексу, або якусь статистику в форматі питання-відповідь. Для того, щоб візуалізувати всі відповіді на запити, була написана Kibana, яка є веб-сервісом [14].

Для більш глибокого розуміння, як саме Кібана візуалізую всі відповіді, розберемо функціонал Кібани.

*Kibana* дозволяє шукати/брати дані та запитувати статистику з бази даних elasticsearch, але на основі відповідей побудовано безліч красивих графіків та дашбордів. Система також має функціонал адміністрування бази даних elasticsearch. А тепер покажемо приклад дашбордів для брандмауера Check Point (рисунок 3.4)[14] і сканера вразливостей OpenVas (рисунок 3.4)[14], які можна побудувати [14].

Изображение выглядит как текст, снимок экрана, диаграмма, График

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 3.4. Приклад дашборду для Check Point [14].

Изображение выглядит как текст, снимок экрана, диаграмма, число

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 3.5. Приклад дашборду для OpenVas [14].

Дослідивши дане питання можна зробити висновки і підсумувати, що ми розглянули, з чого складається стек ELK, ознайомилися з основними продуктами, далі розглянули найпростіше написання конфігураційного файлу Logstash, візуал дашбордів на Kibana, ознайомимося із запитами API.

**3.2 Порядок проведення розслідувань з кібербезпеки в рішенні ELK Stack**

Розслідування кіберінцидентів в інформаційній системі на основі ELK Stack (Elasticsearch, Logstash, Kibana) передбачає реалізацію низки чітко визначених етапів, які охоплюють повний життєвий цикл події: від виявлення інциденту до формування аналітичного звіту. ELK Stack забезпечує можливість ефективного аналізу великих обсягів логів, їх фільтрацію, збагачення, зберігання, а також візуалізацію для прийняття рішень.

*Перший крок* проведення розслідування стартує з первинного збору та агрегації логів

Першим етапом розслідування є налаштування збору журналів із різних джерел:

серверів;

мережевих пристроїв;

прикладних сервісів;

хмарних платформ.

Для цього застосовуються агенти Filebeat, Auditbeat, Packetbeat та інші. Зібрані дані передаються до Logstash, який виконує попередню обробку — очищення, збагачення (наприклад, геолокація IP) та нормалізацію.

Взагалі кожен агент функціоную по різному, тому проаналізуємо перші три і на фоні цього зможемо зробити висновок.

*Filebeat* постачається з модулями для спостереження та безпеки джерел даних, які спрощують збір, аналіз та візуалізацію поширених форматів журналів до однієї команди. Вони досягають цього, поєднуючи автоматичні шляхи за замовчуванням на основі вашої операційної системи, з визначеннями конвеєра Elasticsearch Ingest Node і з інформаційними панелями Kibana. Крім того, кілька модулів Filebeat постачаються з попередньо налаштованими завданнями машинного навчання (рисунок 3.6)[15].

Изображение выглядит как текст, Шрифт, снимок экрана

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 3.6. Дашборд Filebeat [15]

Це не дозволить вам перевантажити воронку продажів, Filebeat використовує протокол, чутливий до зворотного тиску, під час надсилання даних до Logstash або Elasticsearch, щоб врахувати більші обсяги даних. Якщо Logstash зайнятий обробкою даних, він повідомляє Filebeat про необхідність уповільнити їх читання. Як тільки затори будуть вирішені, Filebeat повернеться до свого початкового темпу та продовжить доставляти (рисунок 3.7)[15].

Изображение выглядит как текст, снимок экрана, диаграмма, Шрифт

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 3.7. Протокол, чутливий до зворотнього тиску [15].

Auditbeat дозволяє нам відстежувати активність користувачів і процеси, а також аналізувати дані про свої події в Elastic Stack, не торкаючись перевірених. Auditbeat зв'язується безпосередньо з аудиторською структурою Linux, збирає ті ж дані, що й аудит, і відправляє події в Elastic Stack в режимі реального часу. Якщо ви відчуваєте ностальгію, ви можете запустити аудит разом з Auditbeat (у новіших ядрах) (рисунок 3.8)[16].

Не переписуйте те, що працює. Використовуйте існуючі правила аудиту, щоб безболісно отримувати дані. Хто був актором? Які дії вони виконували і коли? Auditbeat зберігає всі вихідні дані системних викликів і пов'язані з ними шляхи, щоб у вас був потрібний контекст.

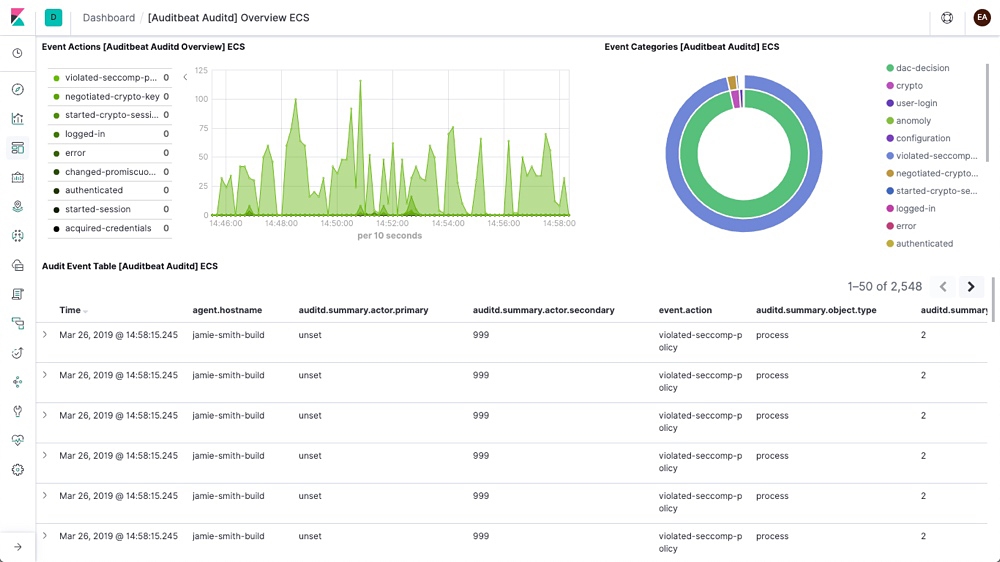


Рис. 3.8. Дашборд Auditbeat [16].

Auditbeat дозволяє уважно стежити за списками директорій для будь-якого смішного бізнесу на Linux, macOS і Windows. Зміни у файлі надсилаються в Elasticsearch у режимі реального часу, кожне повідомлення містить метадані та криптографічні хеші вмісту файлу для подальшого аналізу.

Просто вкажіть шляхи до каталогів, які ви хочете, щоб Auditbeat дивився, і зробіть вітальний ковток кави.

Auditbeat є частиною Elastic Stack, що означає, що він бездоганно працює з Logstash, Elasticsearch і Kibana. Незалежно від того, чи хочете ви трансформувати або збагатити свої показники за допомогою Logstash, повозитися з аналітикою в Elasticsearch або створювати та ділитися інформаційними панелями в Kibana, Auditbeat дозволяє легко відправляти ваші дані туди, де це найважливіше.

На цьому етапі розглянемо також агента під назвою Packetbeat

Моніторинг мережевого трафіку має вирішальне значення для отримання спостережуваності та захисту вашого середовища, забезпечуючи високий рівень продуктивності та безпеки. Packetbeat — це легкий мережевий аналізатор пакетів, який надсилає дані з ваших хостів і контейнерів у Logstash або Elasticsearch.

Packetbeat – це також бібліотека. Він підтримує безліч протоколів прикладного рівня, від бази даних до сховищ ключ-значення до HTTP і протоколів низького рівня. Виберіть потрібний, або додайте свій, відправивши запит на пул (рисунок 3.9)[17].

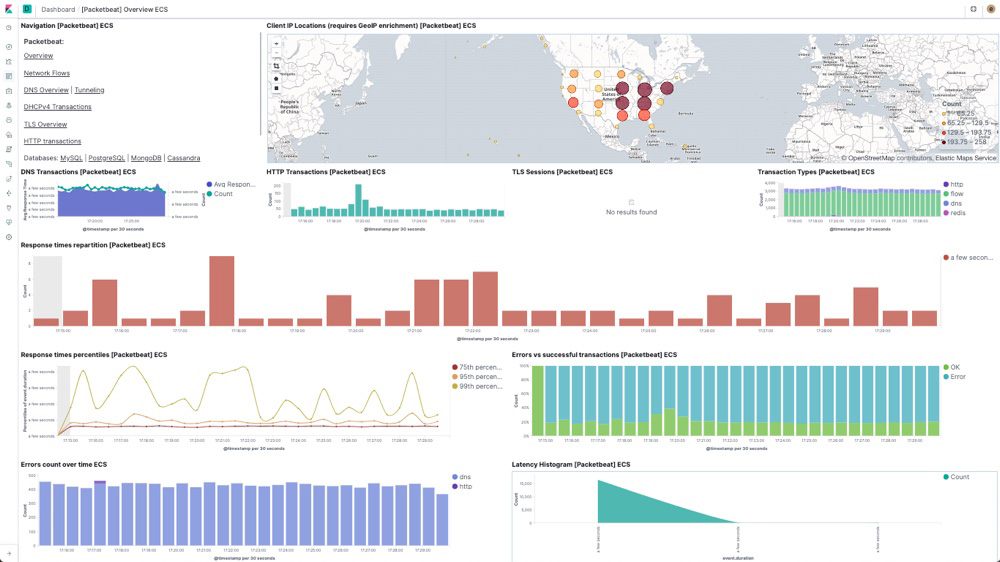


Рис. 3.9. Дашборд Packetbeat [17].

Завдяки пошуку та аналізу мережевого трафіку, ви можете відмовитись від виконання різноманітних заклинань, щоб привести дані в належну форму для пошуку та аналізу. Packetbeat піклується про це за вас у режимі реального часу, на ваших цільових серверах (рисунок 3.10)[17].

Изображение выглядит как текст, Шрифт, диаграмма, линия

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 3.10. Пошук та аналіз мережевого трафіку [17].

*Другий крок* проведення розслідування, обробка та фільтрація даних (Logstash)

Logstash виконує критично важливу роль у процесі розслідування:

фільтрація нерелевантних подій;

збереження структурованих полів;

збагачення даних метаінформацією (наприклад, user agent, країна IP);

розподіл подій за категоріями (успішні/неуспішні логіни, командні дії, помилки тощо).

*Третій крок* розслідування, зберігання та пошук (Elasticsearch)

Після обробки дані надходять до Elasticsearch, який виступає індексаційною базою:

забезпечує швидкий пошук по мільйонах записів;

підтримує запити на основі фільтрів, мови Lucene або DSL;

дозволяє створювати агрегації для виявлення шаблонів.

При розслідуванні Elasticsearch дає змогу:

швидко знайти всі події з IP-адресою, яка проявила підозрілу активність;

переглянути історію дій певного користувача;

створити тимчасові запити для побудови гіпотез.

*Наступний крок*, аналіз, кореляція та візуалізація даних (Kibana)

Kibana надає зручний інтерфейс для побудови графіків, панелей моніторингу та детального аналізу (рисунок 3.11)[18]:

аналіз трендів активності (наприклад, підвищення кількості запитів з певного регіону);

кореляція подій (наприклад, спроба доступу + зміна пароля);

дослідження конкретних записів у розрізі часу, IP-адреси, користувача, тощо;

створення алертів (наприклад, коли кількість невдалих логінів перевищує певний поріг).

Изображение выглядит как текст, снимок экрана, диаграмма, График

Контент, сгенерированный ИИ, может содержать ошибки.

Рис. 3.11. Дашборд Kibana [18].

Є також не менш важливий момент це - документування та формування звітності.

Після аналізу всі зібрані докази та висновки формалізуються у звіт:

опис виявлених інцидентів;

деталізація підозрілих подій;

рекомендації щодо усунення загроз;

експорт візуалізацій Kibana (графіки, heatmaps, таблиці).

*Фінальний крок* в нашому розслідуванні, звичайно ж постінцидентна оптимізація

Після завершення розслідування важливо:

оновити правила фільтрації Logstash;

змінити пороги тригерів алертів;

проаналізувати слабкі місця системи моніторингу.

Постінцидентна оптимізація — це критичний етап, який перетворює інцидент на навчальний кейс, підвищуючи стійкість інформаційної системи до майбутніх атак. Систематичний перегляд налаштувань ELK Stack після кожного інциденту дозволяє не лише покращити виявлення загроз, а й сформувати культуру безперервного вдосконалення кіберзахисту в організації.

**3.3 Рекомендації щодо проведення розслідувань з кібербезпеки в інформаційній системі організації**

На основі проведеного дослідження, присвяченого застосуванню рішення ELK Stack для виявлення та аналізу кіберінцидентів в інформаційній системі організації, сформульовано низку рекомендацій щодо побудови ефективної системи реагування на інциденти безпеки. Ці рекомендації охоплюють аспекти технічної реалізації, процедурного управління, а також питання аналітики та цифрової криміналістики. Особлива увага приділяється можливостям обробки логів, автоматизації пошуку аномалій та забезпеченню доказової бази для подальшого аналізу подій.

*Рекомендації щодо технічного моніторингу та виявлення загроз.* Для забезпечення високого рівня виявлення кіберзагроз у реальному часі рекомендовано використовувати ELK Stack як основу для системи моніторингу безпеки (SIEM). ELK Stack складається з трьох основних компонентів: Elasticsearch, Logstash і Kibana, які забезпечують збір, обробку, індексацію, збереження та візуалізацію подій з логів систем.

Додатково доцільно:

Використовувати Filebeat/Winlogbeat для збору логів з кінцевих точок;

Інтегрувати Suricata як джерело подій IDS-рівня, що дозволяє автоматично аналізувати мережевий трафік і виявляти ознаки атак;

Використовувати ElastAlert, Wazuh або Sigma-регулярки для налаштування правил сповіщення про підозрілу активність;

Здійснювати агрегацію логів з усіх критичних вузлів системи: шлюзів, серверів, файрволів, систем автентифікації;

Забезпечити розмежування доступу до Kibana через зворотній проксі-сервер (наприклад, Nginx) для безпечного управління панелями.

*Організаційні заходи та політика безпеки*. Інформаційна система повинна мати узгоджені процедури реагування на інциденти, які базуються на міжнародних стандартах (наприклад, NIST SP 800-61). Важливо:

Призначити відповідальних за моніторинг та реагування на інциденти;

Впровадити регламент роботи з інцидентами: від виявлення до документування та усунення;

Забезпечити резервне копіювання логів та індексів Elasticsearch для можливості подальшого аналізу та юридичного супроводу;

Проводити періодичні внутрішні аудити з метою перевірки коректності логування та наявності повних слідів подій [1].

*Аналітика, візуалізація та криміналістика.*

Розробити дашборди в Kibana для відстеження підозрілих входів, сканувань портів, Brute Force-атак, експлойтів тощо;

Використовувати візуалізації з кореляцією подій для побудови хронології атак;

Встановити метрики ефективності реагування (середній час виявлення/усунення, кількість інцидентів за місяць тощо);

У разі інциденту — виконати експорт логів, збереження сесій та трасування джерела атаки з подальшим аналізом за допомогою інструментів цифрової криміналістики (Autopsy, Volatility);

Дотримуватися принципів ланцюга зберігання доказів, зокрема забезпечення незмінності логів і контроль доступу до них.

*Підвищення обізнаності персоналу*. Незалежно від технічного рівня захисту, людський фактор залишається критичною ланкою. З метою зниження ймовірності компрометації системи через соціальну інженерію чи необачність працівників, рекомендовано:

Проводити навчання працівників щодо безпечної роботи з електронною поштою, носіями даних, онлайн-ресурсами;

Залучати користувачів до імітаційних сценаріїв фішингу для тестування їхньої обізнаності;

Розміщувати швидкі інструкції дій при підозрі на інцидент у внутрішній документації організації.

*Висновки рекомендацій*

Запропоновані заходи дозволяють створити на базі ELK Stack гнучке, масштабоване рішення, яке ефективно підтримує процеси виявлення, аналізу та реагування на кіберінциденти. Інтеграція інструментів цифрової криміналістики, застосування процедур обробки логів, організаційних політик та навчання персоналу забезпечує побудову цілісної системи кіберзахисту, що враховує як технічні, так і процедурні аспекти безпеки.

**ВИСНОВКИ**

Дослідили сутність проблеми проведення розслідувань з кібербезпеки в інформаційній системі організації та було встановлено, що розслідування інцидентів кібербезпеки є складним процесом, який вимагає залучення технічних, організаційних і правових засобів. Основні проблеми полягають у недостатньому рівні підготовки персоналу, відсутності належних технічних засобів моніторингу та аналізу, труднощах в ідентифікації джерел загроз, а також у необхідності дотримання вимог нормативно-правових актів під час збору та обробки цифрових доказів.

Проаналізували основні підходи до проведення розслідувань з кібербезпеки в інформаційній системі організації. У результаті аналізу було визначено, що існують різноманітні підходи до проведення кіберрозслідувань: традиційні форензичні методи, реагування на інциденти, а також сучасні автоматизовані рішення на основі SIEM-систем. Найефективніші підходи поєднують моніторинг у реальному часі, ретельний збір логів, виявлення аномалій і використання баз знань IoC та TTPs.

Проаналізували існуючі рішення із проведення розслідувань з кібербезпеки в інформаційній системі організації. Було досліджено й оцінено низку популярних інструментів та рішень: SIEM-системи, EDR-рішення, а також відкриті стекові платформи (наприклад, ELK Stack). Рішення на базі ELK відзначаються гнучкістю, масштабованістю та відсутністю ліцензійних обмежень, що робить їх особливо привабливими для організацій з обмеженим бюджетом. Проте для їх ефективного застосування потрібні технічні знання для налаштування та підтримки.

Проаналізували методи та засоби проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack. Було з’ясовано, що ELK Stack (Elasticsearch, Logstash, Kibana) у поєднанні з Beats та інструментами безпеки (наприклад, Wazuh) дозволяє ефективно збирати, зберігати, аналізувати та візуалізувати дані про кіберінциденти. Elasticsearch забезпечує швидкий пошук і аналітику, Logstash – обробку логів, Kibana – зручну візуалізацію, а Beats – збір даних з різних джерел. Разом ці інструменти утворюють потужну платформу для розслідувань.

Запропонували варіант системи проведення розслідувань з кібербезпеки в інформаційній системі організації на базі ELK Stack. Було запропоновано архітектуру системи розслідувань, що включає агенти збору даних (Filebeat, Winlogbeat), обробку даних у Logstash, збереження в Elasticsearch і аналітику в Kibana. Додатково інтегрується Wazuh для розширеного моніторингу безпеки та управління інцидентами. Така система дозволяє оперативно виявляти загрози, досліджувати інциденти та вживати відповідних заходів.

Розробили рекомендації щодо застосування методів та засобів проведення розслідувань з кібербезпеки в інформаційній системі організації. Надано низку практичних рекомендацій, серед яких: регулярний збір та зберігання логів, використання ELK Stack з інтеграцією безпекових модулів, створення сценаріїв виявлення підозрілої активності, автоматизація сповіщень та створення панелей моніторингу. Також підкреслено важливість навчання персоналу та розробки внутрішніх політик реагування на інциденти.

У результаті виконання роботи було комплексно досліджено питання проведення розслідувань інцидентів кібербезпеки в інформаційних системах організацій. Аналіз сутності проблеми показав, що зростання кількості та складності кіберзагроз вимагає від організацій наявності ефективних систем виявлення, реагування та аналізу інцидентів безпеки.

Отримані результати мають практичне значення і можуть бути використані для підвищення рівня кіберзахисту, покращення реагування на інциденти та забезпечення цифрової форензики в умовах сучасного кіберсередовища.

**ПЕРЕЛІК ПОСИЛАНЬ**

1. 2012. NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> (дата звернення: 14.05.2025).
2. 2024. Загрози-2025: звіт Fortinet про майбутні тренди, ризики та рішення у галузі кібербезпеки. URL: [Звіт Fortinet 2025: кіберзагрози, тренди та рішення](https://my-itspecialist.com/zvit-fortinet-zagrozy-2025-kiberbezpeka) (дата звернення: 14.05.2025).
3. 2024. What is Digital Forensics? Phases of Digital Forensics in Cybersecurity. URL: [Що таке цифрова криміналістика? Ключові етапи кібербезпеки | Рада ЄС](https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-digital-forensics/) (дата звернення: 14.05.2025).
4. 2023. What are the 4 phases of digital forensics? URL: [What are the 4 phases of digital forensics? - Darwin's Data](https://darwinsdata.com/what-are-the-4-phases-of-digital-forensics/) (дата звернення: 14.05.2025).
5. 2022. The Cyber Kill Chain: The Seven Steps of a Cyberattack. URL: [Seven Steps Of Cyber Kill Chain Process in Cyberattack | EC-Council](https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/cyber-kill-chain-seven-steps-cyberattack/) (дата звернення: 14.05.2025).
6. 2007. About The Volatility Foundation. URL: [About Volatility Foundation & Volatility Framework - The Volatility Foundation - Promoting Accessible Memory Analysis Tools Within the Memory Forensics Community](https://volatilityfoundation.org/about-volatility/) (дата звернення: 14.05.2025).
7. 2022. Memory forensics tools: a comparative analysis. URL: [Memory forensics tools: a comparative analysis: Journal of Cyber Security Technology: Vol 6 , No 3 - Get Access](https://www.tandfonline.com/doi/full/10.1080/23742917.2022.2100036?scroll=top&needAccess=true) (дата звернення: 14.05.2025).
8. 2003. Autopsy. URL: [Autopsy](https://www.sleuthkit.org/autopsy/) (дата звернення: 14.05.2025).
9. 1998. About Wireshark. URL: [Wireshark · About](https://www.wireshark.org/about.html) (дата звернення: 14.05.2025).
10. 2024. What is Suricata. URL: [What is Suricata - Suricata](https://suricata.io/2024/04/15/what-is-suricata/) (дата звернення: 14.05.2025).
11. 2015. Elastic Stack. URL: [Elastic Stack: (ELK) Elasticsearch, Kibana & Logstash | Elastic](https://www.elastic.co/elastic-stack/) (дата звернення: 14.05.2025).
12. 2024.Підручник із стеку ELK: що таке Kibana, Logstash & Elasticsearch.URL: [Підручник із стеку ELK: що таке Kibana, Logstash & Elasticsearch?](https://www.guru99.com/uk/elk-stack-tutorial.html) (дата звернення: 14.05.2025).
13. 2012. Що таке ELK Stack? URL: [Elk stack - для чого він використовується — Хостинг-компанія FREEhost.UA](https://freehost.com.ua/ukr/faq/wiki/chto-takoe-elk-stack/#:~:text=%D0%A1%D1%82%D0%B5%D0%BA%20ELK%20%28%D0%B0%D0%B1%D0%BE%20ELK%20stack%29%20%E2%80%94%20%D1%86%D0%B5%20%D0%BD%D0%B0%D0%B1%D1%96%D1%80,%D1%96%D0%BD%D1%88%D0%B8%D1%85%20%D0%B4%D0%B6%D0%B5%D1%80%D0%B5%D0%BB%20%D0%B2%D0%B5%D0%BB%D0%B8%D0%BA%D0%B8%D1%85%20%D0%BE%D0%B1%D1%81%D1%8F%D0%B3%D1%96%D0%B2%20%D0%B4%D0%B0%D0%BD%D0%B8%D1%85%20%D0%B2%20%D1%80%D0%B5%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D0%BC%D1%83%20%D1%87%D0%B0%D1%81%D1%96) (дата звернення: 14.05.2025).
14. 2019. Еластичний стек: аналіз журналів безпеки. Введення. URL: [1. Еластичний стек: аналіз журналів безпеки. Вступ / Хабр](https://habr.com/ru/companies/tssolution/articles/480570/) (дата звернення: 14.05.2025).
15. 2015. Filebeat: легкий аналіз журналів і еластичний пошук. URL: [Filebeat: легкий аналіз журналів і еластичний пошук | Пружні](https://www.elastic.co/beats/filebeat) (дата звернення: 14.05.2025).
16. 2015. Auditbeat: легкий вантажовідправник для аудиторських даних. URL: [Auditbeat: легкий вантажовідправник для аудиторських даних | Пружні](https://www.elastic.co/beats/auditbeat) (дата звернення: 14.05.2025).
17. 2015. Packetbeat: мережева аналітика за допомогою Elasticsearch. URL: [Packetbeat: мережева аналітика за допомогою Elasticsearch | Пружні](https://www.elastic.co/beats/packetbeat) (дата звернення: 14.05.2025).
18. 2015. Kibana: досліджуйте, візуалізуйте, знаходьте дані. URL: [Kibana: досліджуйте, візуалізуйте, знаходьте дані | Пружні](https://www.elastic.co/kibana#discover) (дата звернення: 14.05.2025).

**ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ**

**(Презентація)**