МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МОДЕЛЬ УПРАВЛІННЯ ІНЦИДЕНТАМИ БЕЗПЕКИ З ВИКОРИСТАННЯМ SIEM-СИСТЕМ”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Єлизавета НИКИТЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконала: здобувачка вищої освіти гр. УБД-42

Єлизавета НИКИТЕНКО

Керівник: Тетяна КАПЕЛЮШНА
Д.е.н., доцент

Рецензент:
Д.т.н., професор Галина ГАЙДУР

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
“____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Никитенко Єлизаветі Ярославівні
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Модель управління інцидентами безпеки з використанням SIEM-систем”,
керівник кваліфікаційної роботи КАПЕЛЮШНА Тетяна, д.е.н., доцент
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологійвід “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: інформаційна безпека підприємства, технології та інструменти виявлення і реагування на інциденти, системи управління подіями безпеки (SIEM), сучасні методи моніторингу та візуалізації, наукова та технічна література.
4. Перелік питань, які мають бути розроблені:
   4.1. Проаналізувати особливості управління інформаційною безпекою підприємства та ефективність роботи правил виявлення подій безпеки.
   4.2. Дослідити архітектуру, функціональність та різновиди SIEM-систем, а також практичне застосування Elastic SIEM на підприємстві.
   4.3. Вивчити типи та принципи побудови правил виявлення загроз у SIEM-системі, розробити рекомендації щодо вдосконалення механізмів виявлення та реагування на інциденти інформаційної безпеки.
5. Перелік ілюстративного матеріалу: *презентація PowerPoint*
6. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Аналіз особливостей управління інформаційною безпекою підприємства	08.04.2025	
4.	Дослідження основних характеристик технологій формування обізнаності й навчання персоналу.	15.04.2025	
5.	Вивчення інструментів та методів формування обізнаності й навчання персоналу з інформаційної безпеки	22.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	
7.	Оформлення роботи.	06.05.2025	
8.	Оформлення презентації.	09.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ЕК.	__.06.2025	

Здобувачка вищої освіти _____ Єлизавета НИКИТЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(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 здобувачка Никитенко Є.Я. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Модель управління інцидетами безпеки з використанням SIEM-систем"

Кваліфікаційна робота і рецензія додаються.

Директор ННІКБЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувачка НИКИТЕНКО Єлизавета у кваліфікаційній роботі розглянула основний функціонал, принципи роботи та роль SIEM-систем в управлінні інцидентами на підприємстві; проаналізувала визначені правила роботи SIEM-системи на підприємстві та провела моніторинг ризиків безпеки інформації на підприємстві; провела моніторинг безпеки за попередньо налаштованими правилами роботи SIEM-системи. Робота відзначається практичною цінністю за рахунок запропонованої у роботі моделі управління інцидентами безпеки з використанням SIEM-системи на основі ризик-сценаріїв. НИКИТЕНКО Єлизавета продемонструвала розуміння проблематики дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довела володіння методами наукового дослідження. Особисті характеристики, такі, як: організованість, відповідальність, послідовність дозволили виконати роботу цілісно та логічно вибудованою, завершеною.

Враховуючи означене, кваліфікаційну роботу здобувачки НИКИТЕНКО Єлизавети можна оцінити на "відмінно" та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою «Управління інформаційною та кібернетичною безпекою».

Керівник кваліфікаційної роботи _____ Тетяна КАПЕЛЮШНА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____"_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувачка Никитенко Є.Я. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри управління кібербезпекою та захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувачки вищої освіти НИКИТЕНКО Єлизавети
на тему: "Модель управління інцидентами безпеки з використанням SIEM-систем"

Актуальність. Тема кваліфікаційної роботи відзначається актуальністю в умовах зростання кількості та складності інформаційних загроз, що системно впливають на стабільність цифрової інфраструктури підприємств і установ. Кіберсередовище, яке характеризується високим рівнем зростання, непередбачуваності атак та появою нових векторів порушення інформаційної безпеки потребує ефективного управління інцидентами, що дозволить забезпечити цілісність, конфіденційність та доступність інформаційних ресурсів. Тому дослідження типів та принципів побудови правил виявлення загроз у SIEM-системах (Security Information and Event Management), які є невід'ємним елементом сучасної архітектури захисту інформації, а також формування моделі управління інцидентами безпеки з використанням SIEM-систем, дозволять вирішити питання захисту підприємства від кібератак, що вкотре доводить актуальність теми дослідження.

Позитивні сторони.

1. У роботі розглянуто принципи централізованого збору, аналізу, обробки подій безпеки (ідентифікування подій), зокрема виокремлено вплив кореляції подій на інформаційну безпеку підприємства.

2. Аналіз набору правил, що функціонують в SIEM-системі (Elastic) підприємства, що доводить практичність проведеного дослідження.

3. Грунтовно проведений аналіз, а саме - більш, ніж 40 вбудованих правил та 10 кастомних, що використовуються на підприємстві для детектування загроз (фільтрація, агрегація, трансформація та аналіз даних журналів).

Недоліки.

Зважаючи на зростання кількості кібератак та їх складність, а також на широкі можливості застосування новітніх технологій, розробок і технічних рішень в управлінні кібербезпекою на підприємстві, доцільно було б при побудові моделі управління інцидентами безпеки розглянути хмарні SIEM-рішення з використанням ШІ.

Проте дане зауваження не впливає на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки "відмінно", а - здобувачка НИКИТЕНКО Єлизавета заслуговує на присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою «Управління інформаційною та кібернетичною безпекою».

Рецензент: _____ Галина ГАЙДУР
д.т.н., професор, завідувач кафедри Систем та технологій кібербезпеки
підпис
Ім'я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню принципів функціонування, типів та практичного застосування SIEM-систем в управлінні інцидентами інформаційної безпеки. Робота складається зі вступу, трьох розділів, що містять 17 рисунків, 9 таблиць, висновків і списку використаних джерел із понад 35 найменувань. Загальний обсяг роботи становить 65 сторінок.

Метою роботи є дослідження функціоналу, ефективності та практичного використання SIEM-систем для виявлення, аналізу, реагування на інциденти інформаційної безпеки та побудови моделі управління інцидентами на підприємстві.

Об'єктом дослідження виступають SIEM-системи як інструмент управління подіями та інцидентами інформаційної безпеки.

Предмет дослідження – принципи побудови правил аналітики, кореляції подій та реагування на інциденти в SIEM-системі

Методи дослідження. Для вирішення наукового завдання в роботі використано методи аналізу, синтезу, дедукції, узагальнення, спостереження, порівняння.

У результаті дослідження проведено огляд функцій, переваг та недоліків різних типів SIEM-систем; проаналізовано аналітичні правила у Elastic SIEM; проведено моніторинг подій безпеки; побудовано рекомендації щодо оптимізації правил, зменшення хибнопозитивних спрацювань та інтеграції з SOAR-рішеннями.

Галузь застосування. Результати дослідження можуть бути використані фахівцями з кібербезпеки, адміністраторами систем та розробниками політик ІБ для побудови або вдосконалення моделей реагування на інциденти в корпоративних IT-інфраструктурах.

Ключові слова: SIEM, ELASTIC SIEM, ІНФОРМАЦІЙНА БЕЗПЕКА, ІНЦИДЕНТИ БЕЗПЕКИ, ЛОГУВАННЯ, KQL, МОНІТОРИНГ ЗАГРОЗ, KIBANA, КОРЕЛЯЦІЯ ПОДІЙ, SOAR, BRUTE FORCE, ІНДИКАТОРИ КОМПРОМЕТАЦІЇ.

ABSTRACT

The qualification work is devoted to the study of the principles of functioning, types and practical application of SIEM systems in information security incident management. The work consists of an introduction, three chapters containing 17 figures, 9 tables, conclusions and a list of references of more than 35 titles. The total volume of the work is 65 pages.

The purpose of the study is to investigate the functionality, efficiency and practical use of SIEM systems for detecting, analysing and responding to information security incidents.

The object of the study is SIEM systems as a tool for managing information security events and incidents.

The subject of the study is the principles of building analytics rules, correlating events and responding to incidents in a SIEM system.

Research methods. To solve the above scientific task, the paper uses the analysis of scientific sources, practical monitoring of security events, building KQL queries, and testing threat detection rules.

As a result of the study, an overview of the functions, advantages and disadvantages of different types of SIEM systems was conducted; analytical rules in Elastic SIEM were analysed; security events were monitored; recommendations for optimising rules, reducing false positives and integrating with SOAR solutions were made.

Field of application. The results of the study can be used by cybersecurity specialists, system administrators, and IS policy makers to build or improve incident response models in corporate IT infrastructures.

Keywords: SIEM, ELASTIC SIEM, INFORMATION SECURITY, SECURITY INCIDENTS, LOGGING, KQL, THREAT MONITORING, KIBANA, EVENT CORRELATION, SOAR, BRUTE FORCE, COMPROMISE INDICATORS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AD	Active Directory (система каталогів, яка використовується для керування мережами)
GDPR	General Data Protection Regulation (загальний регламент про захист даних)
IDS	Intrusion Detection System (система виявлення вторгнень)
IP	Internet Protocol (міжмережевий протокол)
IPS	Intrusion Prevention System (система запобігання вторгнень)
KQL	Kusto Query Language (мова запитів Kusto)
RDP	Remote Desktop Protocol (протокол віддаленого робочого стола)
SEM	Security event management (управління подіями безпеки)
SIEM	Security information and event management (керування захистом інформації)
SIM	Security information management (управління інформаційною безпекою)
SMB	Server Message Block (протокол, що використовується для надання розділеного доступу до файлів тощо)
SOC	Security Operations Center (операційний центр безпеки)
SOAR	Security Orchestration, Automation and Response (оркестрування, автоматизація та реагування на загрози безпеки)
SSH	Secure Shell (протокол віддаленого адміністрування)
UEBA	User and Entity Behavior Analytics (аналіз поведінки користувачів і суб'єктів)
URL	Uniform Resource Locator (стандартизована адреса певного ресурсу)
VPN	Virtual Private Network (віртуальна приватна мережа)
ІБ	Інформаційна безпека
ПЗ	Програмне забезпечення

ВСТУП

Актуальність теми. На сьогоднішній день підприємства постійно стикаються з дедалі складнішими кібератаками. Одним із напрямів забезпечення кіберзахисту є ефективне управління інцидентами безпеки, що ґрунтується на централізованому зборі, обробці та аналізі подій. SIEM-системи є критично важливими інструментами для своєчасного виявлення загроз, кореляції подій, автоматичного реагування та формування звітності для дотримання нормативних вимог. SIEM-технології дозволяють об'єднати всі події безпеки з різних джерел в єдину інформаційну систему, підвищуючи загальну ефективність управління кіберризиками. Ураховуючи зростання складності IT-інфраструктур, обсягів логів і регуляторних вимог, дослідження SIEM-рішень як інструменту управління інцидентами є актуальним науковим завданням.

Мета роботи є дослідження функціоналу, ефективності та практичного використання SIEM-систем для виявлення, аналізу, реагування на інциденти інформаційної безпеки та побудови моделі управління інцидентами на підприємстві.

Об'єкт дослідження виступають SIEM-системи як інструмент управління подіями та інцидентами інформаційної безпеки.

Предмет дослідження – принципи побудови правил аналітики, кореляції подій та реагування на інциденти в SIEM-системі.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати принципи роботи та архітектуру SIEM-систем.
2. Дослідити типи інцидентів та правила, які використовуються в SIEM-системах.
3. Провести моніторинг подій безпеки на підприємстві та оцінити ефективність налаштованих правил.
4. Запропонувати модель управління інцидентами для підвищення ефективності реагування на інциденти за використання SIEM на підприємстві.

Методи дослідження. Для вирішення наукового завдання в роботі використано методи аналізу, синтезу, дедукції, узагальнення, спостереження, порівняння.

Практичне значення одержаних результатів. Результати дослідження можуть бути використані для удосконалення процесів моніторингу та управління інцидентами в корпоративному середовищі. Запропоновані підходи до аналізу та оптимізації правил виявлення загроз у SIEM-системі дають змогу підвищити точність детекції, знизити навантаження на аналітиків безпеки та забезпечити ефективну і своєчасну реакцію на потенційні загрози. Результати дослідження апробовані на науково-практичній конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу».

Розділ 1 SIEM-СИСТЕМИ ТА ЇХ РОЛЬ В УПРАВЛІННІ ІНЦИДЕНТАМИ БЕЗПЕКИ

1.1. SIEM-системи та їх функціональність (функції)

Компанії чітко розуміють, як забезпечення кібербезпеки покращується завдяки появі нових технологій, штучному інтелекту. Однак одночасно зростають обсяг і складність кібератак, особливо якщо підприємства не використовують відповідні засоби моніторингу інцидентів і виявлення загроз.

Дослідження Deloitte показало, що 2023 року 12,5% підприємств зазнали більше одного інциденту кібербезпеки. Як результат, абсолютна безпека неможлива, але компанії повинні намагатися досягти максимально можливого рівня безпеки.

SIEM — це комбінація двох термінів, що представляють сферу застосування програмного забезпечення: SIM — керування інформацією про безпеку та SEM — керування подіями безпеки. Технологія SIEM забезпечує аналіз у режимі реального часу подій безпеки (сповіщень), що надсилаються мережевими пристроями та програмами, і дозволяє реагувати на них до того, як буде завдано значної шкоди [1].

Подія в контексті кібербезпеки — це будь-яка спостережувана дія або випадок, що відбувається в інформаційній системі, мережі чи сервісі та має значення для підтримки безпеки. Це може бути як нормальна активність (наприклад, авторизацію користувача), так і дія, що потенційно становить загрозу (наприклад, спроба несанкціонованого доступу). Події є базовими компонентами, з яких формується аналіз ситуації стосовно безпеки в системі.

Прикладами подій є:

- вхід або вихід користувача з системи;
- зміни у правах доступу;
- активація антивірусного захисту;
- виявлення підозрілої мережевої активності;

- спроби несанкціонованого доступу;
- помилки автентифікації;
- виявлення шкідливого програмного забезпечення.

Керування подіями безпеки — це процес виявлення, збору, нормалізації, аналізу та реагування на події, що можуть впливати на інформаційну безпеку. Основна мета цього процесу полягає у своєчасному виявленні потенційних загроз, запобіганні інцидентам, та забезпеченні вищого рівня захищеності інформаційних активів.

Основні етапи керування подіями безпеки:

- Збір подій з різних джерел (журнали систем, мережеве обладнання, антивірусні програми, тощо);
- Нормалізація та кореляція — приведення подій до єдиного формату та виявлення зв’язків між ними;
- Аналіз отриманих даних для виявлення потенційних інцидентів;
- Повідомлення та ескалація важливих подій до відповідального персоналу;
- Збереження подій для проведення аудиту, криміналістичних досліджень та дотримання вимог законодавства;
- Візуалізація — представлення подій у вигляді графіків, діаграм тощо для зручності моніторингу.

Керування інформацією про подію — це сукупність процесів, спрямованих на збирання, обробку, зберігання, аналіз та використання даних про події в інформаційній системі. Охоплює як технічні аспекти , як обробка логів чи створення звітів, так і організаційні , зокрема визначення відповідальних осіб та політик реагування [4,5].

Ключові елементи управління інформацією про подію:

- Централізоване логування з систем, пристроїв та додатків;
- Категоризація подій за рівнем критичності або джерелом виникнення;
- Фільтрація шуму (неважливих або повторюваних подій);
- Інтеграція з SOAR-системами для автоматизованого аналізу;

- Аналіз подій з огляду на специфіку та контекст організації;
- Звітність — формування звітів для внутрішнього контролю та зовнішнього аудиту;
- Довгострокове зберігання даних про події для забезпечення безперервного аналізу та відповідності вимогам безпеки.

Постійне зростання обсягів інформації, що обробляється та передається між різними інформаційними системами, передбачає, що організації та окремі користувачі все більше покладаються на безперервність і правильність цих процесів. Для боротьби із загрозами безпеці в ІБ необхідно мати інструменти, які можуть аналізувати події в режимі реального часу, кількість яких буде тільки збільшуватися. Одним з таких рішень проблеми є система SIEM. Ключовою функцією системи SIEM є збір даних про безпеку інформаційної системи з усіх можливих джерел і надання результатів їх обробки в єдиному інтерфейсі, який можуть використовувати аналітики безпеки, що сприяє вивченню характеристик, що відповідають інцидентам безпеки. SIEM — це поєднання системи управління безпекою інформації (SIM) і управління подіями безпеки (SEM) в одну систему управління безпекою [1-3].

Сегмент SIM в основному відповідає за аналіз даних для покращення довгострокової продуктивності системи та оптимізації зберігання даних. З іншого боку, частина SEM зосереджується на отриманні певної кількості інформації з наявних даних, яка може негайно ідентифікувати інциденти безпеки. Оскільки попит на додаткові функції продовжує зростати, функціональність цієї категорії продуктів постійно розширюється та доповнюється [2,3].

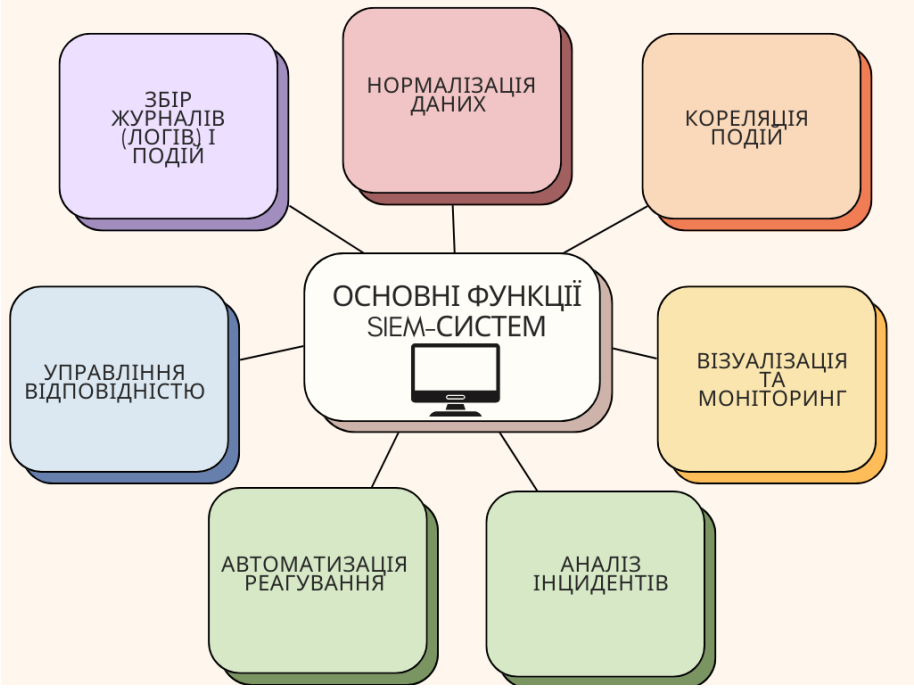

Рис. 1.1. Основні функції SIEM-систем

Розглянемо основні функції SIEM-систем:

- Збір журналів (логів) і подій:

отримання інформації від серверів, мережевих компонентів, систем безпеки (антивіруси, брандмауери, IDS/IPS) тощо.

підтримка різних форматів логів (Syslog, Windows Event Logs, JSON (JavaScript Object Notation), XML (eXtensible Markup Language) тощо).

- Нормалізація даних:

перетворення логів у стандартизований формат для подальшого аналізу.

забезпечує уніфікований вигляд даних з різних джерел.

- Кореляція подій:

аналіз зв’язків між подіями з різних джерел для виявлення складних атак. Наприклад, входи з незвичних IP-адрес, багаторазові невдалі спроби входу, доступ до конфіденційних файлів тощо.

- Виявлення інцидентів безпеки:

генерація сповіщень (alerts) на основі виявлених аномалій або підозрілих шаблонів поведінки.

часто використовуються правила, сигнатури або навіть машинне навчання.

- Візуалізація та моніторинг:

дашборди, графіки, аналітичні панелі для моніиорингу в реальному часі.

фільтрація і агрегація даних за джерелами, типами загроз, критичністю тощо.

- Аналіз інцидентів:

збереження історії подій для подальшого аналізу.

допомога в розслідуванні інцидентів: хто, коли, що зробив.

- Автоматизація реагування (SOAR-функціональність):

інтеграція з системами реагування (наприклад, блокування IP, відключення акаунтів).

запуск скриптів чи автоматизованих дій у відповідь на загрозу.

- Управління відповідністю:

підтримка стандартів безпеки: ISO 27001, GDPR, PCI DSS (Payment Card Industry Data Security Standard), HIPAA (Health Insurance Portability and Accountability Act) тощо.

формування звітів для аудитів та контролюючих органів.

SIEM-системи відіграють ключову роль у забезпеченні відповідності організацій сучасним стандартам кібербезпеки та захисту даних. Вони допомагають автоматизувати збір, зберігання, аналіз подій безпеки й формування звітів, які потрібні для демонстрації дотримання регуляторних вимог. Розглянемо деякі стандарти більш детально.

ISO/IEC 27001 — міжнародний стандарт, що встановлює вимоги до створення, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою. SIEM сприяє дотриманню цього стандарту шляхом ведення журналів доступу, контролю змін у системах та моніторингу безпеки в реальному часі [1].

GDPR — регламент Європейського Союзу (ЄС) про захист персональних даних. Він встановлює вимоги до обробки, зберігання та доступу до персональної інформації. SIEM допомагає виявляти несанкціонований доступ до персональних даних, вести журнал активності користувачів і зберігати докази подій безпеки, що можуть вплинути на конфіденційність [7].

HIPAA — закон США, який регулює обробку та захист медичної інформації (PHI — Protected Health Information). SIEM забезпечує аудит доступу до медичних даних, контроль безпеки електронної медичної інформації та інцидент-менеджмент [8].

Системи SIEM допомагають зменшувати ризики для кібербезпеки за допомогою низки сценаріїв використання, як-от виявлення підозрілих дій користувачів, відстеження поведінки користувачів, обмеження спроб доступу й генерування звітів про відповідність вимогам [2].

Приклад роботи SIEM:

Якщо після послідовних спроб невдалого входу з різних IP-адрес протягом короткого часу, система визначає це як brute-force атаку, тоді вона може вжити автоматичних дій, щоб заблокувати IP або надіслати сповіщення.

1.2. Принципи роботи SIEM-систем та їх роль в управлінні інцидентами

SIEM-системи функціонують за принципом централізованого збору, аналізу та обробки подій безпеки з усієї IT-інфраструктури (рис.1.2).

1. Збір даних.

Основним завданням SIEM є отримання даних від джерела. Більшість рішень SIEM збирають дані з корпоративних інформаційних систем за допомогою агентів, установлених на різних пристроях, включаючи кінцеві точки, сервери та мережеві пристрої, а також інші рішення безпеки, такі як брандмауери та інші пристрої захисту мережі. Рішення SIEM останнього покоління включають підтримку хмарних додатків та інфраструктури, а також корпоративних програм. Рішення SIEM повинні збагачувати вхідні дані інформацією про ідентифікацію, активи, геолокацію та інформацію про загрози, щоб допомогти розслідуванням. Розширення даних заповнює важливу інформацію, необхідну SIEM для поєднання пов’язаних подій та допомогти у виявленні загроз. Після розширення дані безпеки зберігаються в базі даних. Там їх можна шукати та посилатися на них під час

розслідування. Найчастіше зберігаються лише дані з розширеною інформацією, але іноді зберігається все. Все залежить від вимог компанії. Останнє покоління SIEM використовує архітектуру великих даних з відкритим кодом, щоб скористатися їх необмеженою масштабованістю та можливістю зберігати дані у зручному для пошуку форматі [3].

2. Агрегація і нормалізація.

Після отримання даних з різних джерел, система SIEM уніфікує їх у стандартний формат, що робить їх придатними для подальшої обробки – це називається нормалізацією. Порівняйте це з великою компанією, яка складається зі співробітників з різних країн: кожен говорить своєю мовою, а система SIEM слухає всіх і нормалізує це, тобто перекладає все на, наприклад, англійську, щоб ви могли бачити всю розмову однією зрозумілою мовою. Далі система SIEM виконує таксономію, яка є процесом класифікації вже нормалізованих сповіщень на основі їх вмісту: яке з них стосується успішної мережевої комунікації, яке сигналізує про входження користувача на комп'ютер, і яке вказує на спрацювання антивірусу. Таким чином, утворюється послідовність подій, де кожна подія має певний зміст і час виникнення, що дозволяє зрозуміти ланцюжок подій і зв'язки між ними [6].

3. Кореляція подій.

Кореляція в SIEM – це співвідношення між собою подій, які відповідають тим чи іншим умовам (правилам кореляції).

Приклад кореляційного правила: якщо антивірусне програмне забезпечення активується на двох або більше комп’ютерах протягом 5 хвилин, це може вказувати на те, що компанію вразила вірусна атака. Більш складне правило: якщо протягом 24 годин реєструються спроби віддаленого входу на сервер, які зрештою успішні, а потім з цього сервера почалося копіювання даних на зовнішній файлообмінник, це може свідчити про те, що зловмисники підібрали пароль до облікового запису, отримали доступ до сервера та крадуть важливі дані [1].

Рішення SIEM використовують різні методи для виявлення корисної інформації з даних і виявляти аномалії. Ці методи аналізу відрізняються залежно від виробника. Перші SIEM покладалися на просту кореляцію та попередження на

основі підпису. Вони схильні до помилок, генерують велику кількість помилкових спрацьовувань і виявляють лише відомі загрози. Наступне покоління SIEM використовує передові аналітичні методи, крім підходів, заснованих на підписах, для виявлення відомих і невідомих загроз. Вони використовують складні алгоритми машинного навчання для точнішого виявлення загроз (поведінкова аналітика користувачів та сутності (UEBA) та інші) [3].

4. Виявлення загроз. Інформування та реагування

На основі спрацьовування кореляційних правил у SIEM-системі формується інцидент інформаційної безпеки (у деяких системах, наприклад, у SIEM IBM QRadar інцидент називається Offense). При цьому фахівець з ІБ при використанні SIEM повинен мати можливість швидко шукати попередні події, що зберігаються в системі SIEM, якщо йому знадобляться додаткові технічні деталі для розслідування атаки. На базовому рівні SIEM повинна включати інтеграцію зі стороннім рішенням організації, автоматизації та реагування на безпеку (SOAR), щоб допомогти аналітикам проводити розслідування та усувати потенційні загрози. Рішення SOAR надають аналітикам простір для збору інформації, відстеження кроків, зроблених під час розслідування, і запам’ятовування способів усунення загрози [1,3].

5. Звітність

Аналіз подій, інцидентів та їх наслідків передбачає процедури, які моделюють події, атаки та їх наслідки, аналіз вразливостей системи та безпеки, визначення параметрів порушників, оцінки ризику, прогнозування подій та інцидентів. Створення звітів та попереджень означає формування, передачу, відображення чи друк результатів діяльності. SIEM дає можливість швидко здійснювати пошук у даних, дозволяючи заглиблюватися в попередження та шукати учасників. Візуалізація передбачає подання у графічному вигляді даних, що характеризують результати аналізу подій безпеки та стан системи, що захищається, та її елементів [3,4].

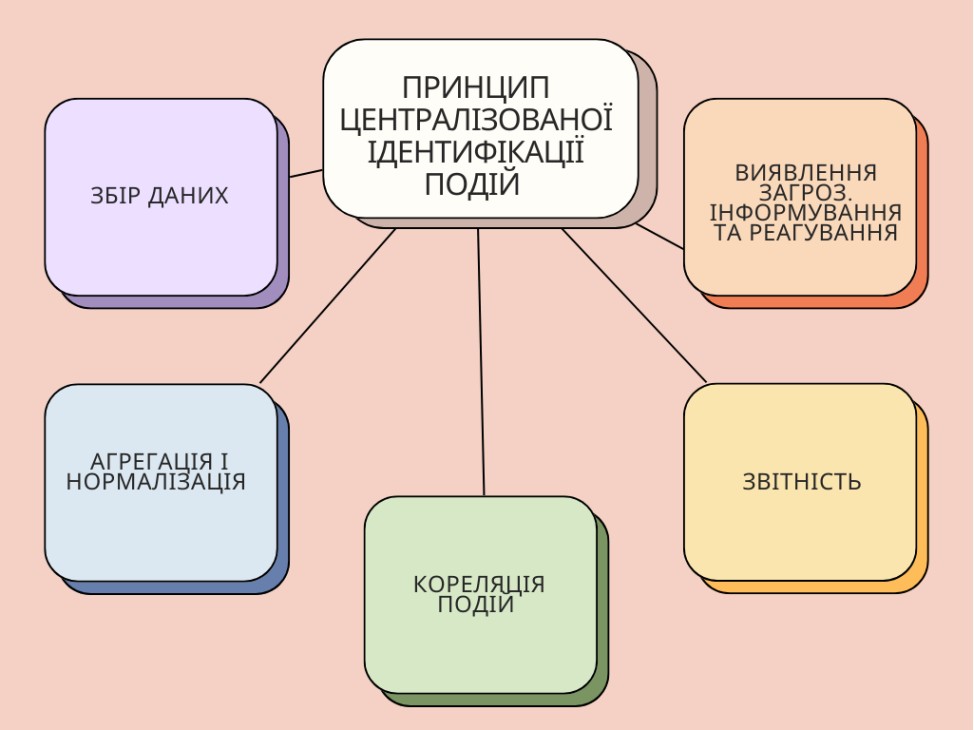

Рис. 1.2. Принцип централізованої ідентифікації подій (збору, аналізу та обробки подій безпеки) IT-інфраструктури

На додаток до зазначених функцій системи SIEM також можуть бути оснащені додатковими функціями, такими як управління ризиками та вразливістю, інвентаризація IT-активів, звіти та діаграми тощо. Автоматизоване реагування на інцидент також можна налаштувати, для цього використовують системи IRP (Incident Response Platform, платформи реагування на інциденти інформаційної безпеки), які можуть без участі людини, наприклад, заблокувати зламаний обліковий запис або відключити інфікований комп'ютер від мережі. Підсумовуючи, ми можемо сказати, що системи SIEM необхідні компаніям для роботи з великим потоком різноманітних даних від різних джерел з метою виявлення потенційних інцидентів інформаційної безпеки та своєчасного реагування на них.

SIEM незамінний інструмент SOC із цінними можливостями. Його головною перевагою є можливість створити централізовану видимість середовища та контекстуалізувати великі обсяги даних. Система збирає інформацію про всі засоби безпеки та рішення, допомагаючи командам SOC краще орієнтуватися в складних

багатокомпонентних середовищах і отримати повне розуміння діяльності всього підприємства. За допомогою SIEM дані безпеки та контекстні джерела об’єднані в єдину систему. Це надає оперативним групам засоби для виявлення потенційних загроз, дотримання нормативних вимог і ефективного управління інцидентами. Аналізуючи дані подій і контекст, SIEM виявляє зв’язки, які інакше могли б бути пропущені в одному джерелі даних [5,6].

1.3. Види SIEM-системи: переваги та недоліки їх використання в управлінні інцидентами

Зростання складності IT-інфраструктур, збільшення кількості кіберзагроз та посилення вимог до захисту даних з боку регуляторів призвели до необхідності створення централізованих рішень для моніторингу та управління інформаційною безпекою. SIEM-системи стали відповіддю на ці виклики.

SIEM-системи виникли як результат декількох ключових чинників:

1. Фрагментованість джерел даних безпеки

У традиційних IT-системах події безпеки реєструються в журналах (логах) окремих пристроїв: серверів, маршрутизаторів, міжмережевих екранів, антивірусів тощо. Без централізованої платформи їх важко корелювати й аналізувати в сукупності.

2. Необхідність оперативного реагування на загрози

Зростання швидкості та складності атак потребує інструментів, які можуть виявити інцидент у реальному часі й автоматично ініціювати захисні дії.

3. Надмірність інформації

Великі обсяги подій безпеки ускладнюють виявлення дійсно важливих інцидентів без спеціальних засобів фільтрації, нормалізації та аналізу.

4. Потреба у відповідності до стандартів і регуляцій

Законодавчі вимоги (наприклад, GDPR, ISO 27001) зобов’язують організації вести облік подій, забезпечувати аудит і зберігати логи протягом визначених строків.

5. Висока вартість кіберінцидентів

Фінансові та репутаційні втрати, пов’язані з витоками даних чи атаками, стимулювали інвестування в проактивні системи кіберзахисту.

6. Поява нових технологій та обчислювальних ресурсів

Розвиток обчислювальних потужностей, хмарних сервісів і великих даних (big data) зробив можливим централізоване збирання, зберігання та аналіз мільйонів подій у реальному часі.

Ці фактори стали рушійною силою для впровадження SIEM-систем, які забезпечують гнучкість, ефективність аналізу та швидке реагування на потенційні загрози.

Історично SIEM-системи були локальними, але з розширенням хмарних технологій з’явилося декілька видів систем. Розглянемо кожну з них:

On-premise (локальна) SIEM — традиційна модель, де вся інфраструктура у користувача.

Cloud-based (хмарна) SIEM — повністю хмарна SIEM, керована вендором.

Hybrid (гібридна) SIEM — комбінація обох підходів.

Вибір SIEM-системи напряму впливає на ефективність управління інцидентами інформаційної безпеки.

Локальні (on-premise) SIEM-системи — це рішення для моніторингу, аналізу та управління подіями безпеки, які розгортаються безпосередньо в інфраструктурі компанії. Тобто, це рішення, яке інсталюється локально на обладнанні компанії. Його обслуговує внутрішній IT-відділ або спеціалізована служба безпеки (SOC). Локальні SIEM-системи дозволяють організаціям повністю контролювати свої дані, забезпечують високий рівень кастомізації та можуть краще відповідати вимогам регуляторів або політик конфіденційності [11, 12].

Перевагами використання локальних SIEM-систем є повний контроль над інфраструктурою та даними. Всі логи, інциденти, конфігурації та аналітика зберігаються локально. Даний вид систем також краще підходить для середовищ з високими вимогами до конфіденційності. Немає потреби передавати чутливу

інформацію через зовнішні мережі або зберігати її в хмарі. Також є можливість глибокої кастомізації та інтеграції з локальними системами.

Серед недоліків можна виділити наступні пункти:

Високі витрати на впровадження та обслуговування (потрібні сервери, місце, IT-персонал для підтримки)

Складність масштабування при зростанні об’ємів логів

Тривалий процес впровадження та налаштування (адміністратор повинен самостійно слідкувати за оновленнями, патчами тощо)

Хмарні (cloud-based) SIEM-системи — це системи управління інформаційною безпекою та подіями, які працюють у хмарному середовищі. Вони збирають, аналізують та корелюють події з різних джерел для виявлення загроз і реагування на інциденти безпеки без необхідності використання локальної інфраструктури. Тобто, джерела подій (сервери, хост-машини, мережеві пристрої, хмара, SaaS-додатки) передають логи в хмарну платформу. Далі SIEM-система приймає дані через агенти, API (application programming interface) або колектори. Вона аналізує події, корелює, формує оповіщення, візуалізує інформацію в дашбордах. В свою чергу аналітик SOC чи система SOAR приймає рішення або автоматично реагує на загрозу. Компанія використовує SIEM як хмарний сервіс, усуваючи потребу мати справу з фізичним обладнанням чи розгортанням системи [12-14].

Основними перевагами хмарної SIEM є швидке розгортання (не потрібно встановлювати фізичне обладнання або локальні сервери), масштабованість (легко адаптується до потреб бізнесу — можна обробляти більше логів при зростанні обсягу даних), цілодобова доступність (доступ з будь-якої точки світу з інтернетом), оновлення та підтримка (постійно оновлюються вендором — немає потреби самостійно оновлювати систему) та вартість (зменшення витрат на інфраструктуру та обслуговування).

Серед недоліків можна звернути увагу на наступні аспекти, як обмежені можливості для глибокої кастомізації та більшу вартість. Також варто зазначити залежність від підключення до Інтернету, менший контроль над внутрішніми

компонентами системи і те, що передача чутливої інформації в хмару може порушувати питання безпеки та відповідності стандартам (наприклад, GDPR).

Багато хмарних SIEM вже включають машинне навчання для виявлення аномалій поведінки користувачів, автоматичної класифікації загроз, виявлення нових (zero-day) атак, автоматичного створення правил на основі поведінкових патернів.

Приклад використання хмарної SIEM

У компанії використовується Microsoft 365, Azure, Salesforce та AWS. Всі сервіси відправляють журнали подій у Microsoft Sentinel. Там автоматично спрацьовує правило:

- Неавторизована спроба логіну з Франції
- Через 3 хвилини – масове скачування файлів із OneDrive
- Система автоматично блокує сесію, надсилає повідомлення в Teams та створює тикет у ServiceNow.

Гібридні (hybrid) SIEM-системи — представляють собою інтегровані рішення, що поєднують в собі локальні та хмарні компоненти SIEM. Вони надають компаніям можливість використовувати переваги обох підходів: контроль і безпеку локальної інфраструктури разом з гнучкістю і масштабованістю хмари. Гібридна SIEM включає компоненти, які можуть бути розміщені як локально (агенти збору логів, джерела даних (сервери, мережеві пристрої, комп’ютери)), так і у хмарі (лог-аналітики, системи зберігання, машинне навчання, візуалізація) [16].

Безпечна взаємодія між компонентами забезпечується через шифровані канали передачі даних (TLS - transport layer security, VPN) та агенти або API, які інтегруються з системами (AWS CloudTrail, Azure Monitor).

Основні переваги такого підходу до SIEM:

можливість зберігати чутливі дані локально, а решту — в хмарі;

гнучкість адаптації під структуру конкретної організації;

підтримка різних джерел даних — від фізичних серверів до хмарних додатків;

висока відмовостійкість — дані можуть дублюватися між хмарою і локальним середовищем;

можливість відповідності вимогам безпеки та регуляторним нормам (наприклад, GDPR, ISO 27001, NIST).

Проблеми використання гібридної SIEM-системи полягає у складності архітектури - потрібно забезпечити узгоджену взаємодію між хмарними та локальними компонентами. Безпека передачі даних є ще однією значною проблемою, оскільки дані мають бути надійно зашифровані під час їхнього переміщення між середовищами. Крім того, підтримка двох середовищ може бути більш затратною, ніж вибір повністю хмарної моделі. Останнім викликом є залучення кваліфікованого персоналу, оскільки потрібна команда з досвідом роботи як з локальними, так і з хмарними технологіями.

Приклади використання гібридної SIEM

Банківська сфера, в якій частина даних — надсекретна (транзакції), але логування зовнішніх сервісів — у хмарі.

Університети чи навчальні заклади. Локальні мережі та використання Google Workspace чи Microsoft 365.

Органи державного управління. Вимоги до зберігання даних в межах країни, але при цьому потреба в сучасній аналітиці.

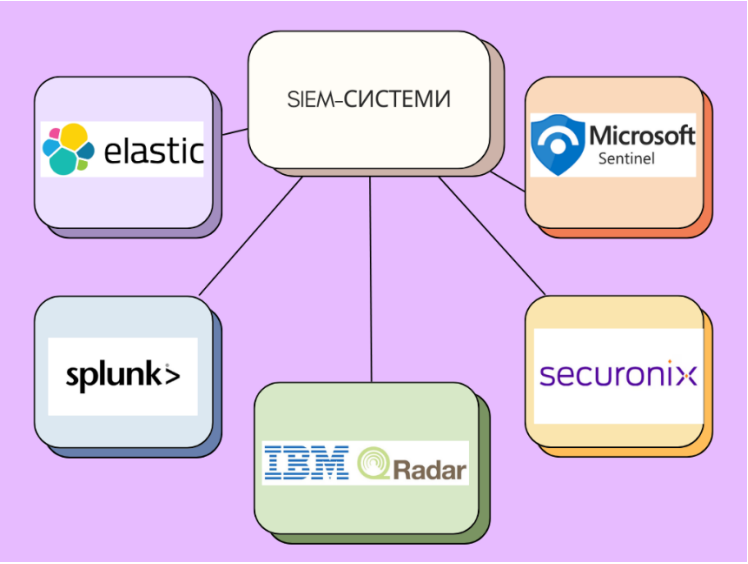

Рис. 1.3. Різновиди представлених на ринку SIEM-систем

Таблиця 1.1.

Переваги та недоліки SIEM-систем

Назва	Тип (вид)	Переваги	Недоліки
Splunk Enterprise Security	Локальна, також є хмарна версія (Splunk Cloud)	Гнучкий пошук і візуалізація. Потужна аналітика даних кореляція подій. Широка екосистема додатків і інтеграцій. Висока масштабованість	Висока вартість. Складність налаштування. Вимагає потужних ресурсів.
IBM QRadar	Локальна, але має хмарні рішення (QRadar on Cloud)	Автоматизація завдяки QRadar SOAR. Сильна інтеграція з продуктами IBM. Вбудована кореляція та поведінковий аналіз	Застарілий інтерфейс. Повільне оновлення та підтримка нових джерел.
Securonix	Хмарна	Побудована на основі машинного навчання. Хороша поведінкова аналітика (UEBA). Масштабованість без прив'язки до інфраструктури.	Повна залежність від хмари. Може бути складною для початкового налаштування. Затримки у підтримці.
Microsoft Sentinel	Хмарна	Глибока інтеграція з Microsoft-екосистемою. Доступна ціна. Хороша автоматизація (SOAR через Logic Apps).	Висока вартість при великому обсязі даних. Обмежена підтримка не-Microsoft рішень. Залежність від Azure.
Elastic Security	Гібридна	Безкоштовна базова версія (ELK Stack). Потужний пошук (Elasticsearch). Гнучкість інтеграції (інтеграція з Beats, Logstash, Kibana).	Складність налаштування. Обмежена підтримка у безкоштовній версії. Менша автоматизація порівняно з іншими.

Вибір типу системи SIEM виступає ключовим рішенням, яке безпосередньо впливає на ефективність управління інцидентами інформаційної безпеки. Кожна модель має певний ряд переваг та обмежень, які слід ретельно оцінювати виходячи з конкретних особливостей бізнесу, бюджетні можливості, вимог до безпеки та

масштабованості. Локальні SIEM є доцільними для організацій, які прагнуть повного контролю над даними, мають суворі регуляторні обмеження та власну технічну інфраструктуру. У той же час вони вимагають великих витрат на розгортання та обслуговування. Хмарні SIEM пропонують швидке впровадження, масштабованість і постійні оновлення, що робить їх привабливими для компаній, які активно використовують хмарні сервіси. Однак їм потрібно бути обережними з питаннями безпеки та дотримуватися стандартів захисту конфіденційних даних. Гібридні системи SIEM пропонують збалансований підхід, поєднуючи локальну безпеку з перевагами гнучкості хмари. Вони оптимально підходять для організацій із гібридною IT-інфраструктурою, хоча вимагають складнішого управління та додаткової підготовки технічних спеціалістів. В умовах постійного зростання обсягів даних, складності інфраструктури та появи нових загроз гібридний підхід дедалі частіше вважається оптимальним — він дозволяє отримати максимум користі з обох типів, мінімізуючи їхні недоліки.

Висновки до розділу 1

В умовах зростаючої складності кіберзагроз і вимог до інформаційної безпеки SIEM-системи відіграють важливу роль у виявленні, аналізі та реагуванні на інциденти. Вони інтегрують функції збору, кореляції та аналізу подій, забезпечуючи централізований контроль над IT-інфраструктурою у режимі реального часу. SIEM дозволяють своєчасно ідентифікувати загрози завдяки нормалізації даних, кореляції подій та автоматизації відповідей на інциденти, що значно підвищує ефективність системи безпеки підприємства. Важливою перевагою SIEM є їх здатність забезпечувати відповідність міжнародним стандартам (ISO 27001, GDPR, HIPAA) і адаптуватися до специфіки конкретної організації. Це можливо завдяки варіативному підходу до вибору конфігурації системи: локальної, хмарної чи гібридної. Локальні системи забезпечують повний контроль над даними, хмарні — гнучкість та швидке масштабування, а гібридні — оптимальний баланс між безпекою і функціональністю. З огляду на зазначені

характеристики, інтерграція SIEM-систем у сучасні моделі кіберзахисту є необхідною умовою для ефективного запобігання потенційним загрозам та забезпечення захисту цифрових активів організації.

Розділ 2 АНАЛІЗ ТА ОЦІНКА ПРАВИЛ РОБОТИ SIEM-СИСТЕМИ НА ПІДПРИЄМСТВІ

2.1. Аналіз визначених правил роботи SIEM-системи на підприємстві

Для проведення практичного дослідження було обрано компанію ‘ACCORD GROUP’. Accord Group — українська діджитал-компанія, яка з 2010 року спеціалізується на системній інтеграції та кібербезпеці. Компанія реалізувала понад 500 проєктів для міжнародних банків, ритейлу, державних організацій та промислових підприємств. Accord Group є партнером провідних світових виробників, таких як Cisco, F5, Riverbed, Dell, HPE, Lenovo, NetApp, та має власне представництво в ЄС. Серед ключових напрямків діяльності — інформаційна та кібербезпека, хмарні рішення, контакт-центри, IT-аутсорсинг та інші.

У рамках практичного дослідження було проведено аналіз набору правил, що функціонують в SIEM-системі (Elastic) підприємства. Основною метою цього аналізу була оцінка ефективності виявлення потенційних загроз і відповідності правил реальним інформаційним ризикам.

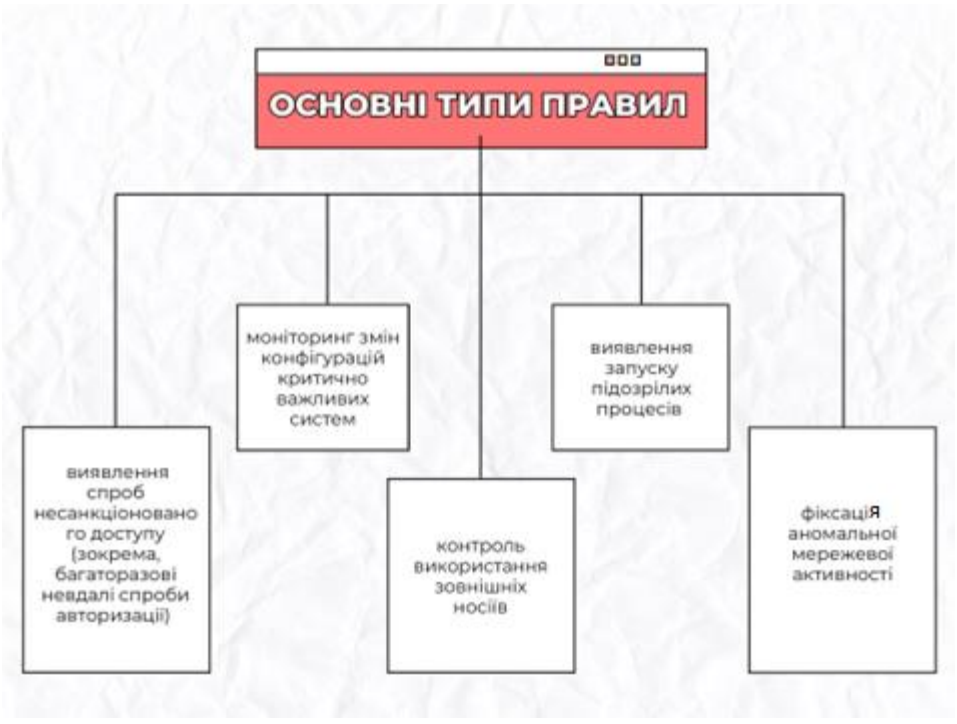

Рис.2.1. Основні типи правил

Основні типи правил включають виявлення спроб несанкціонованого доступу (зокрема, багаторазові невдалі спроби авторизації), моніторинг змін конфігурацій критично важливих систем, виявлення запуску підозрілих процесів, контроль використання зовнішніх носіїв, фіксацію аномальної мережевої активності.

Перейдемо до аналізу діючих механізмів виявлення подій у SIEM-системі підприємства.

1. Призначення та структура правил

Правила, які використовуються в SIEM-системах, являють собою набір логічних умов, що визначають, які події в IT-середовищі необхідно реєструвати, корелювати або розслідувати.

Їх побудова ґрунтується на поєднанні кількох ключових чинників. Передусім, це типові сценарії кіберзагроз, зокрема атаки типу brute force чи спроби підвищення привілеїв. Крім того, враховуються вимоги внутрішньої політики безпеки самого підприємства, що відображають його індивідуальні ризики та бізнес-процеси. Важливу роль також відіграють міжнародні стандарти та нормативи, такі як ISO 27001, NIST чи PCI DSS, які задають рамки відповідності. Доповнює цю систему підхід, заснований на сигнатурах і поведінкових патернах, що дозволяє враховувати як відомі загрози, так і аномалії в поведінці користувачів та систем [7-9, 18].

Наприклад, одне з правил може звучати так: якщо з однієї IP-адреси протягом останніх 5 хвилин зафіксовано понад 10 невдалих спроб входу, система має згенерувати сповіщення.

2. Класифікація правил

Усі правила, що застосовуються в SIEM-системі, зазвичай поділяються на кілька основних типів, кожен з яких виконує свою функцію в процесі виявлення інцидентів. Найбільш поширеними є кореляційні правила, які дозволяють аналізувати послідовність подій, що надходять із різних джерел — таких як мережеві логи, журнали операційних систем, антивірусне програмне забезпечення

тощо. Саме завдяки таким правилам можна виявляти складні багаторівневі атаки, що не завжди очевидні при аналізі окремих подій.

Ще одним важливим типом є сигнатурні правила. Вони побудовані на основі заздалегідь визначених шаблонів, як-от IP-адреси, URL-посилання чи хеші шкідливих файлів. Такі правила ефективні для швидкої ідентифікації вже відомих загроз, зокрема поширених вірусів або атак із характерними ознаками. [20]

Окрему роль відіграють поведінкові правила, які ґрунтуються на аналізі звичної поведінки користувачів і систем. Цей підхід – UEBA, дозволяє виявляти аномалії, які не потрапляють під жодну сигнатуру, але можуть свідчити про компрометацію облікових записів або зловмисні дії з боку внутрішніх користувачів.

3. Етапи аналізу правил

Рис.2.2. Етапи аналізу правил *у* SIEM-системі

Розглянемо детальніше ключові етапи аналізу правил у SIEM-системі. Перш за все, здійснюється ідентифікація активних правил, тобто перевіряється перелік активних правил, їхня актуальність, джерела даних, на які вони реагують, а також визначається рівень критичності кожного з них. Це дозволяє зрозуміти, наскільки правила відповідають сучасним загрозам і які з них потребують оновлення або уточнення.

Наступним важливим кроком є аналіз ефективності. Тут увага зосереджується на тому, як часто спрацьовують правила, чи не генерують вони надто багато хибнопозитивних сповіщень, а також наскільки їхні спрацювання

відповідають реальним інцидентам безпеки. Особливо важливо виявити потенційні прогалини в захисті, наприклад, відсутність правил, які могли б виявити внутрішні загрози чи нетипову поведінку легітимних користувачів.

Після цього виконується аудит джерел подій — перевіряється, чи всі ключові системи належним чином інтегровані з SIEM-рішенням, і чи коректно передаються логи з серверів, робочих станцій, міжмережевих екранів, систем виявлення вторгнень (IDS/IPS) та антивірусного ПЗ.

Завершальним етапом є оцінка відповідності чинних правил політикам безпеки. Це включає не лише відповідність внутрішнім регламентам підприємства, а й узгодженість із зовнішніми нормативними вимогами та галузевими стандартами, такими як ISO 27001, NIST чи PCI DSS. Такий системний підхід дозволяє підтримувати належний рівень кіберзахисту, знижуючи ризик як технічних, так і організаційних уразливостей.

4. Оптимізація правил

На основі аналізу уточнюються існуючі правила: додаються нові умови, часові рамки або винятки. Також створюються правила для виявлення нових загроз, встановлюється пріоритетність і категорії інцидентів (інформаційні, попереджувальні чи критичні).

5. Використання Threat Intelligence

Додавання зовнішніх джерел аналітики (IP reputation lists, indicators of compromise) підвищує ефективність виявлення актуальних загроз.

6. Тестування і моделювання

Проводяться імітації атак із використанням технік MITRE ATT&CK або практик Red Team/Blue Team для перевірки ефективності правил. Цей підхід забезпечує комплексний аналіз і оптимізацію SIEM-системи для максимальної ефективності у виявленні та запобіганні загрозам.

Elastic SIEM використовує так звані детектори загроз (Detection Rules). У процесі роботи було здійснено аналіз більш ніж 40 вбудованих правил та 10 кастомних.

Перед тим як перейти до конкретних правил, що використовуються на підприємстві, доцільно детальніше зупинитися на понятті KQL-запиту правила.

KQL-запит правила — це умова або набір умов, написаних мовою запитів KQL, яка використовується для виявлення подій безпеки в журналах або потоках даних у SIEM-системах. Завдяки KQL можна здійснювати фільтрацію, агрегацію, трансформацію та аналіз даних із журналів. У контексті правил аналітики (analytic rules) — це запити, які автоматично виконуються за визначеним розкладом, щоб ідентифікувати потенційні інциденти безпеки [19].

Далі в роботі розглянемо декілька прикладів правил, що використовуються на обраному підприємстві.

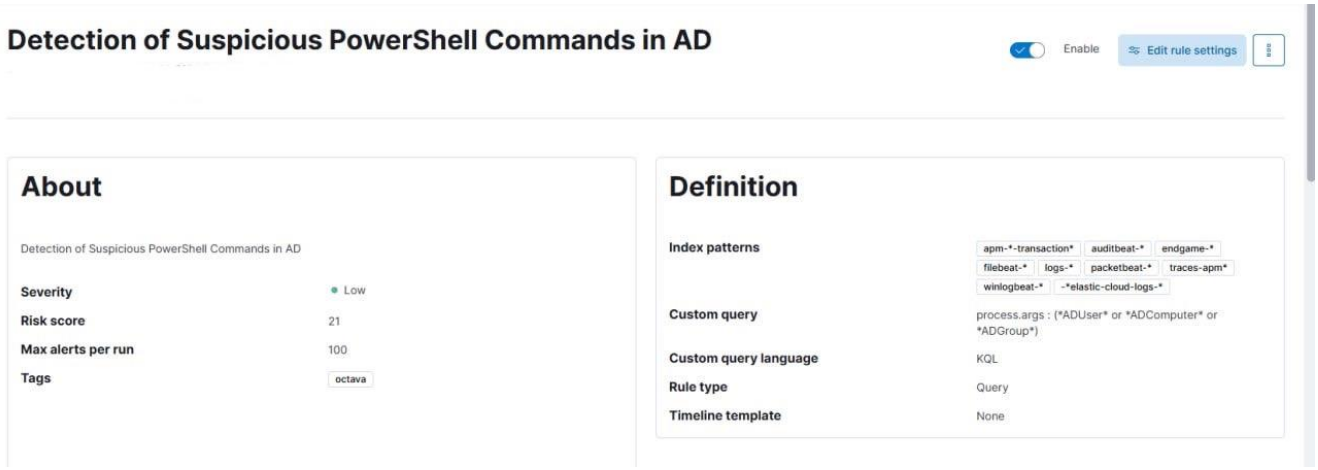

Рис.2.3. Виявлення підозрілих PowerShell-команд у середовищі Active Directory

KQL-запит правила: process. args: (*ADUser* or *ADComputer* or *ADGroup*)

Кореляційне правило спрямоване на ідентифікацію підозрілих PowerShell-команд у середовищі Active Directory має на меті ідентифікувати потенційно шкідливу або нетипову поведінку. Це правило зосереджується на тих випадках, коли PowerShell використовується для виконання дій, що можуть свідчити про спробу компрометації домену або горизонтального переміщення в межах мережі. PowerShell — це легітимний і дуже потужний інструмент адміністрування в Windows-середовищах, однак його універсальність робить його привабливим і для

зловмисників. Після початкового доступу до системи зловмисники часто застосовують PowerShell для збору інформації про домен, користувачів, групи, політики безпеки та для здійснення змін у середовищі AD.

У випадку виявлення такої активності, SIEM-система автоматично генерує попередження, яке може бути передане на ручну перевірку фахівцю з безпеки або автоматично передане до SOAR-платформи для відповідних заходів безпеки — наприклад, блокування облікового запису, завершення процесу PowerShell або ізоляції пристрою в мережі.

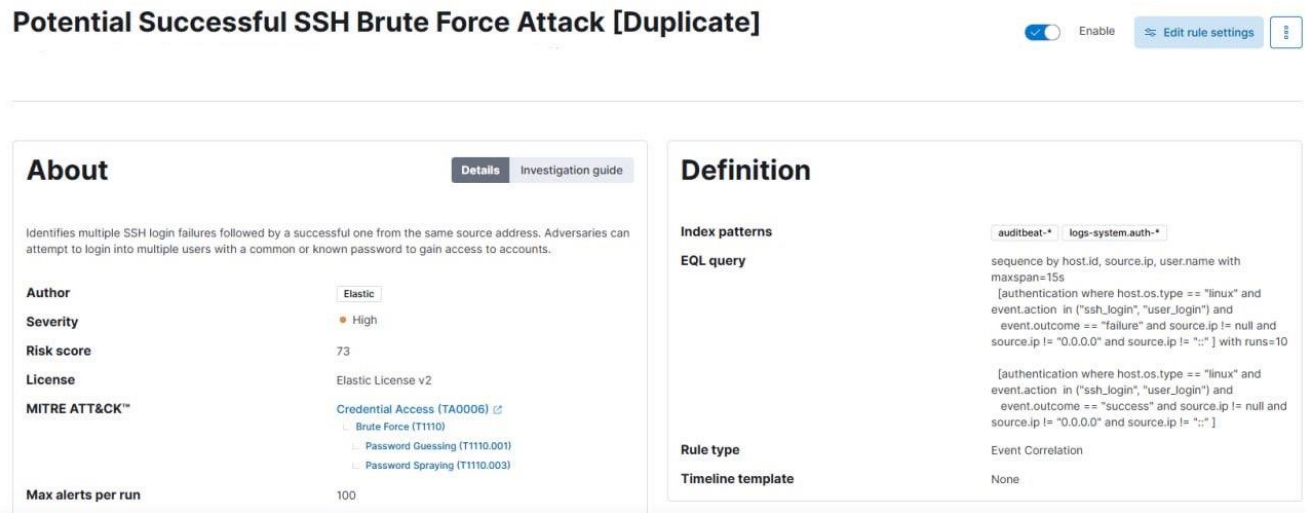

Рис.2.4. Вірогідність успішності атаки brute force через SSH

KQL-запит правила: sequence by host.id, source.ip, user.name with maxspan=15s

[authentication where host.os.type == "linux" and event.action in ("ssh_login", "user_login") and

event.outcome == "failure" and source.ip != null and source.ip != "0.0.0.0" and source.ip != "::"] with runs=10

[authentication where host.os.type == "linux" and event.action in ("ssh_login", "user_login") and

event.outcome == "success" and source.ip != null and source.ip != "0.0.0.0" and source.ip != "::"]

Кореляційне правило "Potential Successful SSH Brute Force Attack" (Можлива успішна атака brute force через SSH) створене для виявлення типового сценарію злому, коли зловмисник багаторазово намагається вгадати пароль до облікового запису через SSH-протокол. Основна ідея цього правила полягає в аналізі послідовності подій автентифікації, що надходять із системних логів, і виявленні випадків, коли велика кількість невдалих спроб входу змінюється раптовим успішним входом з тієї ж IP-адреси. Така поведінка є типовою ознакою brute force-атаки [22].

У наведеному прикладі правило фіксує ситуацію, коли протягом короткого проміжку часу (до 15 секунд) відбувається не менше 10 невдалих спроб входу на Linux-систему з одного джерела, після чого з того ж IP-адресу надходить подія успішної автентифікації. Цей ланцюг подій свідчить про те, що пароль до облікового запису міг бути підібраний автоматизованими засобами, наприклад, через словникову атаку. У разі спрацювання воно сигналізує про високий рівень загрози і дає змогу аналітикам швидко відреагувати: заблокувати доступ, перевірити активність користувача, ініціювати зміну пароля або навіть ізолювати відповідний хост у мережі.

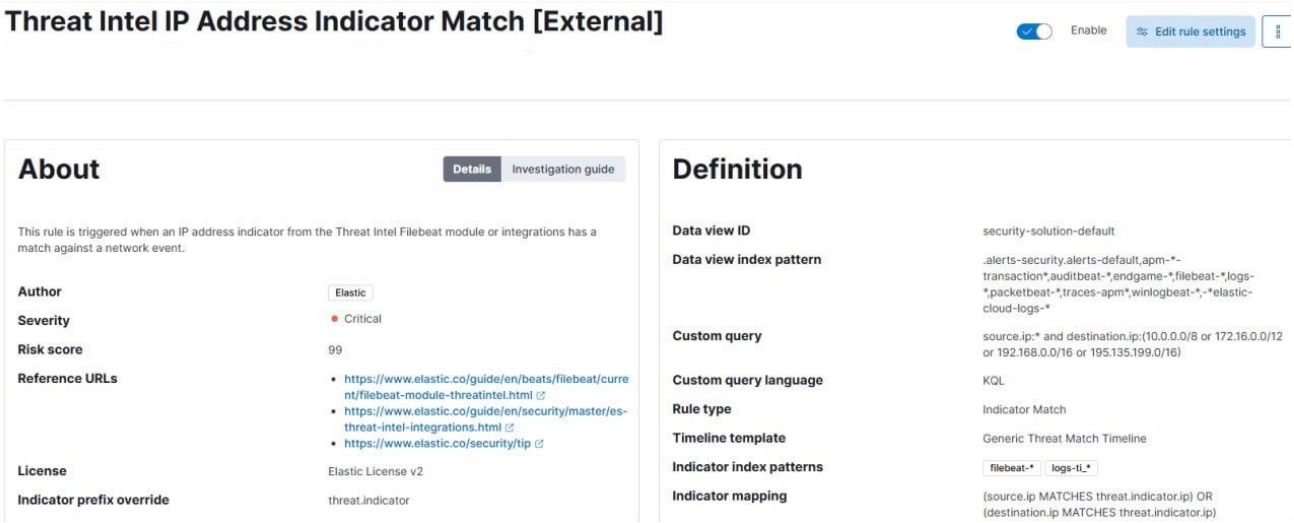

Рис.2.5. Виявлення мережевих конектів до сумнівних зовнішніх IP-адрес

KQL-запит правила: .alerts-security.alerts-default,apm-*-transaction*,auditbeat-*,endgame-*,filebeat-*,logs-*,packetbeat-*,traces-apm*,winlogbeat-*,-*elastic-cloud-logs-* -

Кореляційне правило "Threat Intel IP Address Indicator Match" спрямоване на виявлення зв’язків між активністю в мережі організації та відомими шкідливими IP-адресами, які містяться в зовнішніх або внутрішніх базах загроз. Його основна функція полягає в автоматичному порівнянні IP-адрес, які з’являються в логах трафіку або подіях безпеки, з переліками адрес, які асоціюються з відомими атаками, командно-контрольними серверами, ботнетами, сканерами або джерелами фішингу.

Таке правило активується, коли, наприклад, хост у мережі компанії надсилає запит до IP-адреси, яка згадується в базі threat intel як шкідлива. Це може означати, що пристрій був скомпрометований і намагається передати викрадені дані.

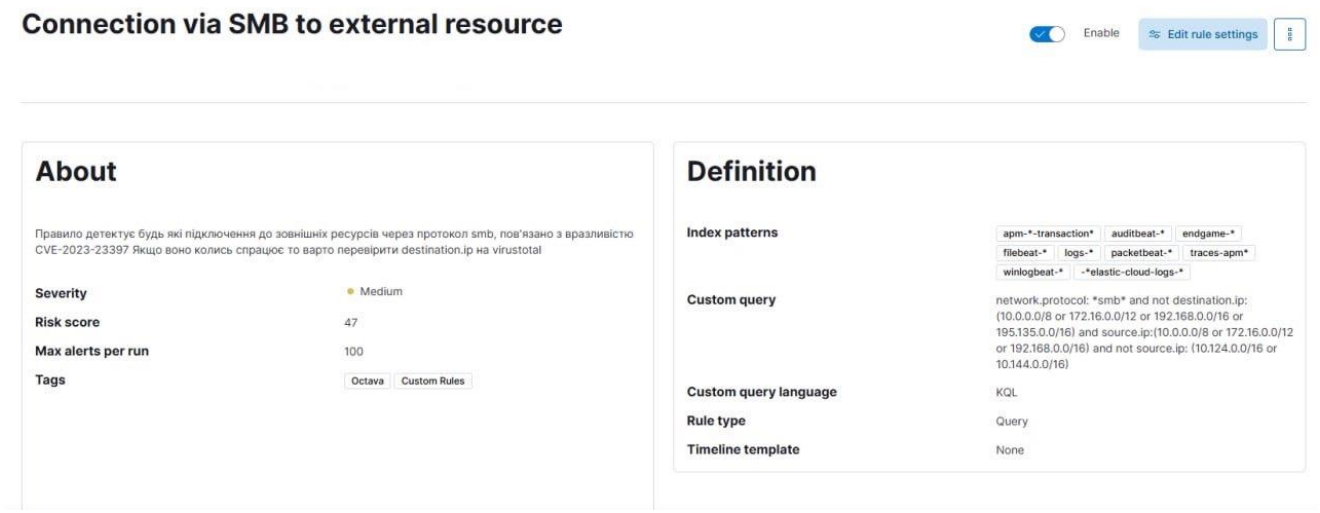

Рис.2.6. Детектування підключення до зовнішніх ресурсів через протокол smb, пов'язано з вразливістю CVE-2023-23397

KQL-запит правила: network.protocol: *smb* and not destination.ip:(10.0.0.0/8 or 172.16.0.0/12 or 192.168.0.0/16 or 195.135.0.0/16) and source.ip:(10.0.0.0/8 or 172.16.0.0/12 or 192.168.0.0/16) and not source.ip: (10.124.0.0/16 or 10.144.0.0/16)

Підключення через SMB до зовнішнього ресурсу - створено для виявлення потенційно небезпечної мережевої активності, коли внутрішній хост встановлює з’єднання з зовнішньою IP-адресою за допомогою протоколу SMB. Така поведінка вважається нетиповою для стандартної роботи корпоративної мережі й може свідчити про витік даних, спробу передачі шкідливого програмного забезпечення або використання вразливостей, як-от CVE-2023-23397.

Протокол SMB зазвичай використовується всередині організації для доступу до файлів, принтерів або спільних ресурсів у локальній мережі. Проте його використання за межами внутрішнього сегменту — тобто з підключенням до Інтернету — майже завжди є підозрілим. Особливо це актуально в контексті експлуатації відомих вразливостей, за допомогою яких зловмисники можуть отримати доступ до облікових даних або віддалено виконувати код на вразливих пристроях.

Це правило активується тоді, коли SIEM-система фіксує мережеву подію з протоколом smb, де IP-адреса призначення не належить до приватних підмереж (в даному випадку, 10.x.x.x, 172.16.x.x, 192.168.x.x). Таким чином, воно спрямоване саме на виявлення спроб підключення до зовнішніх SMB-ресурсів — таких, які фізично або логічно розміщені поза периметром організації.

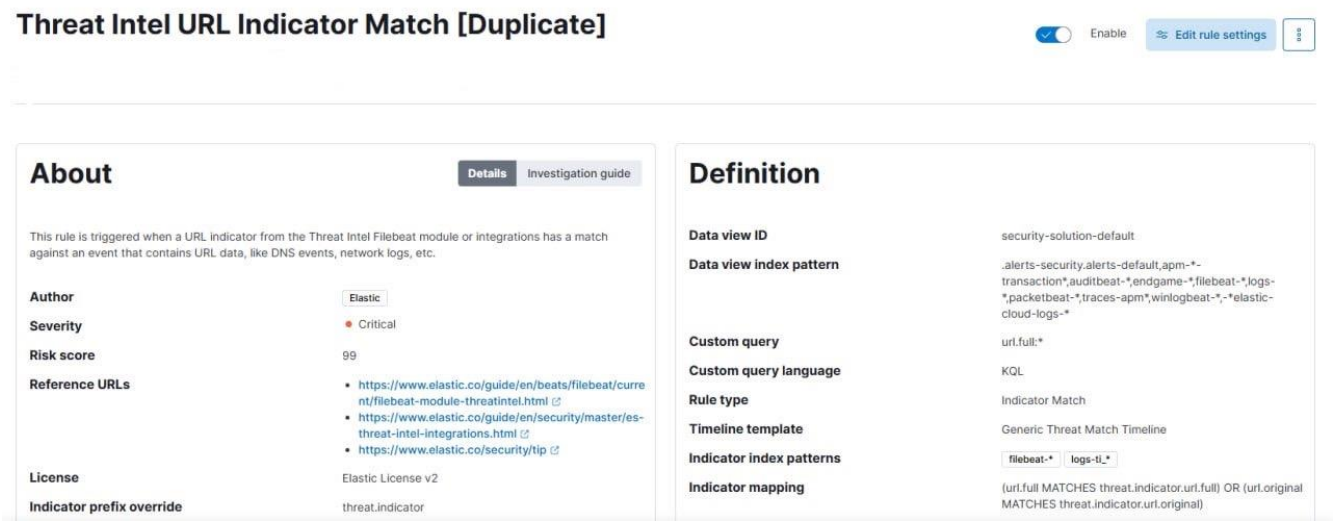

Рис.2.7. Виявлення взаємодії з сумнівними URL

KQL-запит правила: (url.full MATCHES threat.indicator.url.full) OR (url.original MATCHES threat.indicator.url.original)

Правило кореляції "Threat Intel URL Indicator Match" призначене для виявлення підозрілих або шкідливих дій у мережі, пов’язаних із доступом до URL-адрес, які вже відомі як індикатори компрометації згідно з розвідданими про загрози (threat intelligence). Це правило спрацьовує тоді, коли в логах подій з’являється звернення до веб-ресурсу, що збігається з URL, внесеним до бази даних потенційно шкідливих адрес. Такі бази постійно оновлюються аналітичними центрами, вендорами безпеки або самою організацією.

У типових сценаріях мова йде про випадки, коли користувач або внутрішній процес отримують доступ до підозрілої URL-адреси, що асоціюється із фішингом, командно-контрольними серверами (C2 - command and control), експлойтами або іншими типами зловмисної активності. Наприклад, працівник міг натиснути на посилання в листі-фейку, а браузер виконав HTTP-запит до домену, який вже фігурує у threat intelligence як такий, що використовувався в атаках [25,26].

Основна концепція правила полягає у порівнянні URL-адрес із репутаційною базою. Якщо збіг є, це сигналізує про потенційний інцидент безпеки. Завдяки такому механізму SIEM-система дає змогу оперативно виявити спроби звернення до відомих шкідливих ресурсів — ще до того, як ці дії призведуть до завантаження шкідливого ПЗ, передачі даних або запуску коду. У випадку спрацювання, відповідна подія може бути передана до системи автоматизованого реагування (SOAR), що, наприклад, блокує домен на проксі-сервері, або створює тикет для перевірки інциденту.

Таким чином, аналіз демонструє, що ключовим чинником ефективності SIEM-системи є якісно налаштовані та своєчасно оновлювані правила виявлення загроз. Їхня актуальність напряму впливає на здатність системи ідентифікувати як класичні, так і нові, складніші атаки. Важливу роль відіграє також адаптивність самої системи — її здатність динамічно інтегрувати зовнішні джерела аналітики, наприклад, бази threat intelligence, а також застосовувати сучасні підходи тестування, як-от імітація атак за методологією MITRE ATT&CK або Red

Team/Blue Team. Завдяки цьому SIEM може не лише фіксувати вже відомі загрози, але й ефективно виявляти нетипову, нову або цільову шкідливу активність. Такий підхід дозволяє підтримувати високий рівень безпеки в умовах постійної еволюції кіберзагроз.

2.2. Моніторинг ризиків безпеки інформації на підприємстві

Протягом семи днів був проведений моніторинг логів і подій безпеки на прикладі реального середовища з такими компонентами:

Filebeat: збір логів з Linux-серверів

Winlogbeat: журнали Windows Event Log

Auditbeat: системні події (відкриття файлів, зміни прав)

Packetbeat: мережеві запити

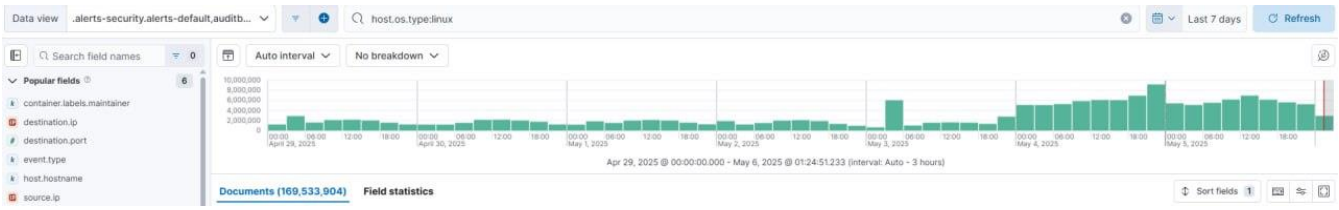

Рис.2.8. Об’єднання компонентів в одному discovery (сторінка пошуку подій)

В результаті системного моніторингу логів за 7 днів на хостах з операційною системою Linux було зафіксовано аномальні сплески активності.

Аналітичні дані вказують на те, що впродовж аналізованого періоду, зокрема 3 травня 2025 року близько 03:00 та 5 травня у вечірній час, спостерігалися різкі сплески кількості подій. Такі пікові навантаження, як правило, не є типовими для штатної роботи систем, що може свідчити про масові, можливо — автоматизовані дії, які потребують подальшого, більш глибокого аналізу.

Загальний обсяг оброблених даних за цей період сягнув 169 533 904 подій, що є суттєвим навантаженням навіть для масштабованих SIEM-рішень. Варто

зазначити, що до логів була застосована фільтрація, яка обмежила результати лише до подій з Linux-хостів (host.os.type: linux), що дозволило сфокусуватись саме на цій частині інфраструктури. Первинний пошук за параметром host.name показав наявність одного або кількох вузлів із явно перевищеним обсягом активності, що дозволяє припустити — активність мала централізований або сконцентрований характер.

Ситуація, що розглядається, містить низку потенційних ризиків, які можуть свідчити про загрозу безпеці інформаційної системи. Зокрема, масове завантаження або копіювання файлів із репозиторіїв може бути ознакою як легітимного внутрішнього резервного копіювання, так і несанкціонованого витоку конфіденційної інформації. Окрім цього, фіксується можлива автоматизована активність — запуск скриптів, ботів чи повторюваних завдань, які створюють надмірну кількість логів і можуть ускладнювати виявлення справжніх інцидентів безпеки. Також викликає занепокоєння підозріла мережева активність, зокрема звернення до невідомих або зовнішніх IP-адрес, що потребує глибокого аналізу з акцентом на параметри source.ip і destination.ip для з'ясування джерела та мети з'єднань.

Використовуючи Kibana SIEM UI, було виявлено ключові інциденти, що представлені в таблиці 2.1.

Таблиця 2.1.

Ключові інциденти на підприємстві за використання Kibana SIEM UI

Інцидент	**Джерело логів**	**Правило спрацювання**	**Кількість**
Підозрілий PowerShell-скрипт	Winlogbeat	Suspicious PowerShell	3
Брутфорс на SSH-сервер	Filebeat	SSH Brute Force	27
Запуск непідписаного EXE-файлу	Winlogbeat	Unsigned Executable Started	5

Продовження таблиці 2.1.

Інцидент	Джерело логів	Правило спрацювання	Кількість
Зміна прав на конфігураційний файл	Auditbeat	File Permission Changed	4
Зовнішнє підключення на порт 445	Packetbeat	SMB Traffic from External IP	6

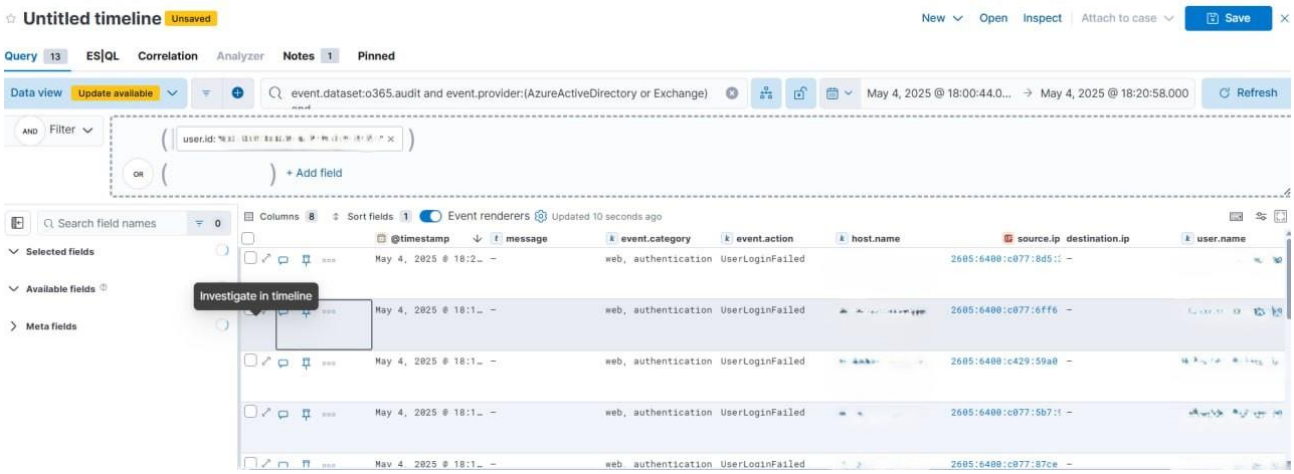

Рис.2.9. Потенційна атака brute force

На рисунку 2.9 показаний один з ключових інцидентів - потенційна атака brute force на підприємстві. Розглянемо даний інцидент більш детально.

Основним маркером є велика кількість подій типу *UserLoginFailed*, які фіксуються протягом короткого проміжку часу. Усі спроби спрямовані на одного й того самого користувача, що вказує на цілеспрямовану атаку. Особливої уваги заслуговує факт використання різних IPv6-адрес, що може свідчити про застосування проксі-сервісів, VPN або ботнет-інфраструктури для обходу захисту на основі IP-обмежень.

Таблиця 2.2.

Характерні ознаки атаки

Ознака	Інтерпретація
Повторювана помилка автентифікації	UserLoginFailed, типовий маркер перебору
Однакова user.id	Націлення на конкретного користувача
Різні IP-адреси	Обхід захисту за IP (поширено в розподілених brute-force атаках)
Висока частота подій	Якщо кілька спроб/хв — висока ймовірність атаки

Тобто серед характерних ознак атаки ми маємо наступне: повторювана автентифікаційна помилка (*UserLoginFailed*), фіксація одного і того ж *user.id,* чергування IP-адрес і висока частота подій — наприклад, кілька спроб на хвилину. Така поведінка є типовою для розподілених brute force-спроб, які спрямовані на злам одного конкретного облікового запису шляхом перебору можливих комбінацій пароля.

Разом із тим, для остаточного підтвердження факту атаки бракує деяких важливих даних. Зокрема, відсутність подій типу *UserLoginSuccessful* свідчить про те, що зловмиснику не вдалося пройти автентифікацію, що означає неуспішність атаки. Також необхідно проаналізувати геолокацію IP-адрес — IPv6-адреси можуть належати до легітимних мереж CDN (Content Delivery Network), VPN або навіть до вузлів TOR. Ще одним критичним аспектом є перевірка, чи атака була спрямована виключно на одного користувача, чи має місце ширша атака на кілька облікових записів, що дозволить точніше оцінити масштаб загрози.

Подія автоматично передається в модуль Cases в Kibana для подальшого розслідування.

Модуль "Cases" у Kibana — є частиною екосистеми Elastic Security**,** призначений для ведення, документування та спільного розслідування інцидентів

безпеки**.** В основному цей модуль допомагає користувачам створювати, керувати та відслідковувати справи (інциденти) в системі безпеки на основі даних, зібраних із різних джерел (наприклад, з логів, мережевого трафіку, антивірусів, IDS/IPS) [27].

Після виявлення потенційної атаки brute force система генерує сповіщення. Аналітик безпеки відкриває модуль *Cases*, створює новий кейс, додає спрацьоване сповіщення, залишає коментар із первинним аналізом, прикріплює логи з відповідного хоста і ставить тег brute-force. Далі кейс передається наступному рівню для поглибленої перевірки.

Моніторинг ризиків безпеки інформації є невід'ємною складовою частиною загальної стратегії управління інформаційною безпекою на підприємстві. Регулярне відстеження та оцінка ризиків дозволяє оперативно виявляти потенційні загрози, оцінювати їхній вплив на бізнес-процеси та приймати своєчасні управлінські рішення для мінімізації наслідків.

Забезпечення ефективного моніторингу вимагає інтеграції різних інструментів та методологій для збору, аналізу та оцінки даних, що стосуються безпеки інформаційних систем і ресурсів. Використання засобів автоматизації та аналізу допомагає оперативно виявляти зміну рівня ризиків, підвищуючи тим самим рівень захищеності підприємства.

Цей процес також дозволяє здійснювати постійний аудит політик безпеки, коригувати стратегії реагування на інциденти та удосконалювати заходи щодо запобігання витокам даних, збоїв у роботі систем чи інших негативних впливів. Тому моніторинг ризиків є критично важливим для підтримки стабільної та надійної роботи організації в умовах постійно змінюваного кіберсередовища.

2.3. Оцінка результатів моніторингу безпеки за попередньо налаштованими правилами роботи SIEM-системи

Проведений моніторинг активності та безпеки в середовищі Elastic SIEM підтвердив його високу ефективність як інструменту виявлення потенційних загроз у корпоративній інфраструктурі. Система швидко й чітко реагувала на підозрілі події, автоматично формуючи відповідні сповіщення для відповідальних осіб або команд реагування. Це дозволило скоротити час між виникненням потенційної загрози та її виявленням, а також покращити загальну динаміку реагування на інциденти.

Таблиця 2.3.

Оцінка ефективності SIEM

Інцидент	Параметр	Результат
Підозрілий PowerShell-скрипт	Середній час виявлення загрози	30–90 секунд
	False Positives	~14% (особливо на логах Windows)
	Coverage ключових зон	Висока, покриває мережу, файли, аудити
Брутфорс на SSH-сервер	Середній час виявлення загрози	від 10 секунд до кількох хвилин
	False Positives	10–30%
	Coverage ключових зон	Auditbeat, Filebeat з system модулем
Запуск непідписаного EXE-файлу	Середній час виявлення загрози	30 сек – 2 хв
	False Positives	10–30%
	Coverage ключових зон	Elastic Agent (Endpoint), Winlogbeat (Sysmon або 4688),Вбудовано у telemetry Endpoint, Event ID 1 (Sysmon)
Зміна прав на конфігураційний файл	Середній час виявлення загрози	1–3 хв
	False Positives	50–80%, Базове правило: дуже багато шуму)
	Coverage ключових зон	Auditbeat з audit.rules на chmod, chown, або Elastic Agent File Rule

Продовження таблиці 2.3.

Інцидент	Параметр	Результат
Зовнішнє підключення на порт 445	Середній час виявлення загрози	1–3 хв, при хорошій інтеграції мережевого моніторингу.
	False Positives	10–30%
	Coverage ключових зон	Packetbeat, Zeek, Suricata, Elastic Agent, ECS: source.ip, destination.port, geo.*

Ці показники демонструють, що система має гарний рівень чутливості до інцидентів і здатна ідентифікувати загрози на ранніх етапах їх реалізації

Завдяки модулю Kibana, який інтегрується з Elastic SIEM, було розгорнуто кілька аналітичних дашбордів (рис. 2.10., рис.2.11., рис.2.12). Вони дозволили візуально відображати події безпеки, розподілу за IP-адресами, користувачами, типами атак та часовими мітками. Це дало змогу не лише швидко оцінити загальну ситуацію з безпекою в організації, а й оперативно реагувати на аномалії або зміну шаблонів поведінки в мережі.

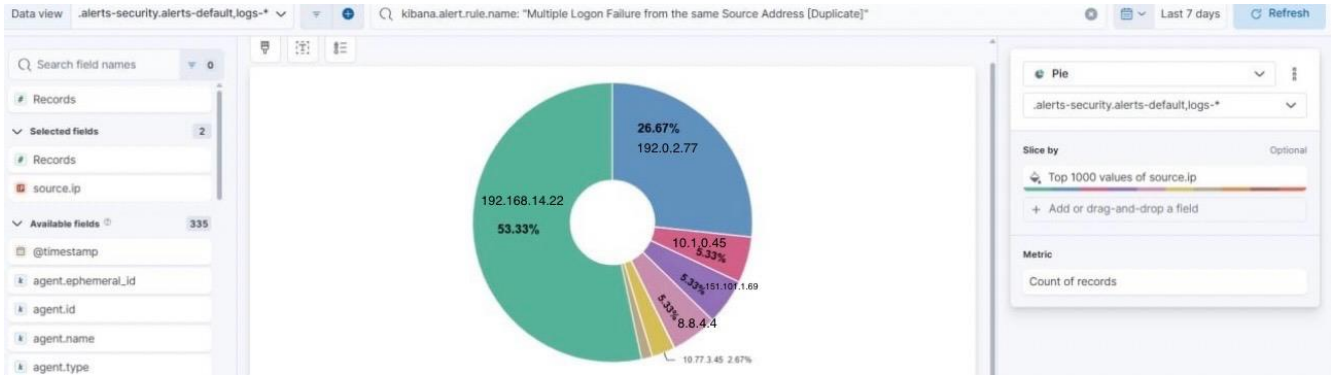

Рис.2.10. Топ IP-адрес з невдалими логінами

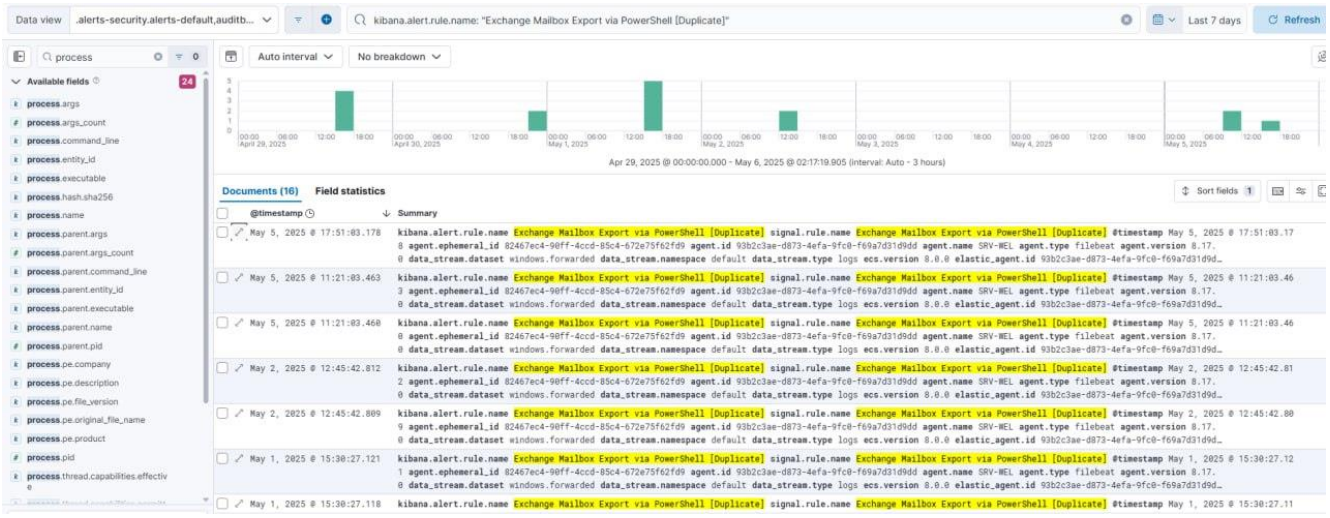

Рис.2.11. Частота запуску PowerShell за 7 днів

Рис.2.12. Частота запуску PowerShell за 30 днів

Аналіз показав, що система здатна швидко виявляти широкий спектр загроз — від запуску підозрілих PowerShell-скриптів до змін прав на конфігураційні файли та зовнішніх підключень до критичних портів. Середній час виявлення інцидентів варіюється від кількох секунд до кількох хвилин, залежно від типу події та джерел логів, , що є прийнятним показником для оперативного реагування.

Найшвидше система реагувала на brute force-атаки та запуск непідписаних виконуваних файлів, тоді як виявлення змін конфігурацій супроводжувалося високим рівнем хибнопозитивних спрацювань через обмеження базових правил.

Водночас результати моніторингу виявили і ряд недоліків, які потребують подальшого вдосконалення. Зокрема, фіксується доволі високий рівень хибнопозитивних спрацювань — від 10% до 30% для більшості правил, а в окремих випадках (наприклад, зміна прав доступу до конфігураційних файлів) цей показник сягає 50–80%. Це створює інформаційний “шум”, перевантажує аналітиків безпеки та знижує загальну ефективність реагування. Проблема значною мірою пов’язана з обмеженнями базових правил, які недостатньо контекстуалізують події та не враховують особливості звичної поведінки систем або користувачів.

Інтеграція з Kibana дозволила створити інформативні дашборди, що візуалізують розподіл подій за IP-адресами, користувачами, типами атак і часовими інтервалами. Це підвищило прозорість ситуації з безпекою в організації та дозволило оперативно виявляти аномалії або нові патерни поведінки в мережі.

Висновки до розділу 2

У результаті проведеного аналізу функціонування SIEM-системи в компанії Accord Group було підтверджено її ключову роль у забезпеченні проактивного захисту корпоративного середовища. Ефективність виявлення загроз значною мірою залежить від якісно налаштованих правил — як сигнатурних, поведінкових, і кореляційних. Це дозволяє ідентифікувати як стандартні атаки, так і нетипові види шкідливої активності. Завдяки використанню мови запитів KQL, система демонструє здатність фіксувати широкий спектр інцидентів — від brute force-атак до взаємодії з зовнішніми шкідливими IP чи URL. Проведений моніторинг показав, що система здатна реагувати на загрози від кількох секунд до кількох хвилин. Така оперативність суттєво підвищує ефективність реагування на критичні інциденти. Водночас аналіз засвідчив наявність певних обмежень, зокрема високого рівня хибнопозитивних спрацювань. Ця проблема вимагає додаткової оптимізації правил, а також подальшої адаптації до специфіки корпоративного середовища. Загалом Elastic SIEM демонструє здатність підтримувати високий рівень інформаційної безпеки в умовах зростаючих загроз.

Розділ 3 МОДЕЛЬ УПРАВЛІННЯ ІНЦИДЕНТАМИ БЕЗПЕКИ ЗА ВИКОРИСТАННЯ SIEM-СИСТЕМИ НА ОСНОВІ РИЗИК-СЦЕНАРІЇВ

3.1. Шляхи удосконалення рішень управління інцидентами безпеки з використанням SIEM-систем

У процесі аналізу роботи SIEM-системи Elastic в інформаційному середовищі підприємства було встановлено, що система повністю виконує ключові функції — виявлення та класифікація інцидентів, централізований збір логів, передача сповіщень і побудова аналітичних візуалізацій за допомогою Kibana. Значною перевагою є підтримка адаптивної логіки кореляційних правил, інтеграція з джерелами загроз, а також використання модулів візуалізації та ефективне використання кейс-менеджменту для документування інцидентів.

Втім, практика показала, що система потребує постійного вдосконалення. Актуальність правил, їх точність і здатність знижувати рівень хибнопозитивних спрацювань є критичними факторами, що визначають загальну ефективність захисту. Проведений моніторинг виявив проблему надмірної генерації сповіщень на деякі події, що знижує продуктивність аналітиків SOC — зокрема, у випадку змін конфігураційних файлів рівень false positives сягав 50–80%.

Разом із цим, виявлено кілька напрямків, які мають потенціал для подальшого підвищення рівня зрілості SIEM-рішення на підприємстві. До них належать як технічні вдосконалення, так і організаційні підходи.

Таблиця 3.1.

Шляхи вдосконалення SIEM-рішення та очікувані результати

Напрям удосконалення	Опис	Очікуваний результат
Розширення правил виявлення нетипового RDP-доступу	Впровадження логіки виявлення підозрілих RDP-сесій (нічний час, інші країни, незвичні IP)	Виявлення потенційного компрометованого доступу

Продовження таблиці 3.1.

Напрям удосконалення	Опис	Очікуваний результат
Інтеграція з SOAR-системами	Налаштування автоматизованих сценаріїв реагування	Налаштування автоматизованих сценаріїв реагування
Обмеження доступу до SIEM через VPN або Zero Trust	Доступ до системи лише через захищені канали, з обов'язковою аутентифікацією	Підвищення безпеки самої SIEM-системи
Elastic Actions (автоматизоване реагування)	Реалізація відповідей на інциденти: блокування IP, створення кейсів, оповіщення	Прискорення реакцій та зменшення втручання людини в стандартних сценаріях
Оптимізація кореляційних правил і виключень	Уточнення умов спрацювання, додавання виключень, врахування контексту користувача	Зниження рівня хибнопозитивних спрацювань, покращення релевантності інцидентів

Розглянемо кожен напрям більш детально.

Розширення правил детекції нетипового використання RDP.

Оскільки RDP є поширеним вектором атак, доцільно додати спеціалізовані правила, які будуть фіксувати спроби аномального або підозрілого використання цього протоколу — наприклад, RDP-сесії за межами робочого часу, з нетипових геолокацій або з IP-адрес, що не належать до корпоративної мережі. Такі правила можуть доповнювати інші сценарії, що базуються на поведінковому аналізі.

Інтеграція SIEM із системами автоматизованого реагування (SOAR).

Попри те, що SIEM дозволяє виявляти широкий спектр загроз, фактичне реагування часто виконується вручну, що уповільнює процес нейтралізації. Впровадження інтеграції з SOAR-платформами дозволить автоматизувати рутинні дії — наприклад, блокування шкідливого трафіку, закриття портів, або відправку запитів на ізоляцію скомпрометованих вузлів. Це суттєво скорочує "вікно вразливості" (time to respond) і знижує навантаження на фахівців [28, 29].

Обмеження доступу до SIEM через VPN або інші захищені канали.

В умовах гібридного доступу, коли адміністрування SIEM може відбуватись віддалено, Рекомендовано реалізувати обмеження, які дозволяють адміністративний доступ лише через захищені канали зв’язку, з багатофакторною аутентифікацією та геообмеженням. Це мінімізує ризик несанкціонованого доступу до аналітичної платформи.

Автоматизовані дії реагування через Elastic Actions.

Elastic SIEM підтримує функцію Elastic Actions, яка дозволяє налаштовувати сценарії автоматичної реакції на інциденти — наприклад, блокування зловмисного IP через брандмауер, надсилання повідомлень у Slack або Microsoft Teams, створення кейсу в модулі *Cases* або тикету в Jira. Впровадження такого підходу зробить систему не лише детектором загроз, а й активним учасником у протидії їм.

Таким чином, шлях удосконалення управління інцидентами безпеки через SIEM передбачає поєднання аналітичної глибини, технічної автоматизації та стратегічного управління ризиками. Це дозволить створити більш адаптивну, стійку та саморегульовану модель інформаційної безпеки.

3.2. План реагування на інциденти на основі ризик-сценаріїв

У контексті зростаючої складності кіберзагроз, збільшення поверхні атаки внаслідок цифрової трансформації та гібридного доступу до систем, традиційні підходи до реагування на інциденти часто виявляються неефективними. Це створює об'єктивну необхідність формування чіткого, структурованого плану реагування, побудованого з урахуванням ймовірних сценаріїв ризиків. Такий підхід дозволяє не тільки швидко реагувати на події, але й діяти проактивно, мінімізуючи наслідки загроз. План реагування на основі ризик-сценаріїв передбачає поетапне виявлення, аналіз, класифікацію та усунення інцидентів безпеки з урахуванням потенційного збитку, рівня критичності активів, а також специфіки IT-інфраструктури підприємства.

У контексті використання SIEM-системи Elastic Security план реагування базується на поєднанні аналітичної моделі загроз, попередньо створених

кореляційних правил, і сценаріїв реагування, визначених згідно з критичністю активів та потенційними наслідками.

Таблиця 3.2.

Етапи реалізації плану реагування на інциденти на основі ризик-сценаріїв

Етап реагування	Опис	Приклад реалізації
Ідентифікація ризик-сценаріїв	Визначення типових загрозових шаблонів, характерних для організації	Brute-force по SSH, звернення до шкідливих URL, підозрілий доступ до SMB
Класифікація інцидентів за рівнем ризику	Присвоєння інциденту рівня критичності (низький, середній, високий, критичний)	Аномальна активність адміністратора — високий рівень
Призначення відповідальних осіб	Визначення команди або фахівця, відповідального за реагування	Аналітик SOC 2-го рівня або DevSecOps
Реалізація реагування	Застосування відповідних дій залежно від типу інциденту	Блокування IP, створення кейсу, сповіщення через Slack
Документування інциденту	Фіксація всіх дій і результатів у модулі *Cases*	Додавання логів, нотаток, результатів аудиту
Післяінцидентний аналіз	Аналіз ефективності реагування, оцінка часу відповіді, уточнення логіки правил	Перегляд кореляційного правила “Brute Force + Success”, додавання винятків

Розглянемо етапи плану реагування на основі ризик-сценаріїв.

На першому етапі формується перелік потенційно небезпечних сценаріїв, які можуть бути актуальними саме для конкретної організації. Такі сценарії базуються на реальних інцидентах, аналітиці загроз (threat intelligence) та історичних логах. Наприклад, спроба підбору паролів через SSH (brute force), аномальна активність облікового запису в позаробочий час, підключення до зовнішнього SMB-ресурсу, звернення до URL, що фігурує у threat intelligence feeds [30].

На наступному етапі відбувається класифікація інцидентів за рівнем ризику. Виявлені інциденти ранжуються за рівнем критичності: від низького до

критичного. Для цього враховуються такі параметри, як тип і джерело загрози, контекст активності (користувач, хост, час, тривалість), важливість залучених ресурсів (сервер, база даних, контролер домену тощо) [30,31].

Це дає змогу визначати, які сценарії потребують миттєвого втручання, а які — лише моніторингу або періодичної перевірки.

На етапі призначення відповідальних осіб або груп реагування визначається, хто саме відповідатиме за реагування на інциденти певного рівня: SOC-аналітики 1–2 рівня, DevSecOps-команда, керівник IT-відділу або зовнішній підрядник. Важливою умовою є наявність чітко прописаних ролей і процедур ескалації.

В залежності від типу інциденту, можуть бути застосовані наступні дії (відбувається реалізація сценаріїв реагування):

- автоматичне блокування IP-адреси за допомогою Elastic Actions;
- створення кейсу у модулі *Cases* і прив'язка відповідних логів;
- завершення процесу або ізоляція хосту через інтегровані інструменти;
- оповіщення зацікавлених сторін через e-mail, Slack, Microsoft Teams або систему тикетів (наприклад, Jira).

Усі етапи повинні бути чітко зафіксовані в системі — хто виявив, які дії були вжиті, коли та з яким результатом. Тому наступним етапом є аналіз та документування інциденту. Модуль *Cases* у Kibana дозволяє вести повне документування з додаванням нотаток, логів, доказів та історії рішень. Це забезпечує прозорість і аудитність, а також спрощує аналіз повторних випадків [29].

Рис.3.1. Компоненти зворотного аналізу

Після завершення роботи над інцидентом проводиться зворотний аналіз, який включає оцінку часу реагування, перевірку ефективності застосованих дій, перегляд відповідних кореляційних правил, актуалізацію сценарію або доповнення винятків. Цей цикл дозволяє постійно вдосконалювати систему безпеки.

Один із типових ризик-сценаріїв, що реалізується в SIEM-системі, передбачає фіксацію потенційної brute force-атаки. Зокрема, після серії невдалих спроб входу з однієї IP-адреси система реєструє раптово успішну авторизацію, що свідчить про ймовірне підбирання пароля. У цьому випадку автоматично спрацьовує правило “Brute Force + Success”, після чого в системі створюється кейс, а відповідальній особі (SOC-аналітику) надходить сповіщення через інтерфейс Kibana. Завдяки інтеграції з Elastic Actions запускається автоматичне реагування: IP-адреса блокується, а підозрілий обліковий запис тимчасово деактивується. Після цього SOC-аналітик ініціює ретельний аудит активності, пов’язаної з компрометованим входом, зокрема аналізує команди, які виконувалися через SSH, щоб виявити потенційно шкідливі або нетипові дії користувача [32-34].

Таким чином, впровадження плану реагування, заснованого на ризик-сценаріях, дозволяє організації перейти від спонтанного або запізнілого реагування до контрольованої, проактивної моделі кіберзахисту. Такий підхід забезпечує не лише технічну ефективність, а й відповідність сучасним вимогам стандартів безпеки (ISO 27001, NIST), покращує документацію та підвищує рівень загальної кіберстійкості підприємства в довгостроковій перспективі.

3.3. Побудова моделі управління інцидентами за використання SIEM-системи на основі ризик-сценаріїв

Ефективне управління інцидентами інформаційної безпеки потребує системного підходу, що поєднує як технологічні інструменти, так і організаційні механізми реагування. Одним із найефективніших підходів до цього завдання є побудова моделі управління інцидентами на основі ризик-сценаріїв, реалізованої за допомогою можливостей SIEM-системи, зокрема Elastic Security.

Така модель дозволяє систематизувати процеси моніторингу, аналізу, реагування та документування інцидентів, при цьому враховуючи специфіку конкретних загроз, пріоритетність активів та поведінкові особливості інформаційного середовища організації.

Рис.3.2. Модель управління інцидентами

Модель побудована на взаємопов’язаних структурних компонентах, які забезпечують її ефективність, гнучкість і здатність до самонавчання.

Основу становить сценарна база ризиків, що включає найбільш імовірні технічні та поведінкові загрози — від атак через SSH до аномальної активності користувачів і нетипового доступу до критичних ресурсів. Ці сценарії формуються на основі аналізу інцидентів, зовнішніх джерел threat intelligence та індивідуального профілю ризику підприємства.

У випадку компанії Accord Group, яка активно використовує SIEM-систему Elastic для збору та аналізу подій безпеки, можна виокремити п’ять ключових сценаріїв, які складають основу ризик-бази.

Таблиця 3.3.

Ризик-сценарії за ймовірними технічними та поведінковими загрозами для підприємства

Ризик-сценарій	Ймовірність	Потенційний вплив	Тип загрози
Масовий підбір паролів (SSH brute force)	Висока	Ескалація прав, розгортання backdoor	Технічна
Несанкціоноване адміністрування через PowerShell	Середня	Доменно-локальна ескалація	Технічна/внутрішня
Зовнішні SMB-з'єднання (CVE-2023-23397)	Низька	Витік даних	Технічна/вразливість
Запуск непідписаних EXE-файлів	Середня	Впровадження malware	Технічна
Звернення до фішингових URL	Висока	Витік облікових даних	Поведінкова

Масовий підбір паролів (SSH brute force) — один із найкласичніших сценаріїв. Зловмисники автоматизовано намагаються підібрати логіни й паролі, надсилаючи десятки або сотні запитів входу за дуже короткий час. У логах це виглядає як серія невдалих спроб автентифікації з тієї ж IP-адреси або з цілого пулу (наприклад, через VPN або ботнет). Якщо спроби успішні - сервер швидко стає точкою входу в мережу [35].

Використання PowerShell для втручання в Active Directory.

PowerShell —інструмент адміністрування, який водночас є улюбленим засобом атак для хакерів. Після отримання доступу до будь-якого внутрішнього пристрою зловмисник запускає команди PowerShell для збору інформації про домен: користувачів, групи, політики. Іноді це йде далі — створюються нові

облікові записи, змінюються групи доступу або розгортається шкідливий скрипт. Такі дії складно виявити без поведінкового аналізу.

Підключення до зовнішніх IP-адрес через SMB.

Протокол SMB зазвичай працює виключно всередині корпоративної мережі: для обміну файлами, доступу до спільних ресурсів тощо. Але коли фіксується спроба з'єднання із зовнішньою IP-адресою через SMB , то така активність може вказувати на спробу витоку даних або на те, що систему вже скомпрометували й використовують для передачі інформації назовні. У деяких випадках мова може йти про експлуатацію відомих вразливостей (наприклад, CVE-2023-23397).

Запуск непідписаного виконуваного файлу (EXE).

Непідписані EXE-файли - типовий індикатор шкідливого програмного забезпечення. Найчастіше їх завантажують через електронну пошту (фішингові листи з вкладеннями) або через шкідливі скрипти. У корпоративному середовищі будь-яке виконання такого файлу на кінцевій точці повинно викликати підозру. Це може бути або перший етап атаки, або вже частина розгорнутого зловмисного ланцюжка.

Звернення до відомих шкідливих доменів або URL-адрес.

Завдяки інтеграції з базами threat intelligence (зокрема IOC — indicators of compromise), SIEM-система здатна виявити факти звернення користувачів або процесів до вже відомих шкідливих доменів. Це можуть бути C2-сервери, фішингові ресурси, сайти, що поширюють malware, або URL-адреси, які вже були зафіксовані як частина попередніх атак. У багатьох випадках це перший крок до зараження системи — клієнт натискає фішингове посилання, після чого завантажується експлойт або бекдор [37].

Кожен сценарій, що міститься в ризик-базі, повинен мати відповідне логічне представлення у вигляді кореляційного правила. Його завдання — у реальному часі виявити відповідний ланцюг подій у логах і сповістити аналітика про потенційний інцидент. Кожне таке правило - це логічна конструкція, яка перевіряє задану умову або послідовність умов. Нижче наведено відповідність між сценарієм та логікою його виявлення в Elastic SIEM.

Таблиця 3.4.

Логіка кореляції ключових сценаріїв підприємства

Назва сценарію	KQL / логіка кореляції (Elastic SIEM)
SSH Brute Force	sequence by host.id, source.ip with maxspan=20s [authentication where host.os.type == "linux" and event.outcome == "failure" and event.action in ("ssh_login","user_login") and source.ip != "0.0.0.0"] with runs=8 [authentication where host.os.type == "linux" and event.outcome == "success" and event.action in ("ssh_login","user_login")]
PowerShell в AD	process where process.name : "powershell.exe" and process.args : ("*Get-ADUser*","*Get-ADComputer*","*Get-ADGroup*") and not user.domain : "IT-ADMIN-SVC"
Unsigned Executable	file where event.action == "creation" and file.extension : ("exe","dll") and not file.code_signature.exists and source.ip in private_ip_ranges() and not destination.ip in private_ip_ranges()
З'єднання з шкідливими IP	destination.ip : * AND destination.ip MATCHES threat.indicator.ip
Зовнішні SMB-з’єднання	network where network.protocol == "smb" and source.ip in private_ip_ranges() and not destination.ip in private_ip_ranges() and not destination.ip in approved_smb_whitelist
Фішингові URL	(url.full : threat.indicator.url.full or url.original : threat.indicator.url.original) and event.category == "network"

У рамках роботи SIEM-системи одним із ключових завдань є виявлення підозрілої активності, яка потенційно свідчить про спробу компрометації мережі або її окремих компонентів. Саме тому правило, що стосується підбору паролів через SSH , перевіряє, чи не надходить багато невдалих спроб входу на сервер протягом короткого часу, а потім — раптово успішна. Така картина часто вказує на те, що пароль було підібрано [39].

Інший характерний сценарій - запуск PowerShell-команд, пов’язаних із об'єктами Active Directory. У випадку, якщо на машині запускається PowerShell зі

згадками типу ADUser, ADGroup тощо - SIEM вважає це підозрілою активністю, оскільки вона пов’язана з управлінням обліковими записами домену.

Ще одним важливим тригером є виявлення SMB-з’єднань із зовнішніми IP-адресами Якщо з внутрішнього хосту відбувається вихід на зовнішню IP-адресу за протоколом SMB, спрацьовує правило. У нормальному сценарії така комунікація мала би бути забороненою.

Крім того, SIEM активно реагує на запуск виконуваних файлів без цифрового підпису. Правило перевіряє, чи запускається файл із розширенням .exe, який не має підпису або має статус Unsigned (вияв типової поведінки для вірусів або інструментів, завантажених поза офіційними каналами).

Система також фіксує звернення до відомих шкідливих веб-ресурсів. Коли в логах фіксується звернення до URL або IP-адреси, яка позначена як шкідлива в аналітиці загроз, правило активується автоматично. Це може бути ознакою фішингової атаки або зв'язку з C2-сервером [37].

Наприклад, якщо визначено сценарій "успішне підключення після серії невдалих спроб входу", правило буде шукати саме таку послідовність подій у логах і активувати попередження. Перевагою Elastic SIEM є можливість гнучко адаптувати правила: налаштовувати фільтри, виключення, часові рамки, порогові значення. Це дає змогу постійно вдосконалювати точність виявлення та зменшувати рівень false positives.

У разі високої довіри до певного сценарію до справи вступають механізми автоматизованого реагування. Зокрема, за допомогою Elastic Actions можуть бути автоматично ініційовані дії, такі як блокування IP-адреси, деактивація облікового запису, створення кейсу або надсилання сповіщення відповідальним особам або командам. Це значно скорочує час реагування та знижує ризик поширення атаки.

Усі виявлені інциденти фіксуються в модулі Cases, де ведеться структуроване документування — хронологія дій, коментарі аналітиків, відповідні логи та рішення. Це формує єдину базу знань про інциденти в організації, що також важливо для аудиту, звітності та повторного використання досвіду.

Таблиця 3.5.

Виявлені інциденти на підприємстві

ID інциденту	Назва	Дата / Час	Тип	Джерело	Критичність	Коментар аналітика	Вжиті дії	Посилання на лог
CASE-2025-001	SSH Brute Force	03.05.2025 03:10	Технічна	Filebeat (auth.log)	Висока	Масовані спроби входу з IP 2a01:...	IP заблоковано, пароль змінено	[log-001]
CASE-2025-002	PowerShell у AD	03.05.2025 05:33	Внутрішня	Winlogbeat	Середня	Незвичні запити AD через PowerShell	Запит скрипту, обліковий запис перевірено	[log-002]
CASE-2025-003	EXE без підпису	04.05.2025 09:00	Технічна	Endpoint, Winlogbeat	Середня	Виявлено запуск невідомого exe	Перевірка SHA256, карантин	[log-003]
CASE-2025-004	SMB назовні	05.05.2025 20:22	Вразливість	Packetbeat	Висока	Підключення до зовн. SMB	IP заблоковано, кейс передано на SOC	[log-004]
CASE-2025-005	URL фішинг	06.05.2025 11:45	Поведінкова	Filebeat (proxy)	Висока	Відкрито URL з IOC бази	Домен заблоковано на проксі	[log-005]

Завершальним компонентом є зворотній цикл навчання. Після закриття кожного кейсу проводиться оцінка точності спрацювання правила, ефективності автоматизованого реагування та аналіз потенційних хибнопозитивних або пропущених спрацювань.

На основі цих висновків оновлюються умови кореляції, вносяться корективи до сценаріїв, створюються нові виключення або додаються додаткові індикатори. Таким чином, система постійно адаптується до нових реалій та загроз.

У підсумку, побудова такої моделі управління інцидентами на основі ризик-сценаріїв із використанням можливостей Elastic SIEM дозволяє перейти від фрагментарного реагування на події до структурованого та стратегічного

управління інцидентами, в основі якого лежить контекстуалізований підхід до ризиків. Завдяки поєднанню автоматизації, сценарного аналізу, візуалізації подій і адаптивної логіки, організація отримує інструмент, здатний не лише виявляти інциденти, а й активно протидіяти їм на ранніх етапах розвитку. Це створює передумови для підвищення загального рівня кіберстійкості і формує основу для впровадження принципів безпеки, орієнтованих на ризик.

Висновок до розділу 3

У межах дослідження було розроблено комплексну модель управління інцидентами інформаційної безпеки на основі ризик-сценаріїв із використанням SIEM-системи Elastic. Цей підхід продемонстрував високу ефективність у виявленні та нейтралізації загроз завдяки поєднанню аналітичних інструментів, автоматизації, сценарного планування та організаційних механізмів реагування. Впровадження кореляційних правил, інтеграція з SOAR-системами, використання Elastic Actions і побудова ризик-орієнтованих сценаріїв дозволяють значно скоротити час реагування, зменшити навантаження на аналітиків SOC і забезпечити більш точне виявлення загроз.

ВИСНОВКИ

У межах проведеного дослідження було охарактеризовано принципи функціонування, типи та особливості використання SIEM-систем в управлінні інцидентами інформаційної безпеки. Досліджено архітектуру та функціональні можливості різних типів SIEM-систем. Визначено, що кожен тип має свої переваги та обмеження, а оптимальність вибору залежить від конкретних потреб і характеристик інфраструктури підприємства.

На основі аналізу актуальних наукових джерел та практичного досвіду впровадження таких рішень у компанії Accord Group встановлено, що SIEM-технології є ефективним засобом для централізованого збору, кореляції та аналізу подій безпеки в реальному часі. Однак продемонстровано, що навіть добре налаштований стек правил потребує регулярного аудиту. Аналіз засвідчив, що найчастіше хибнопозитивні спрацювання провокують універсальні сигнатурні правила, тоді як поведінкові, побудовані на KQL-запитах, у поєднанні з джерелами Threat Intelligence забезпечують точнішу детекцію реальних атак. Виявлені прогалини демонструють, що стандартні правила були прописані недостатньо чітко, є недосконалими, тому спричиняли значну кількість хибнопозитивних спрацювань. В свою чергу така ситуація призводила до перевантаження команди моніторингу й іноді відволікало її від своєчасної обробки істинно позитивних інцидентів. З метою розв’язання даної проблеми, було проаналізовано організаційну базу знань про кіберінциденти, розроблено модель реагування на основі ризик-сценаріїв та, скориставшись функціоналом Elastic SIEM, вдосконалено кореляційні правила. За результатами дослідження доведено, що систематичний аудит та адаптивне налаштування правил є обов’язковою передумовою ефективної експлуатації SIEM.

За результатами дослідження запропоновно модель, що побудована на взаємопов’язаних структурних компонентах, які забезпечують її ефективність, гнучкість і здатність до самонавчання, підгрунтям якої слугує сценарна база ризиків, що включає найбільш імовірні технічні та поведінкові загрози.

Результати можуть бути впроваджені в корпоративних SOC для мінімізації навантаження на аналітиків за рахунок зниження шуму, прискорення розслідування інцидентів завдяки збагаченому контексту та удосконаленню роботи щодо відсілдкування та упередження інцидентів за рахунок ідентифікованих ризик-сценаріїв на підприємстві. Робота має преспективу для подальших досліджень - зосередження на впровадженні методів прогнозування та розширення автоматичних дій у відповідь на загрози, що надасть змогу підвищити рівень захисту важливих даних і систем підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements. Geneva: ISO, 2022. 44 p.

2. ISO/IEC 27035-1:2023 Information technology — Information security incident management — Part 1: Principles of incident management. Geneva: ISO, 2023. 26 p.

3. NIST. Framework for Improving Critical Infrastructure Cybersecurity. Version 2.0. Gaithersburg: National Institute of Standards and Technology, 2024. 94 p.

4. NIST Special Publication 800-61 Rev.3. Computer Security Incident Handling Guide. Gaithersburg: NIST, 2023. 120 p.

5. Guidelines on Cybersecurity, Data Protection and Privacy for SIEM Implementations. European Union Agency for Cybersecurity (ENISA). Athens, 2023. 88 p.

6. PCI Security Standards Council. PCI DSS v4.0. Requirements and Security Assessment Procedures. Wakefield, 2022. 360 p.

7. GDPR. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Official Journal of the EU. 2016. L 119. p. 1–88.

8. HIPAA Security Rule. 45 CFR Parts 160, 162, 164. Washington, DC: U.S. Government Publishing Office, 2023.

9. Stallings W. Effective Cybersecurity: A Guide to Using Best Practices and Standards. 2nd ed. Boston: Addison-Wesley, 2023. 608 p.

10. Chuvakin A., Borisov I. Security Information and Event Management (SIEM) Implementation. 2nd ed. Amsterdam: Elsevier, 2022. 412 p.

11. Scarfone K., Kent K. Guide to Intrusion Detection and Prevention Systems (IDPS). NIST SP 800-94 Rev.2. Gaithersburg: NIST, 2023. 134 p.

12. Sangster B., Brookes A. Cyber Attack Incident Response: A Rigorous Approach. London: BCS Learning & Development, 2022. 268 p.

13. Bejtlich R. The Practice of Network Security Monitoring. Boston: No Starch Press, 2024. 376 p.

14. Souppaya M., Scarfone K. Guide to Security Log Management. NIST SP 800-92 Rev.1. Gaithersburg: NIST, 2024. 116 p.

15. Fontaine J., Zangana V. Implementing UEBA in Modern SIEM Platforms. Journal of Cybersecurity, 2023, Vol. 9, № 2, p. 41-57.

16. Kraemer-Mueller F. SOAR Orchestration Patterns for Automated Incident Response. Information & Software Technology, 2024, Vol. 158, 104 p.

17. Bărcanescu E. Elastic SIEM Threat Detection Rules: Efficiency Assessment. IEEE Access, 2023, Vol. 11, p.453-467.

18. Moustafa N., Slay J. The Evolution of SIEM toward XDR Platforms. Computers & Security, 2024, Vol. 127, № 1, p. 102-109.

19. Мідляновський Р. В. SIEM-системи: методи кореляції подій для виявлення аномалій. Вісник НТУУ “КПІ” Інформатика, управління та обчислювальна техніка, 2023, № 70, с. 58-65.

20. Омельченко І. Б. Порівняльний аналіз відкритих SIEM-рішень ELK та Wazuh. Наукові праці ЧНТУ. 2024, № 2 (284), с. 112-120.

21. Степаненко О. М. Методологія побудови KPI для SOC на базі SIEM-платформи. Проблеми інформаційної безпеки, 2023, № 1, с. 34-43.

22. Коваленко Т. С. Оцінювання ефективності правил кореляції в Kibana SIEM. Системи обробки інформації, 2024, Вип. 3 (171), с. 79-85.

23. ДСТУ ISO/IEC 27002:2017. Інформаційні технології. Методи захисту. Практичні правила управління інформаційною безпекою. Київ: Мінекономрозвитку України, 2018. 96 с.

24. ДСТУ ISO/IEC 27005:2015. Менеджмент ризиків інформаційної безпеки. Київ: Мінекономрозвитку України, 2016. 54 с.

25. АНБ США. Best Practices for Securing Log Sources. Fort Meade, 2023. 32 p.

26. AWS Security. Architecting a Cloud-Native SIEM on AWS. Seattle: Amazon Web Services, 2023. 74 p.

27. Google Cloud. Chronicle SIEM: Architecture and Deployment Guide. Mountain View, 2024. 60 p.

28. Microsoft. Microsoft Sentinel: Best Practices. Redmond, 2024. 98 p.

29. Splunk. The Essential Guide to Security Monitoring with Splunk 6. San Francisco, 2023. 148 p.

30. Elastic. Elastic Security Solution 8.11: Detection Rules Reference. Mountain View, 2024. 122 p.

31. Rapid7. InsightIDR Detection Library. Boston, 2023. 55 p.

32. Cisco. SecureX and Secure Cloud Analytics Integration Guide. San José, 2024. 48 p.

33. García-Fernández J. M. Machine-Learning Approaches for Alarm Deduplication in SIEM. Future Generation Computer Systems, 2024, Vol. 150, p. 364-378.

34. Brown L., Sharma P. Threat-Hunting Playbooks Using MITRE ATT&CK in SIEM Platforms. Journal of Digital Forensics, Security and Law, 2023, Vol. 18, № 4, p. 1-18.

35. Panchal H., Chandra S. Benchmarking Open-Source SIEMs for Cloud Environments. International Journal of Information Security Science, 2024, Vol. 13, № 2, p. 89-104.

36. European Union Agency for Cybersecurity (ENISA). State-of-the-Art Report: Security Information and Event Management. Athens, 2024. 102 p.

37. Козлова К. В. Формування системи менеджменту інформаційної безпеки підприємства : бакалаврська робота [Електронний ресурс] / Сумський державний університет. Суми, 2021. 66 с. – Режим доступу: https://essuir.sumdu.edu.ua/bitstream/download/123456789/84405/1/Kozlova_bac_rob.pdf.

38. Kent K. et al. Guide for Cybersecurity Event Recovery : NIST SP 800-184. — Gaithersburg : NIST, 2023. — 62 p.

39.Управління інформацією та подіями безпеки (SIEM) [Електронний ресурс] / Інститут інформаційних технологій та безпеки. 2024. – Режим доступу: https://iitd.ua/upravlinnya-informacziyeyu-ta-podiyamy-bezpeky-siem/.