МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет

Факультет електроніки та інформаційних технологій

Кафедра кібербезпеки

«До захисту допущено»
Завідувач кафедри

_____ Володимир ЛЮБЧАК
(підпис)

«___»_____ 20___ р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня бакалавр

зі спеціальності 125 Кібербезпека, освітньо-професійної програми Кібербезпека на тему: Аналіз роботи системи ELK при розгляді кіберінцидентів

Здобувача групи КБ-01 Гришина Артема Олександровича
(шифр групи) (прізвище, ім'я, по батькові)

Кваліфікаційна робота містить результати власних досліджень.

Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Артем Гришин
(підпис) (прізвище, ім'я, по батькові)

Керівник зав.кафедри кібербезпеки, к.ф.-м.н., доцент _____
(посада, науковий ступінь, вчене звання, Ім'я та ПРІЗВИЩЕ) (підпис)

Суми — 2024

АНОТАЦІЯ

Кваліфікаційна робота виконана на 34 аркушах та містить 17 рисунки та 21 джерел.

Об’єкт дослідження: система операційного моніторингу і аналізу даних — ELK: Elasticsearch, Kibana & Logstash.

Мета роботи: дослідження методів системи ELK при розгляді кіберінцидентів з метою з'ясування їх ефективності та придатності для використання в реальних умовах. Розробка та впровадження алгоритму реагування та правила реагування на кіберінцидент.

Метод дослідження: оглядовий метод — для вивчення інформаційних джерел; порівняльно-аналітичний — для порівняння рішень та висновків; моделювання та алгоритмізації — для запровадження алгоритму реагування в різних модельних ситуаціях; випробування — для перевірки дієздатності.

Результати роботи: визначені переваги та недоліки системи ELK та її методів та підходів до розгляду інцидентів інформаційної безпеки, а також розроблено та впроваджено правило детектування інцидентів інформаційної безпеки підприємства, що дозволить знизити ризики втрати інформації та забезпечити її надійний захист.

Ключові слова: інформаційна безпека, система ELK, Elastic, кіберінцидент, правило детектування, алгоритм реагування, кіберзагроза, кібербезпека, SIEM.

Зміст

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

IC — Інформаційна система

ELK — Elasticsearch, Kibana, Logstash

IoT — Internet of things

MAC — Media Access Control

IPS — Image Packaging System

IOC — Indicator of compromise

VT — Virus total

SIEM — System Information and Event Management

ВСТУП

Кіберінцидент — подія або ряд несприятливих подій ненавмисного характеру та/або таких, що мають ознаки можливої кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем, ставлять під загрозу безпеку електронних інформаційних ресурсів [1].

За останні десятиліття інтенсивний розвиток технологій супроводжується зростанням кількості кіберінцидентів [2]. Ці події, які мають значний вплив на приватних осіб, організації та навіть цілі країни, підкреслюють важливість створення ефективних систем кібербезпеки.

Актуальність роботи полягає в необхідністю оперативного виявлення та реагування на кіберінциденти, що вимагає використання ефективних інструментів і технологій. Зростаюча кількість та складність кіберзагроз, які постійно еволюціонують, викликаючи серйозні ризики для безпеки інформаційних систем, вимагає від сучасних організацій новітніх методів боротьби з ними. Система ELK (Elasticsearch, Logstash, Kibana) є потужним інструментом для збору, аналізу та візуалізації даних, що робить її надзвичайно корисною для вирішення завдань кібербезпеки.

Завдання роботи включають:

1) інформаційний огляд аспектів захисту інформаційної системи;

2) формалізована постановка задачі й формування завдань дослідження;

3) огляд та опис основних функцій системи ELK;

4) дослідження при розгляді кіберінцидентів за допомогою системи ELK;

5) розробка алгоритму реагування на кіберінцидент;

6) розробка та впровадження нового правила реагування на кіберінцидент

5) аналіз отриманих результатів.

Новизна роботи полягає у використанні сучасних інструментів системи ELK для детального аналізу кіберзагроз та розробки ефективних методів реагування. Особливу увагу приділено створенню та впровадженню нових правил і алгоритмів для автоматизованого виявлення та реагування на кіберінциденти, що раніше не були достатньо висвітлені в літературі.

Практична потреба в даній роботі обумовлена необхідністю забезпечення високого рівня кібербезпеки у сучасних інформаційних системах, що є критично важливим для стабільного функціонування організацій та захисту конфіденційних даних. Впровадження розроблених методик і рекомендацій сприятиме підвищенню ефективності кіберзахисту та мінімізації ризиків, пов'язаних із кіберінцидентами.

Таким чином, дана робота є внеском у сферу кібербезпеки, пропонуючи нові підходи та рішення для моніторингу і реагування на кіберзагрози за допомогою системи ELK.

В даній роботі висвітлюються розділи що описують основні методи системи ELK, представляють аналіз алгоритмів реагування та надають висновки та рекомендації щодо їх використання, а також виконується детальний опис створення правила-реагування на кіберінцидент. Зроблені висновки слугуватимуть підґрунтям для подальших досліджень у сфері кібербезпеки та розробки відповідних стратегій та рішень для підвищення безпеки інформаційних систем.

1 ІНФОРМАЦІЙНИЙ ОГЛЯД ТА МЕТОДИ ДОСЛІДЖЕННЯ

Протягом останніх десятиліть стрімкий розвиток технологій супроводжується збільшенням кількості кіберінцидентів [2]. Ці інциденти, які суттєво впливають на окремих людей, організації та навіть цілі держави, акцентують необхідність створення дієвих систем кібербезпеки. Аналіз та відстеження цих загроз вимагають використання високоефективних інструментів. Вже використовуються доволі багато таких програмних застосунків, наприклад QRadar [3], Splunk [4], Alienvault [5].

QRadar від IBM забезпечує глибокий аналіз і кореляцію даних для виявлення та реагування на загрози в реальному часі. Переваги: висока точність виявлення загроз, інтеграція з багатьма іншими системами. Недоліки: висока вартість, складність налаштування.

Splunk пропонує платформу для моніторингу та аналізу машинних даних, що дозволяє швидко знаходити та усувати проблеми. Переваги: гнучкість, масштабованість, потужні аналітичні можливості. Недоліки: висока вартість ліцензій, вимоги до апаратних ресурсів.

Alienvault інтегрує кілька інструментів для виявлення загроз, керування вразливостями та реагування на інциденти в єдиній платформі. Переваги: універсальність, доступна ціна, простота використання. Недоліки: обмеженість у масштабуванні, менше функцій порівняно з конкурентами.

Одним з найбільш поширених та ефективних інструментів є система ELK, яка об'єднує Elasticsearch, Logstash і Kibana [6] .

ELK є комплексним рішенням, яке поєднує Elasticsearch для зберігання та індексації великих обсягів даних пов’язаних з кібербезпекою, Logstash для обробки та структуризації інформації з різних джерел, та Kibana для візуалізації, що дозволяє дослідникам кібербезпеки легко їх аналізувати. Ця інтеграція створює потужний інструментарій для обробки інформації щодо кібератак та допомагає налагодити аспекти захисту ІС.

Метою цієї роботи є дослідження методів системи ELK при розгляді кіберінцидентів з метою з'ясування їх ефективності та придатності для використання в реальних умовах. Основними завданнями були:

- Вивчення наявних методів системи ELK при розгляді кіберінцидентів та їхніх переваг та недоліків.
- Розгляд та порівняння різних алгоритмів реагування на кіберзагрози, що використовуються у системі ELK.
- Оцінка ефективності та придатності платформи ELK з урахуванням специфічних потреб організації.
- Розробка алгоритму реагування на кіберінцидент
- Розробка та впровадження нового правила реагування на кіберінцидент

Для досягнення мети дослідження методів використання системи ELK при розгляді кіберінцидентів було використано наступні підходи та методи:

Аналіз літературних джерел: Проведено систематичний огляд наукових статей, книг, настанов, журнальних публікацій та інших джерел, пов'язаних з кібербезпекою та системи ELK. Цей аналіз дозволив отримати фундаментальні знання про різні методи аналізу, їх переваги та недоліки.

Законодавчі акти України, такі як Закон "Про основні засади забезпечення кібербезпеки України" [1], визначають базові принципи та стратегії забезпечення кібербезпеки на національному рівні. Важливі деталі та поточний стан кібербезпеки в Україні відображені на ресурсах, таких як cert.gov.ua [2], який надає актуальну інформацію про кіберзагрози та заходи їх нейтралізації.

ENISA (The European Union Agency for Cybersecurity) та їх методологія OCTAVE [7] представляють комплексний підхід до управління ризиками, що є критично важливим для оцінки та зменшення кіберризиків у різних організаціях.

Книга "Windows Security Monitoring: Scenarios and Patterns" Мірошникова [8] детально описує сценарії та патерни моніторингу безпеки в середовищі Windows, що є корисним ресурсом для фахівців, які займаються захистом операційних систем.

Ряд джерел присвячений ELK Stack (Elasticsearch, Logstash, Kibana) як потужному інструменту для аналізу та візуалізації даних. Серед них документи Elasticsearch Guide [9] та навчальні матеріали, такі як "Introduction to logging with the ELK Stack" [10], що надають базову інформацію про встановлення та використання цієї платформи.

Практичні аспекти використання ELK Stack детально розглядаються в книзі Sachdeva G. S. "Practical ELK Stack" [12][13][14][15][16][17][18], що включає всі етапи від створення, індексування та видалення даних до їх аналізу і візуалізації в Kibana.

Наукові статті та конференційні матеріали, такі як робота Kumar H. S. про систему виявлення вторгнень за допомогою ELK Stack [19], дослідження Sankar P. та колег щодо моніторингу соціальних медіа з використанням ELK Stack [20], а також дослідження SHIBANI M. A. та E A. про автоматизоване полювання на загрози з використанням ELK Stack [21], доповнюють теоретичні знання практичними кейсами та прикладами використання.

Цей всебічний огляд літератури надає цілісне розуміння сучасних методів та інструментів забезпечення кібербезпеки, акцентуючи увагу на перевагах та недоліках різних підходів, а також їх практичному застосуванні.

Вивчення відкритої інформації про систему ELK: Проведено ретельний огляд різних функцій, що використовуються у секторі SOC аналітики. Досліджено їх функціональні можливості, архітектуру, властивості та інші характеристики. Використання відкритої інформації дало можливість зробити передбачення про ефективність та придатність платформи для різних сценаріїв використання.

Проведення тестувань та експериментів: Для отримання конкретних даних про роботу системи ELK, було проведено тестування та експерименти. Це включало встановлення та налаштування платформ, симуляцію різних кібератак та аналіз результатів. Тестування дозволило оцінити ефективність платформи, її здатність виявляти й реагувати на інциденти, а також їхню швидкодію та стабільність.

Ці методи дослідження забезпечили широкий обсяг інформації про різні методи аналізу кібербезпеки та системи ELK. Комбінація аналізу літературних джерел, вивчення відкритої інформації та проведення тестувань та експериментів дозволила отримати об'єктивні результати, які будуть використані для подальшого порівняння та висновків у звіті.

Отримані результати цього дослідження мають велике значення для власного розвитку. Вони надають змогу визначити найбільш підходящі способи та алгоритми реагування на кіберінциденти для власних потреб, забезпечуючи оптимальний захист інформації та ефективну реакцію на кібератаки.

Вже використовуються доволі багато подібних програмних застосунків, наприклад QRadar [3], Splunk [4], Alienvault [5]. Одним з найбільш поширених та ефективних інструментів є система ELK, яка об'єднує Elasticsearch, Logstash і Kibana [6] . Саме цей застосунок було впроваджено у роботу, та проведено дослідження працездатності при розгляді реальних кіберінцидентів, а також впроваджено нове правило реагування на підозрілу подію.

2 ОГЛЯД СИСТЕМИ ELK ЯК ІНСТРУМЕНТУ ДЛЯ РОЗГЛЯДУ КІБЕРІНЦИДЕНТІВ

Elastic - це платформа SOC аналітики, розроблена компанією Elastic, яка надає широкі можливості для збору, аналізу та використання данних для виявлення кіберзагроз та реагування на них, до інструментарія якого входить система ELK.

Система ELK (Elasticsearch, Logstash, Kibana) є відкритим та безкоштовним програмним забезпеченням, яке забезпечує потужну платформу для збору, обробки та аналізу великих обсягів даних, що надходять у вигляді логів. ELK широко використовується в області кібербезпеки, операційного моніторингу, аналізу даних і бізнес-аналітики завдяки своїм потужним можливостям та гнучкості.

ELK є комплексним рішенням, яке застосовує Elasticsearch для зберігання та індексації великих обсягів даних пов’язаних з кібербезпекою, Logstash для обробки та структуризації інформації з різних джерел, та Kibana для візуалізації, що дозволяє дослідникам кібербезпеки легко їх аналізувати.

Elasticsearch — це розподілена пошукова та аналітична система, яка базується на бібліотеці Lucene. Elasticsearch забезпечує високопродуктивний пошук та індексування даних у реальному часі. Завдяки своїй масштабованості та можливості обробки великих обсягів даних, Elasticsearch є ідеальним рішенням для задач, пов'язаних з аналізом логів та моніторингом.

Logstash — це інструмент для збору, обробки та передачі логів. Logstash може отримувати дані з різних джерел, таких як файли логів, бази даних, мережеві потоки, та перетворювати ці дані в уніфікований формат, що підходить для подальшого аналізу в Elasticsearch. Logstash підтримує різні фільтри та плагіни, які дозволяють очищати, збагачувати та нормалізувати дані перед їх відправкою.

Kibana — це платформа для візуалізації даних, що надає користувачам можливість створювати інтерактивні дашборди, графіки, діаграми та інші

візуальні представлення даних, що зберігаються в Elasticsearch. Kibana також дозволяє виконувати пошукові запити та аналізувати дані в реальному часі, що є надзвичайно корисним для виявлення та реагування на кіберінциденти.

Система ELK забезпечує повну інтеграцію між своїми компонентами, що дозволяє створити безперервний потік даних від їх збору до візуалізації. Ключові етапи інтеграції включають:

1. Збір даних. Logstash збирає дані з різних джерел, включаючи сервери, мережеві пристрої, бази даних, додатки та інші системи. Це може бути будь-яка інформація, яка генерує логи.
2. Обробка даних. Після збору дані проходять через низку фільтрів у Logstash, де вони можуть бути очищені, нормалізовані, збагачені додатковою інформацією та підготовлені для індексації. Фільтри Logstash дозволяють, наприклад, парсити лог-файли, додавати геолокаційні дані або перетворювати дані в потрібний формат.
3. Індексування та зберігання. Оброблені дані надсилаються до Elasticsearch, де вони індексуються і зберігаються для подальшого пошуку та аналізу. Elasticsearch забезпечує високу продуктивність і швидкий доступ до даних, незалежно від їх обсягу.
4. Візуалізація даних. Kibana підключається до Elasticsearch і дозволяє користувачам створювати інтерактивні дашборди та візуалізації, які допомагають аналізувати дані, виявляти аномалії та відстежувати ключові показники.

Ця інтеграція створює потужний інструментарій для обробки інформації щодо кібератак(Рисунок 2.1).

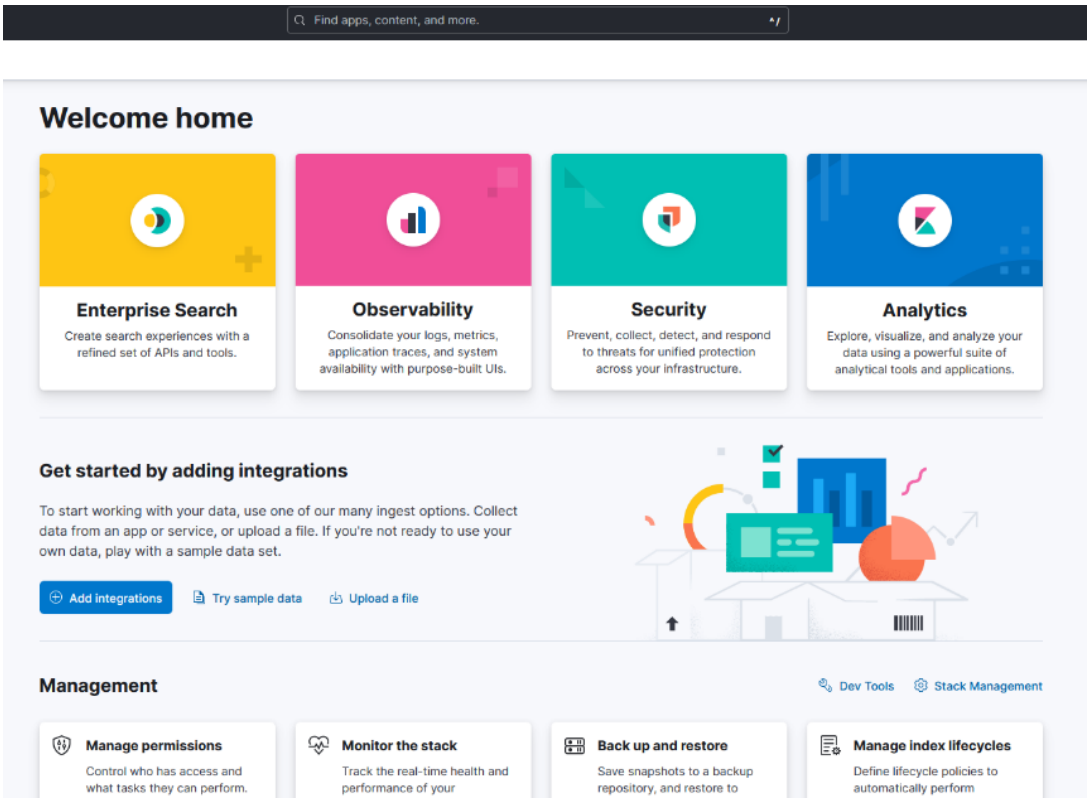

Рисунок 2.1 — Головна сторінка Elastic

Основні функціональні можливості та характеристики платформи Elastic включають:

- Збір та аналіз даних: Elastic забезпечує масштабовану інфраструктуру для збору, індексування та аналізу різноманітних даних, таких як логи, події, метадані тощо. Вона дозволяє виявляти зв'язки між різними джерелами даних та проводити розширений аналіз для виявлення загроз(Рисунок 2.2).

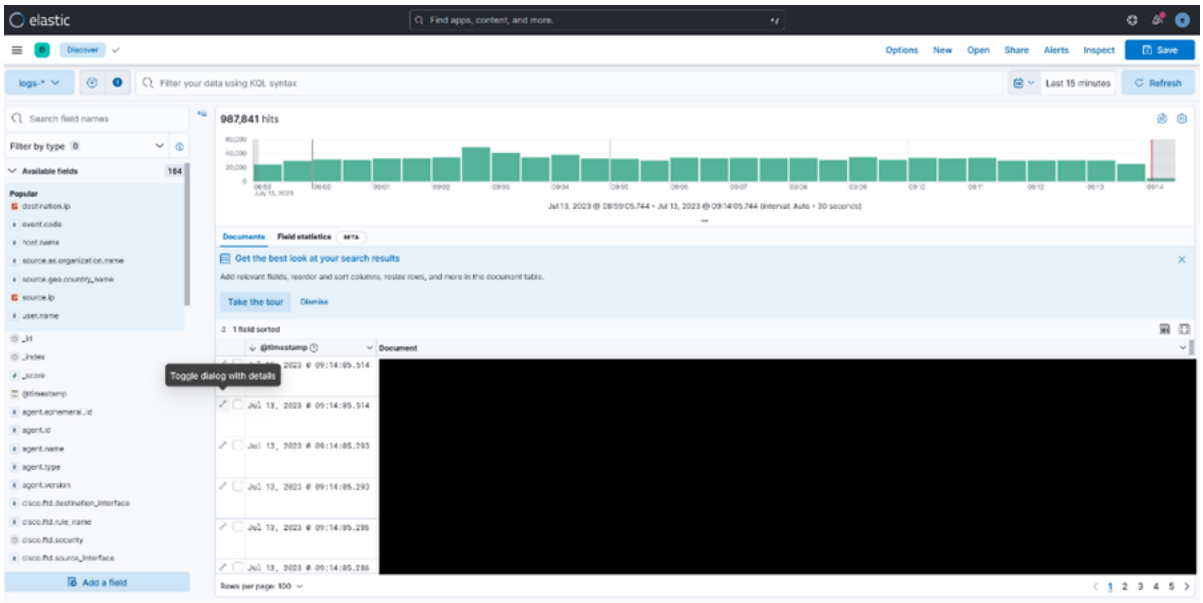

Рисунок 2.2 — Сторінка аналізу Elastic

- Виявлення загроз: Платформа використовує аналітичні алгоритми та машинне навчання для виявлення аномальної активності, підозрілих подій та потенційних загроз. Elastic дозволяє встановлювати правила та налаштування для виявлення конкретних типів загроз та здійснювати реал-тайм моніторинг(Рисунок 2.3).

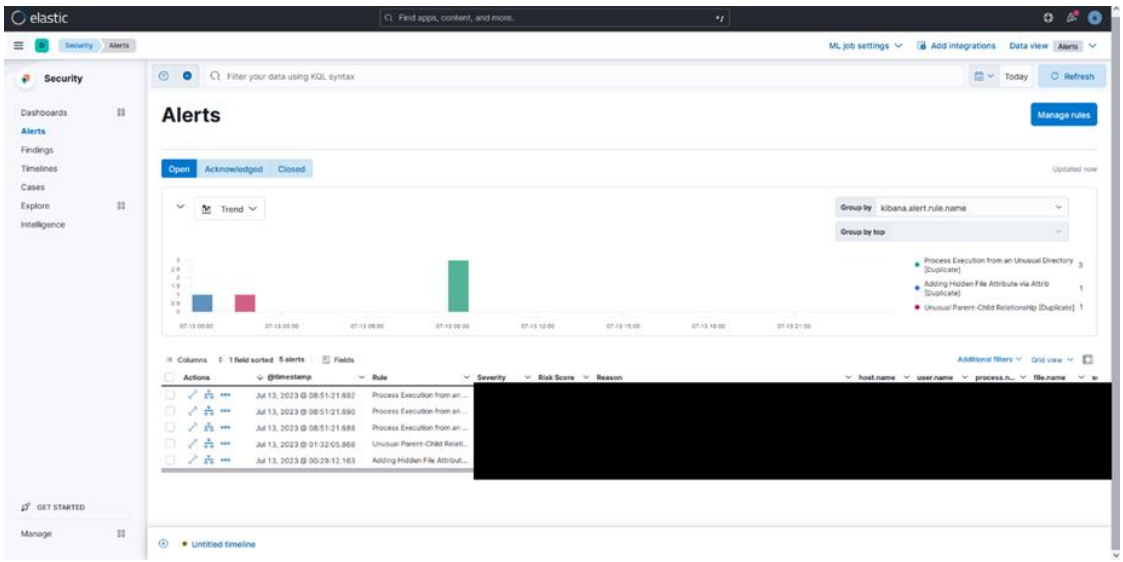

Рисунок 2.3 — Сторінка сповіщень Elastic

- Кореляція даних: Платформа Elastic дозволяє проводити кореляцію різних джерел даних та встановлювати зв'язки між ними. Це допомагає виявляти складні атаки, що можуть проявлятися в різних частинах системи(Рисунок 2.4).

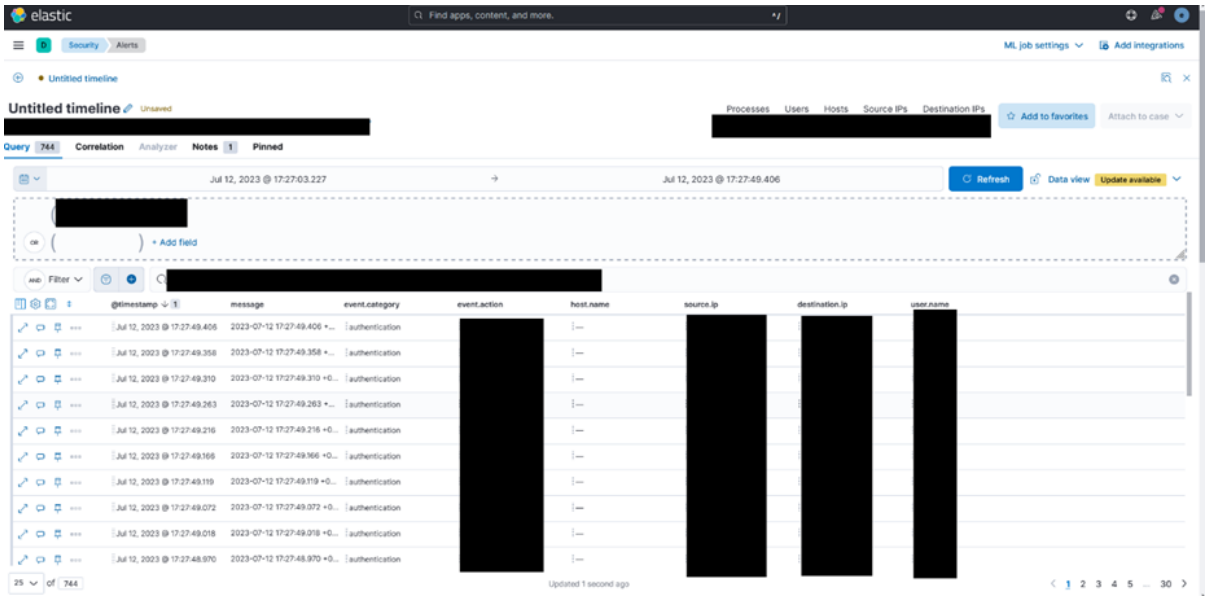

Рисунок 2.4 — Сторінка кореляції Elastic

- Візуалізація та звітність: Elastic надає інтуїтивний інтерфейс для візуалізації даних та створення звітів. Вона дозволяє створювати налаштовані та інтерактивні графіки, дашборди та звіти, що полегшує аналіз даних та прийняття рішень(Рисунок 2.5).

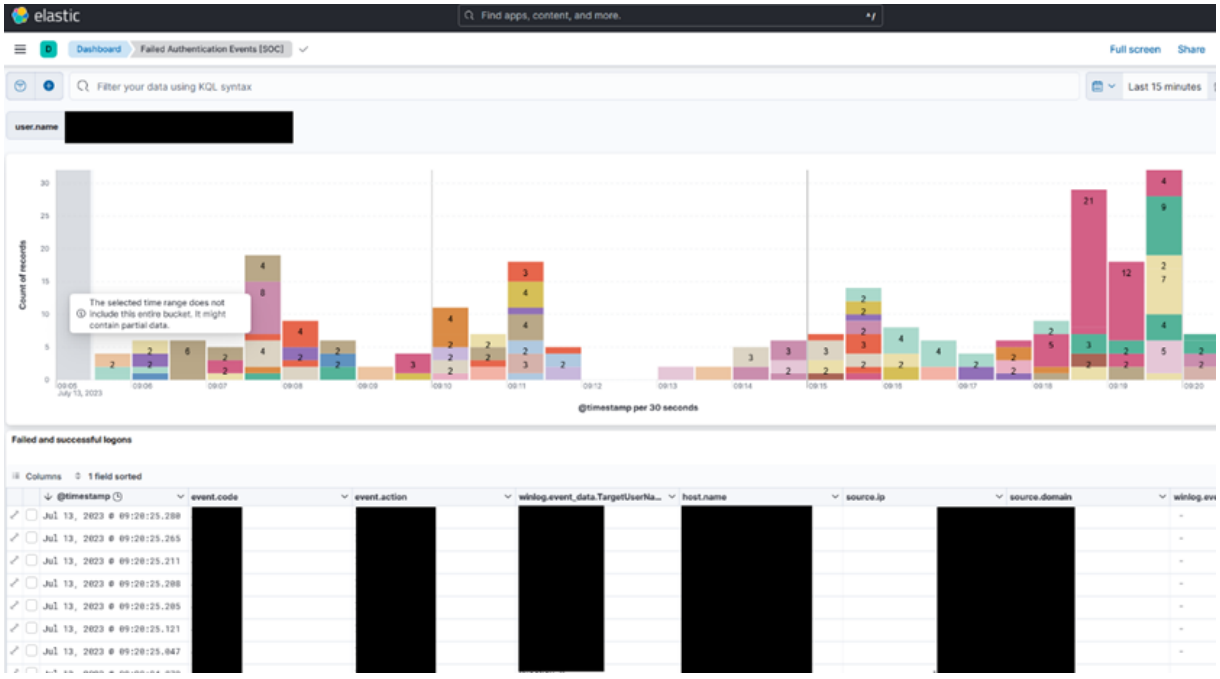

Рисунок 2.5 — Сторінка візуалізації Elastic

Система ELK виявляється ефективною в аналізі реальних випадків кіберінцидентів. Здатність зберігати та індексувати великі обсяги даних дозволяє ефективно виявляти шаблони атак та виявляти вразливості.

Приклади використання платформи Elastic в реальних сценаріях можуть включати виявлення та аналіз аномалій в мережі, розпізнавання зловмисного програмного забезпечення, виявлення атак на веб-додатки та інші види загроз. Elastic дозволяє реалізувати розширені функціональності SOC аналітики, що полегшує виявлення та реагування на кібератаки.

Система ELK є потужним та гнучким інструментом для розгляду кіберінцидентів. Її можливості швидкого збору, обробки та аналізу великих обсягів даних, а також інтерактивна візуалізація даних роблять її незамінною для організацій, що прагнуть підвищити свою кібербезпеку. Використання ELK дозволяє ефективно відстежувати та реагувати на загрози, забезпечуючи надійний захист інформаційних систем.

3 АЛГОРИТМИ РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ

3.1 Розробка алгоритму реагування на кіберінцидент

Використання ELK вимагає чіткої методології аналізу та реагування на кіберінциденти. Ця методологія повинна включати:

- Процес збору та обробки даних
- Методи аналізу даних для виявлення кібератак
- План реагування на виявлені кіберзагрози

ELK відіграє важливу роль у розгляді кіберінцидентів завдяки здатності збирати, зберігати, аналізувати та візуалізувати дані з різноманітних джерел. ELK може збирати дані з журналів серверів, мережевих пакетів, веб-сайтів та IoT-пристроїв, забезпечуючи всебічний погляд на кібербезпеку організації. Ці дані потім можна зберігати протягом тривалого часу, що дає можливість проводити ретроспективний аналіз та виявляти потенційні загрози, які могли бути пропущені раніше. ELK також може використовуватися для створення сигнатур кіберінцидентів, що дає можливість автоматично їх виявляти. Це значно економить час і ресурси, дозволяючи кіберфахівцям зосередитися на більш складних завданнях(Рисунок 3.1.1).

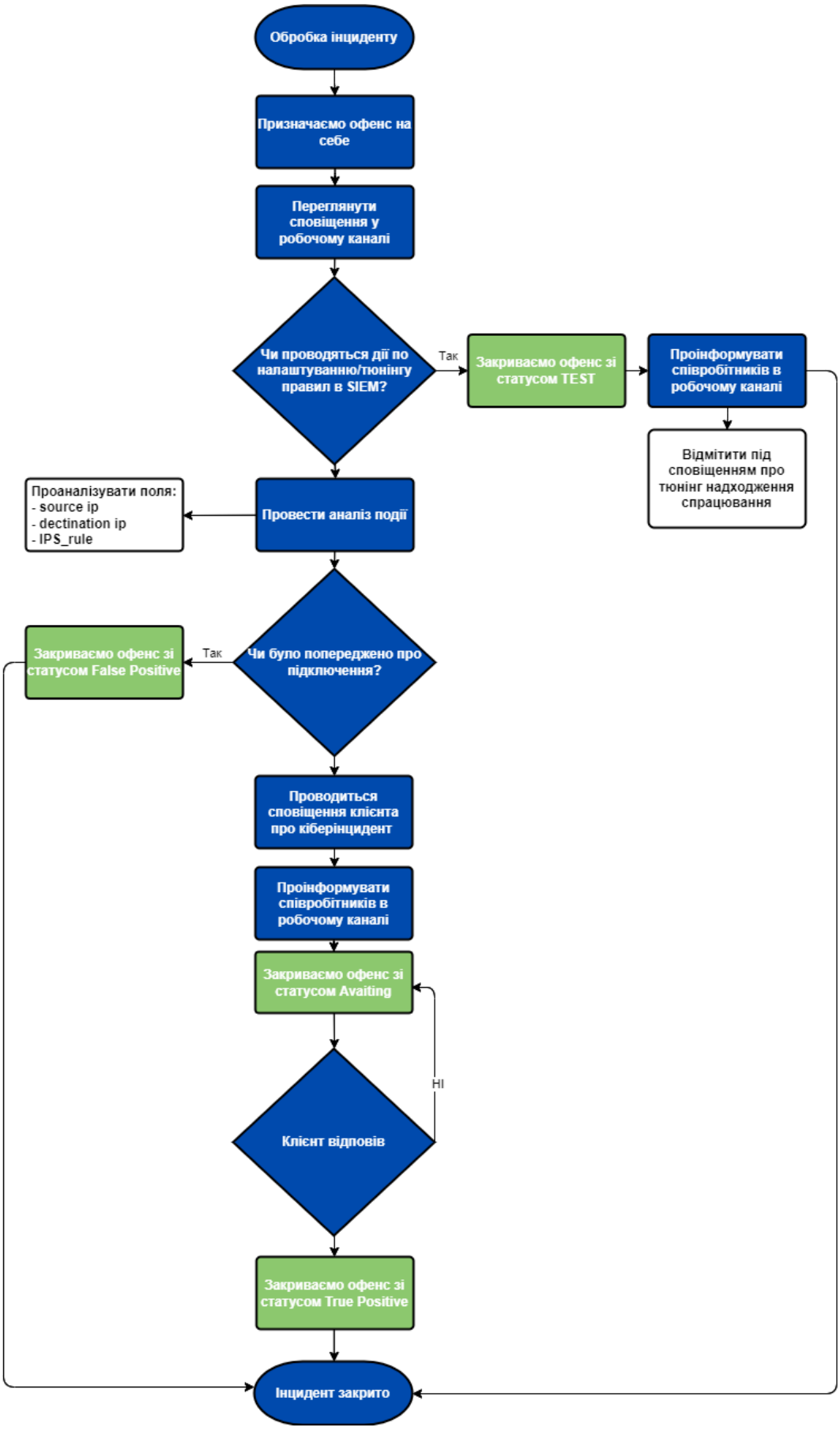

Рисунок 3.1.1 — Алгоритм

У випадку кіберінциденту ELK може використовуватися для швидкого реагування, щоб мінімізувати збитки та відновити нормальну роботу організації. Система також може допомогти у розслідуванні інцидентів, щоб знайти причину та наслідки, а також запобігти подібним інцидентам у майбутньому. ELK також може використовуватися для підвищення обізнаності про кіберінциденти серед персоналу організації, для дотримання нормативних вимог щодо кібербезпеки.

Алгоритм реагування на кіберінцидент представлений на рисунку(Рисунок 3.1) та детально розглянутий нижче, дозволяє ефективно виявляти, аналізувати та реагувати на кіберзагрози. Кожен етап цього процесу виконується з метою мінімізації шкоди та забезпечення безпеки інформаційних систем.

1. Обробка інциденту:

Цей етап включає початкову реєстрацію та фіксацію інциденту, який був виявлений у системі моніторингу або отриманий від користувачів. Важливо задокументувати всі деталі інциденту для подальшого аналізу.

2. Призначаємо офенс на себе:

Відповідальна особа або команда бере на себе інцидент для розслідування. Це включає визначення ролей і відповідальностей, щоб уникнути дублювання зусиль та забезпечити координацію.

3. Переправити сповіщення у робочому каналі:

Сповіщення про інцидент направляється у внутрішній робочий канал, такий як Slack або Microsoft Teams. Це дозволяє всім членам команди залишатися в курсі подій і забезпечує зручний спосіб координації дій.

4. Чи проводяться дії по налаштуванню/тюнингу правила в SIEM?:

Перевірка, чи вже існує заявка по налаштуванню/тюнингу правила в SIEM (System Information and Event Management), яке автоматично реагує на цей тип інциденту.

5. Так: Закриваємо офенс зі статусом TEST:

Якщо інцидент відповідає вже існуючим заявкам, його можна закрити зі статусом "TEST". Це означає, що дії по інциденту вже легітимні.

6. Проінформувати співробітників в робочому каналі:

Оповіщення команди про те, що інцидент обробляється відповідно до встановлених правил.

7. Відмітити під сповіщенням про точний час надходження спрацювання:

Додання точних деталей про час та обставини спрацювання правила в SIEM для подальшого аналізу.

8. Ні: Провести аналіз події:

Ручний аналіз події включає детальне вивчення логів, даних і контексту, щоб зрозуміти природу інциденту та його потенційні наслідки.

9. Проаналізувати поля: source ip, destination ip, IPS_rule:

Аналіз ключових полів, таких як IP-адреси джерела та призначення, а також відповідних правил IPS (Intrusion Prevention System), щоб визначити походження та масштаб загрози.

10. Чи було попереджено про підключення?:

Перевірка, чи був інцидент попереджений і чи є в системі запис про дозвіл на відповідне підключення.

11. Так: Закриваємо офенс зі статусом False Positive:

Якщо інцидент виявляється помилковим спрацюванням (False Positive), він закривається зі статусом "False Positive".

12. Ні: Проводиться сповіщення клієнта про кіберінцидент:

Клієнт або відповідальна особа інформується про інцидент, надаються всі необхідні деталі та рекомендації щодо подальших дій.

13. Проінформувати співробітників в робочому каналі:

Оповіщення команди про новий кіберінцидент для координації спільних дій.

14. Закриваємо офенс зі статусом Awaiting:

Інцидент отримує статус "Awaiting", що означає очікування додаткової інформації або підтвердження від клієнта.

15. Клієнт відповів:

Перевірка наявності відповіді від клієнта або відповідальної особи, яка підтверджує або спростовує інцидент.

16.Так: Закриваємо офенс зі статусом True Positive:

Інцидент закривається зі статусом "True Positive", підтверджуючи, що загроза була реальною і були вжиті відповідні заходи.

17.Інцидент закрито:

Процес реагування на інцидент завершено, і інцидент офіційно закрито в системі. Це включає підготовку звіту про інцидент, документування всіх дій і висновків, а також проведення післяінцидентного аналізу для поліпшення майбутніх реакцій.

Цей детальний опис алгоритму допомагає забезпечити систематичну і ефективну обробку кіберінцидентів, зменшуючи ризики та покращуючи загальну безпеку інформаційних систем.

3.2 Приклад реагування на кіберінцидент за алгоритмом

Наглядно розберемо один з інцидентів (всі данні замінені та не мають нічого спільного з реальними даними клієнтів)

Розглянемо як приклад такий алгоритм розслідування інцидента :

1. Надходження алерта
2. Агрегування всіх алертів за одним патерном
3. Створення інцидента
4. Пошук відповідного алерта в Elastic
5. Розслідування на основі аналітики
6. Написання листа на клієнта/ переведення в статус хибно позитивний
7. Закриття інциденту

Перші три пункти система ELK виконує автоматично без втручання оператора, томі їх ми можемо пропустити, та перейти до розгляду наступних

Пошук відповідного алерта в Elastic(Рисунок 3.2.1).

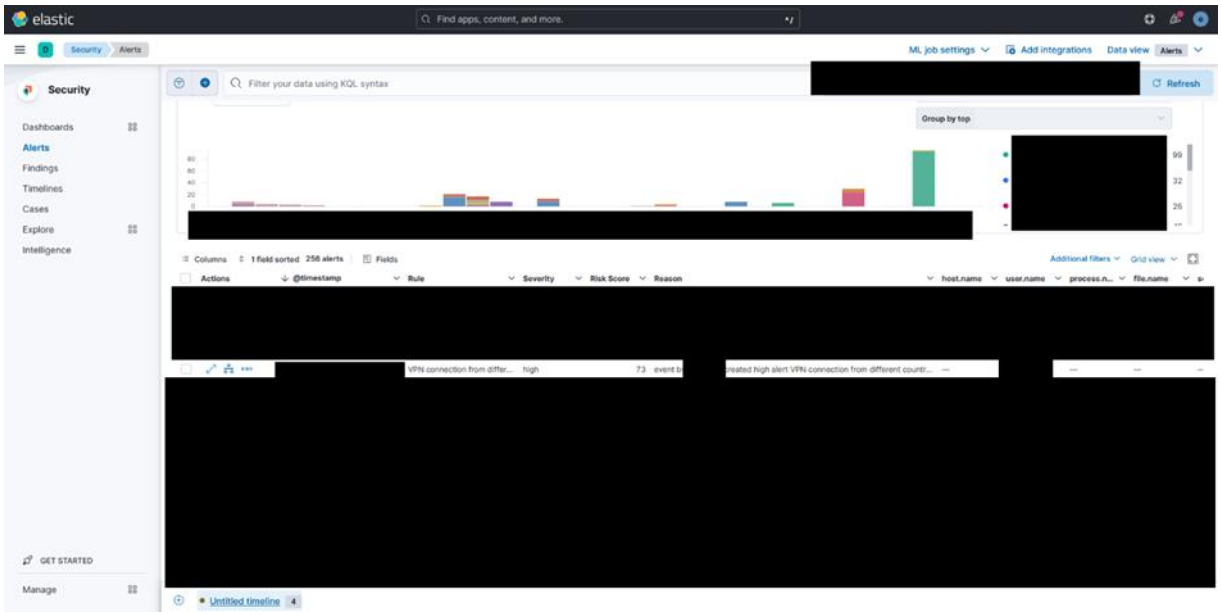

Рисунок 3.2.1 — Пошук відповідного алерта в Elastic

Розслідування на основі аналітики

Для розслідування потрібно дослідити логи, там ми побачимо, що дійсно використовувалися різні адреси для автентифікації(Рисунок 3.2.2).

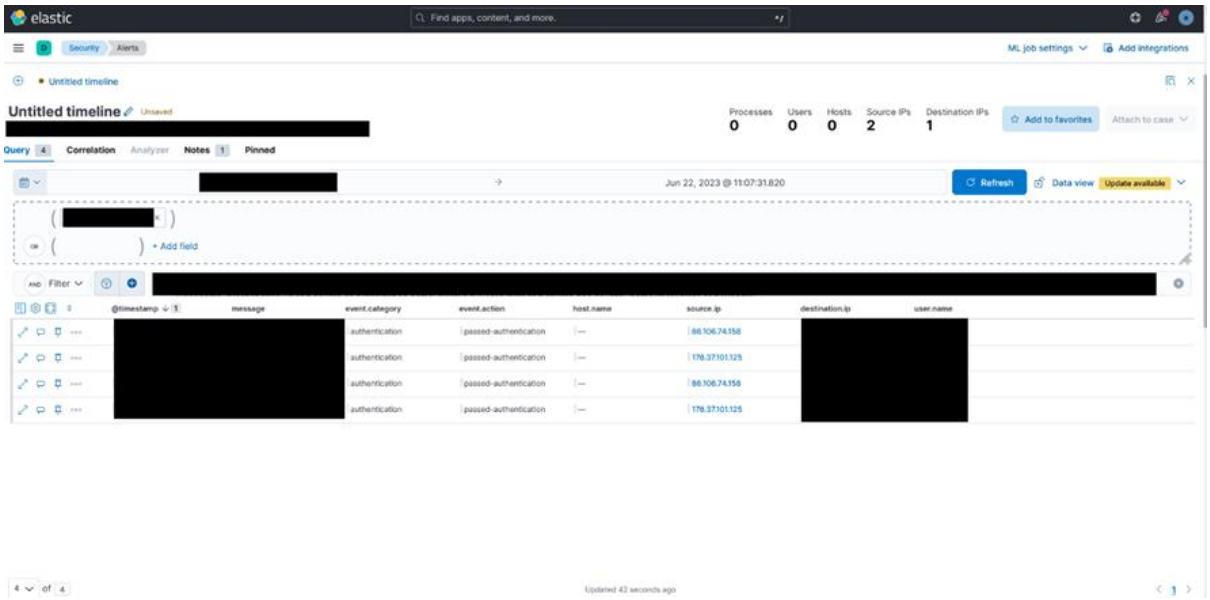

Рисунок 3.2.2 — Розслідування на основі аналітики

Далі, нам слід впевнитися, що девайси, з яких була здійснено автентифікацію мають різні MAC адреси, якщо мають однаковий, то дії легітимні за домовленістю з клієнтом. Для цього передивимося історію логів цього користувача(Рисунок 3.2.3).

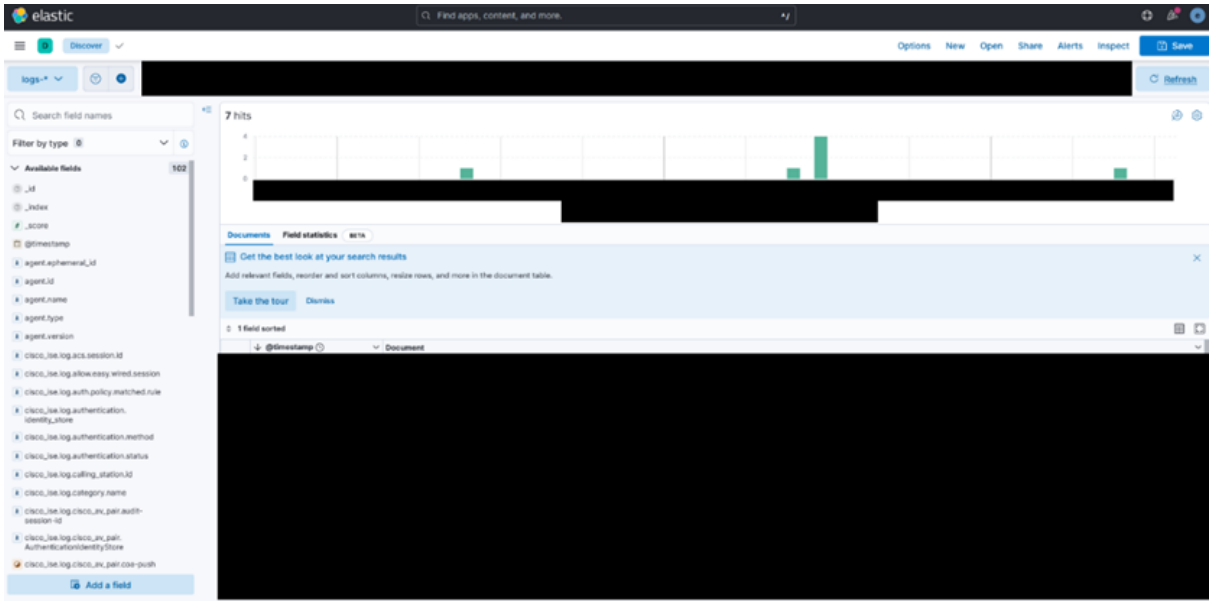

Рисунок 3.2.3 — Розслідування на основі аналітики

Так ми можемо побачити, що адреси дійсно різні, що свідчить про те, що нам слід сповістити замовника про можливий не легітимний інцидент.

Спроможність ELK забезпечувати велику швидкість опрацювання та візуалізації даних є важливою перевагою. Однак слабкі сторони, такі як

складність конфігурації та обмеження при обробці деяких типів даних, потребують великого досвіду у роботі з системою та розуміння стратегій захисту.

Для максимізації потенціалу ELK у виявленні та аналізі кіберінцидентів, важливо розглядати можливості оптимізації архітектури системи та вдосконалення інтеграції з іншими інструментами кібербезпеки.

Потенціал ELK можна максимізувати, оптимізувавши архітектуру системи та вдосконаливши інтеграцію з іншими інструментами кібербезпеки. Це може включати:

- Використання хмарних технологій;
- Автоматизація процесів;
- Розробка нових методів аналізу даних;

4 РОЗРОБКА ТА ПРАКТИЧНЕ ВПРОВАДЖЕННЯ ПРАВИЛА РЕАГУВАННЯ

4.1 Розробка та впровадження правила реагування

Розділ присвячений детальному опису процесу створення та інтеграції специфічного правила реагування на кіберінциденти в систему управління інформаційною безпекою (SIEM).

У цьому розділі буде розглянуто основні етапи розробки правила реагування, починаючи від аналізу типових загроз і визначення відповідних сценаріїв, до практичного впровадження цього правила у SIEM.

Аналіз типових загроз :

Подія "Watch Guard IPS External" являє собою спроби зовнішніх атак через систему запобігання вторгненням (IPS) Watch Guard. Це подія є важливим елементом у комплексній системі кіберзахисту організації, оскільки вона дозволяє фіксувати та обробляти підозрілу активність, яка може свідчити про потенційні загрози ззовні. Тому з’явилася потреба у автоматичному фіксуванні таких подій за допомогою правила реагування на кіберінцидент.

Для фіксування таких подій, потрібно визначити, які саме поля відповідають за головні складові кореляції. Оскільки подія називається "Watch Guard IPS External", цілком правильно буде визначити, що до головних полів входять :

- wg-msg-type (поле відповідає за походження)
- msg (поле відповідає за повідомлення)
- source.ip (поле відповідає за адресу джерела)

Виходячи з відомої логіки правила та відомих полів, можна скласти кореляцію, на основі якої SIEM буде автоматично виділяти події такого типу в інциденти(Рисунок 4.1.1).

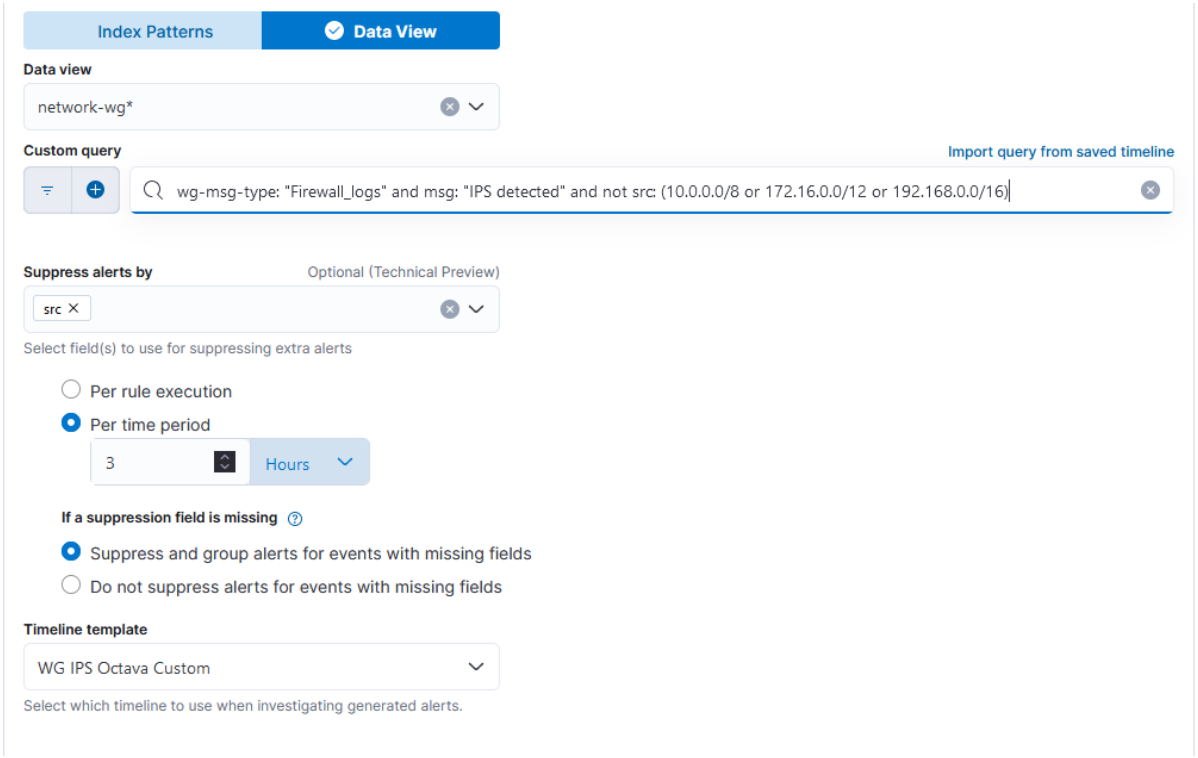

Рисунок 4.1.1 — Створення кореляції

Правило фокусується на моніторингу трафіку, що надходить ззовні мережі, зокрема з інтернету, що дозволяє виключити з пошуку приватні адреси.

Далі слід налаштувати часові проміжки, коли буде спрацьовувати правило(Рисунок 4.1.2).

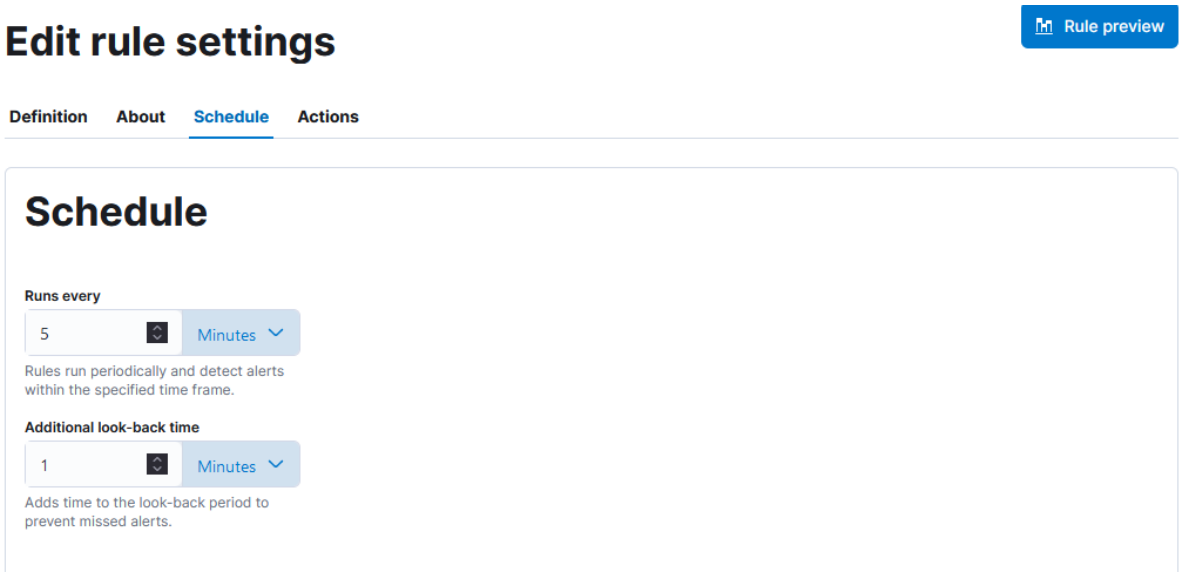

Рисунок 4.1.2 — Налаштування часових рамок

А також визначити потенційні ризики від спрацювання та налаштувати Risk score(Рисунок 4.1.3).

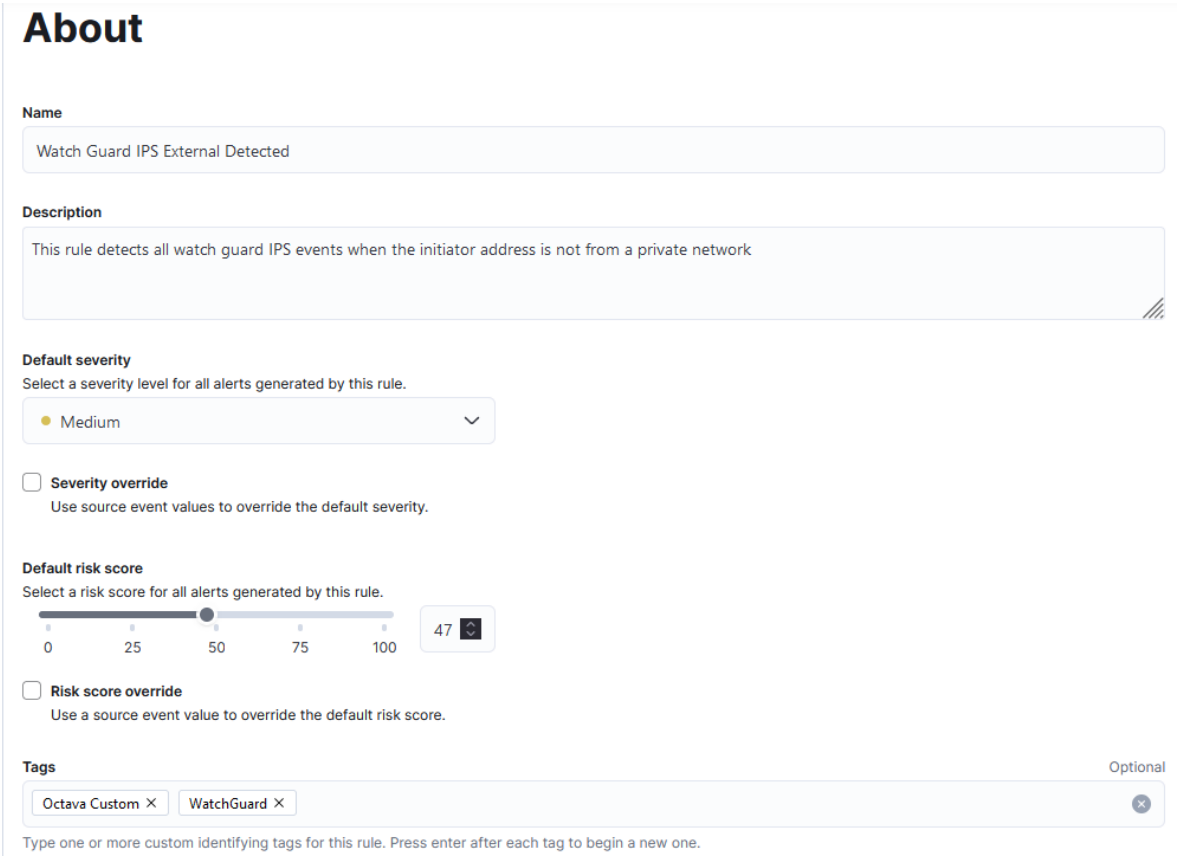

Рисунок 4.1.3 — Risk score

Впровадження ефективних правил реагування не лише підвищує рівень безпеки організації, але й дозволяє зменшити навантаження на аналітиків з кібербезпеки, автоматизуючи рутинні завдання та зосереджуючи їхню увагу на більш складних і нетипових інцидентах. Таким чином, це правило, яке було створено та впроваджено, неодноразово використовувалось аналітиками ТОВ «ОКТАВА ДЕФЕНС» для прискорення роботи без втрати якості.

4.2 Практичне впровадження процедури реагування на інцидент

Переходячи до виконання одного з завдань дослідження, розглянемо повний процес реагування на інцидент кібербезпеки, з подальшим звітом та розв’язанням проблеми. Важливо відмітити, що спрацювання стосується раніше створеного нами правила.

Під час моніторингу консолі ELK ми помічаємо нове спрацювання(Рисунок 4.2.1)

Рисунок 4.2.1 — Консоль ELK

Спрацювання викликало робота правила «Watch Guard IPS External Detected».

Слід перейти на сторінку правила та зрозуміти логіку і суть спрацювання.(Рисунок 4.2.2)

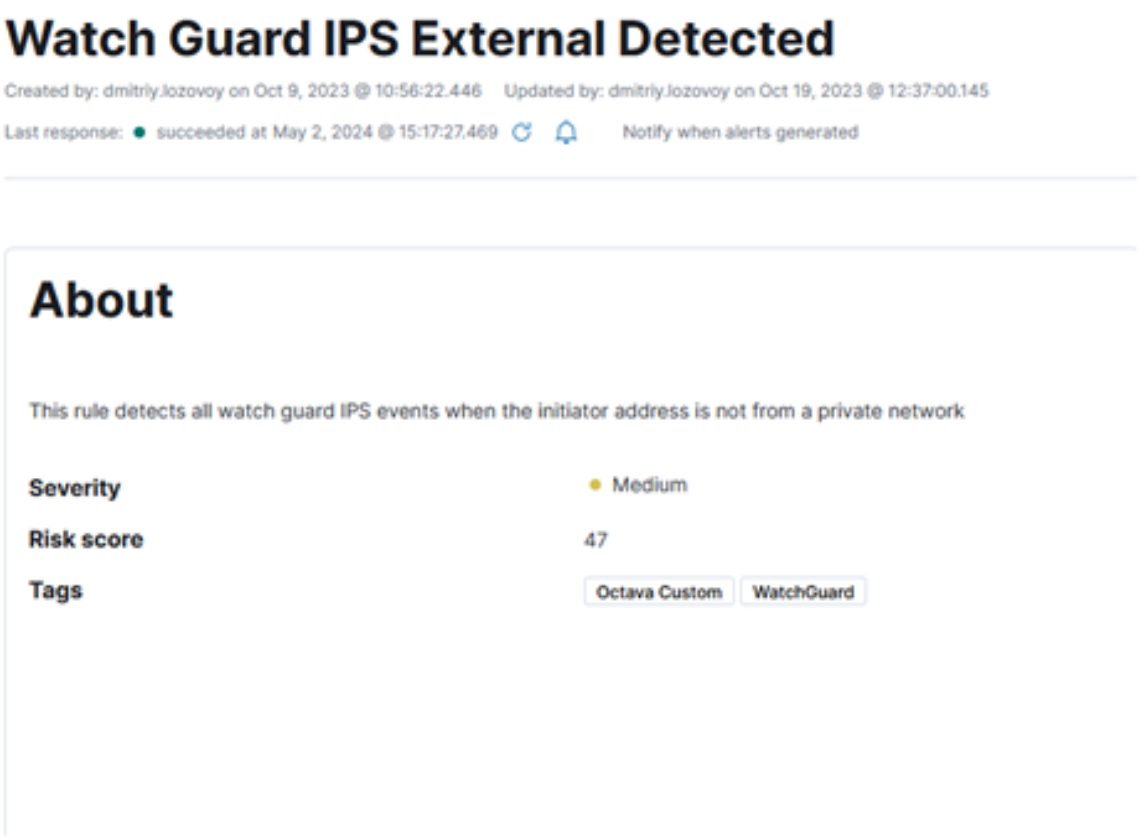

Рисунок 4.2.2 — Сторінка правила

Як бачимо, правило спрацьовує, коли системою IPS зафіксована підозріла активність пов’язана з ip-адресою, яка знаходиться у ioc-list.

Далі слід передивитися логіку правила, щоб дізнатися поля з лог-записів, на які правило реагує, щоб сповістити клієнта, надавши коректні дані.(Рисунок 4.2.3)

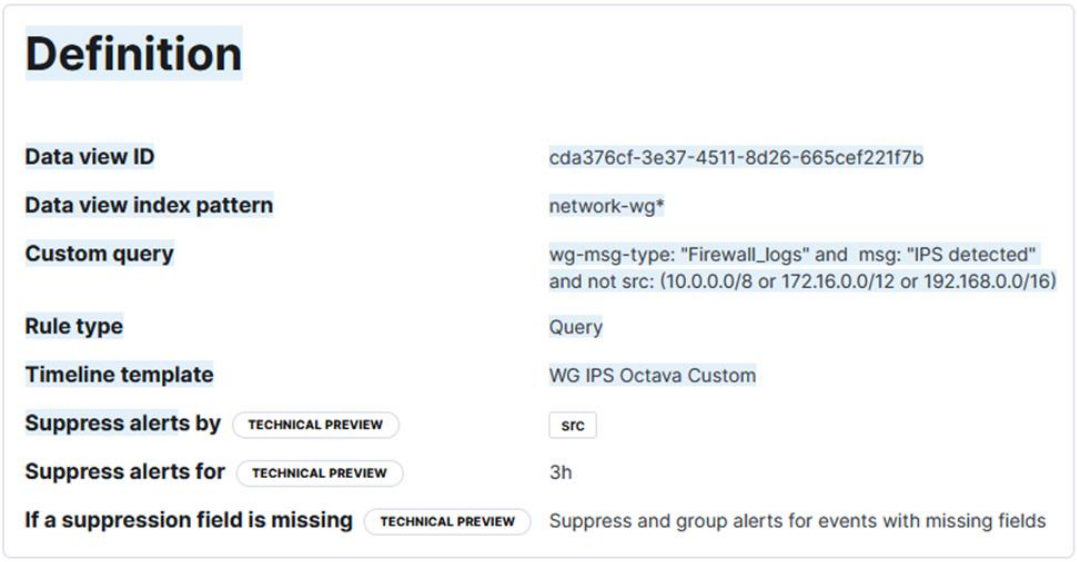

Рисунок 4.2.3 — Логіка правила

Як можемо впевнитися, правило повністю базується на сповіщенні з IPS, окрім тих випадків коли виклик йде з внутрішніх адрес.

На наступному етапі слід створити вибірку з подій та передивитися, що саме сталося.(Рисуонк 4.2.4)

@timestamp	host.name	IPS_cat	IPS_rule	src	dst	disp	dstPort
May 2, 2024 @ 14:48:16.806	CZ-PR-NGFW2	Exploits	WEB Remote Command E...	84.54.51.41	194.213.192.30	Deny	80
May 2, 2024 @ 13:51:27.006	CZ-PR-NGFW2	Exploits	WEB Remote Command E...	84.54.51.41	194.213.192.12	Deny	80

Рисунок 4.2.4 — Вибірка подій

Можемо побачити, що правило спрацювало за сигнатурою IPS_rule: "WEB Remote Command Execution via Shell Script -1.h". Відбувався мережевий конект з src: "84.54.51.41"(невідома зовнішня адреса) до dst: "194.213.192.12"(відома адреса сервера клієнта). Можемо впевнитися в тому, що IPS працює коректно, оскільки програмне забезпечення саме заблокувало конект - disp: "Deny".

Далі слід упевнитися, що src: "84.54.51.41"(невідома зовнішня адреса) дійсно є підозрілою.(Рисунок 4.2.5)

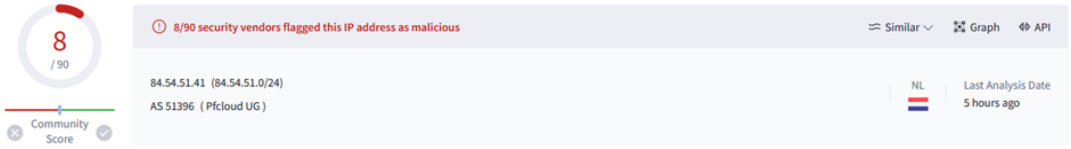

Рисунок 4.2.5 — Перевірка адреси

Упевнившись, що правило спрацювало вірно, можемо надсилати листа на замовника послуг з таким текстом:

«An IPS attack on WatchGuard using the signature "WEB Remote Command Execution via Shell Script -1.h". The initiator of the connections is the host with the IP address src: "84.54.51.41" (Korea Telecom , status on vt - 8 security vendor flagged this IP address as malicious, Korea). Connections were made to resources "194.213.192.30" on port 443. Please identify the source of the connections and block the address on the cross-network devices.

Зафіксовано IPS-спрацювання на WatchGuard по сигнатурі "WEB Remote Command Execution via Shell Script -1.h". Ініціатором підключень виступає хост з ip-адресою src: "84.54.51.41" (Korea Telecom , status on vt - 8 security vendor

flagged this IP address as malicious, Korea). Підключеня відбувались до ресурсів "194.213.192.30"" по 443 порту. Прохання визначити джерело з’єднань та заблокувати адресу на мережевих пристроях.»

ВИСНОВКИ

У результаті дослідження методів використання системи ELK при розгляді кіберінцидентів, було отримано наступні висновки:

- Сучасні методи аналізу кібербезпеки мають великий потенціал для ефективного виявлення, аналізу та відповіді на кібератаки. Ці методи включають автоматизовану обробку даних, машинне навчання, аналіз поведінки загроз та кореляцію даних.
- Система ELK має різні функціональні можливості та характеристики. Платформа має свої переваги та недоліки, які потрібно враховувати при виборі.
- Elastic - гнучка платформа, що ґрунтується на відкритих стандартах, яка надає можливості для збору, аналізу та використання даних для виявлення загроз та відповіді на них. Elastic забезпечує масштабовану інфраструктуру та засоби візуалізації даних для ефективного аналізу.
- Вибір Elastic повинен залежати від конкретних потреб організації, її розміру, бюджету та іншого контексту. Важливо ретельно вивчити характеристики та можливості кожної платформи, порівняти їх з вимогами організації та здійснити обґрунтований вибір.

Написано нове правило реагування на кіберінцидент та впроваджено у роботу на підприємстві ТОВ «ОКТАВА ДЕФЕНС». Проводено аналіз спрацювання з поданням висновку, що до працездатності правила.

Також було виконано розгляд реального кіберінциденту.

У подальшому, рекомендації, отримані з дослідження, можуть бути використані для впровадження та підвищення ефективності платформ SOC аналітики, а також для подальших досліджень у сфері кібербезпеки та розробки стратегій захисту інформаційних систем.

СПИСОК ЛІТЕРАТУРИ

1. Про основні засади забезпечення кібербезпеки України. Законодавство України. URL: https://web.archive.org/web/20190209132913/https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 09.03.2024).

2. Cert-ua. cert.gov.ua. URL: https://cert.gov.ua/article/5436463 (дата звернення: 09.03.2024).

3. IBM documentation. IBM in Deutschland, Österreich und der Schweiz. URL: https://www.ibm.com/docs/ru/qsip/7.5?topic=started-qradar-overview (дата звернення: 09.03.2024).

4. Splunk | the key to enterprise resilience. Splunk. URL: https://www.splunk.com/ (дата звернення: 09.03.2024).

5. AlienVault - open threat exchange. AlienVault Open Threat Exchange. URL: https://otx.alienvault.com/ (дата звернення: 09.03.2024).

6. Elasticsearch Platform – Find real-time answers at scale. Elastic. URL: https://www.elastic.co/ (дата звернення: 09.03.2024).

7. The European Union Agency for Cybersecurity (ENISA) – Octave [Електронний ресурс] – Режим доступу: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html – Дата звернення: 18.03.2024.

8. Miroshnikov A. Windows Security Monitoring: Scenarios and Patterns. Wiley & Sons, Incorporated, John, 2018. 648 с.

9. Elasticsearch Guide [8.13] | Elastic. Elasticsearch Platform – Find real-time answers at scale | Elastic. URL: https://www.elastic.co/guide/en/elasticsearch/reference/current/index.html (дата звернення: 03.05.2024).

10. Introduction to logging with the ELK Stack: A primer for beginners. Elastic. URL: https://www.elastic.co/webinars/introduction-elk-stack?page=docs&placement=top-video (дата звернення: 03.05.2024).

11. Windows Security Logging and Monitoring Policy. Windows® Security Monitoring: Scenarios and Patterns. Indianapolis, Indiana, 2018. С. 1–9. URL: https://doi.org/10.1002/9781119390909.ch1 (дата звернення: 03.05.2024).

12. Sachdeva G. S. Introduction to the ELK Stack. Practical ELK Stack. Berkeley, CA, 2017. С. 1–17. URL: https://doi.org/10.1007/978-1-4842-2626-1_1 (дата звернення: 03.05.2024).

13. Sachdeva G. S. The Kibana Dashboard. Practical ELK Stack. Berkeley, CA, 2017. С. 201–214. URL: https://doi.org/10.1007/978-1-4842-2626-1_10 (дата звернення: 03.05.2024).

14. Sachdeva G. S. The ELK Stack in Production. Practical ELK Stack. Berkeley, CA, 2017. С. 245–285. URL: https://doi.org/10.1007/978-1-4842-2626-1_12 (дата звернення: 03.05.2024).

15. Sachdeva G. S. Creating, Indexing, and Deleting Data. Practical ELK Stack. Berkeley, CA, 2017. С. 57–80. URL: https://doi.org/10.1007/978-1-4842-2626-1_4 (дата звернення: 03.05.2024).

16. Sachdeva G. S. Mapping and Analysis. Practical ELK Stack. Berkeley, CA, 2017. С. 101–116. URL: https://doi.org/10.1007/978-1-4842-2626-1_6 (дата звернення: 03.05.2024).

17. Sachdeva G. S. Exploring Kibana. Practical ELK Stack. Berkeley, CA, 2017. С. 151–158. URL: https://doi.org/10.1007/978-1-4842-2626-1_8 (дата звернення: 03.05.2024).

18. Sachdeva G. S. Practical ELK Stack. Berkeley, CA : Apress, 2017. URL: https://doi.org/10.1007/978-1-4842-2626-1 (дата звернення: 03.05.2024).

19. Kumar H. S. Intrusion Detection System using ELK Stack. International Journal for Research in Applied Science and Engineering Technology. 2019. Т. 7, №

6. С. 667–670. URL: https://doi.org/10.22214/ijraset.2019.6115 (дата звернення: 03.05.2024).

20. Sankar P., George D. E., S A. S. N. Social media monitoring using ELK Stack. 2022 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), м. THIRUVANANTHAPURAM, India, 10–12 берез. 2022 р. 2022. URL: https://doi.org/10.1109/spices52834.2022.9774273 (дата звернення: 03.05.2024).

21. SHIBANI M. A., E A. Automated Threat Hunting Using ELK Stack - A Case Study. Indian Journal of Computer Science and Engineering. 2019. Т. 10, № 5. С. 118–127. URL: https://doi.org/10.21817/indjcse/2019/v10i5/191005008 (дата звернення: 03.05.2024).

22. Гришин А.О. Використання системи ELK при розгляді кіберінцидентів. 2024. URL: https://drive.google.com/file/d/1odMNmTuXPjFJAMe194n6WEDiMpf2qDgz/view (дата звернення: 22.05.2024).