ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія виявлення скомпрометованих ідентифікаційних даних в корпоративній мережі на базі Splunk»

зі спеціальності *125 Кібербезпека та захист інформації*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Ілля СПІВАК
(підпис)

Виконала: здобувачка вищої освіти групи БСДМ-63
СПІВАК ІЛЛЯ
(прізвище, ім'я)

Керівник д.ф., доцент СОБЧУК Андрій
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
кібербезпеки
_____ Галина ГАЙДУР
“___” жовтня 2025 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

СПІВАК Ілля Дмитрович
(прізвище, ім’я)

1. Тема кваліфікаційної роботи: «Технологія виявлення скомпрометованих ідентифікаційних даних в корпоративній мережі на базі Splunk»
керівник кваліфікаційної роботи д.ф., доцент СОБЧУК Андрій
(прізвище, ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «___» жовтня 2025 року № ___.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 25.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи
наукова та технічна література, експлуатаційна документація, нормативні документи, міжнародні стандарти.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми виявлення скомпрометованих ідентифікаційних даних в корпоративних мережах
2. Аналіз методів та засобів виявлення скомпрометованих ідентифікаційних даних
3. Технологія автоматизованого виявлення скомпрометованих ідентифікаційних даних
4. Перелік графічного матеріалу

Презентація PowerPoint.

6. Дата видачі завдання 01.10.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ зп	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення актуальності проблеми виявлення скомпрометованих ідентифікаційних даних в корпоративній мережі	01.10.2025 р.	
2.	Аналіз наукової та технічної літератури з питань виявлення скомпрометованих ідентифікаційних даних	12.10.2025 р.	
3.	Аналіз методів і засобів виявлення скомпрометованих ідентифікаційних даних в корпоративній мережі на базі Splunk	27.10.2025 р.	
4.	Розробка технології автоматизованого виявлення скомпрометованих ідентифікаційних даних	03.11.2025 р.	
5.	Розроблення рекомендацій щодо впровадження створеної технології в корпоративній мережі	15.11.2025 р.	
6.	Оформлення результатів дослідження.	26.11.2025 р.	
7.	Підготовка доповіді до захисту.	15.12.2025 р.	

Здобувачка вищої освіти _____ Ілля СПІВАК
(підпис) *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Андрій СОБЧУК
(підпис) *(ім'я, прізвище)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

здобувача СПІВАКА Іллі

на тему: «Технологія виявлення скомпрометованих ідентифікаційних даних в корпоративній мережі на базі Splunk»

Актуальність: У сучасних умовах цифрової трансформації організації дедалі активніше використовують хмарні сервіси, віддалений доступ і розподілені інформаційні системи. За таких умов облікові дані користувачів стають одним із ключових елементів доступу до корпоративних ресурсів і водночас одним із найбільш вразливих компонентів системи безпеки. Компрометація облікових даних є одним із найпоширеніших векторів сучасних кібератак.

У зв'язку з цим впровадження ефективних методів і засобів виявлення скомпрометованих облікових даних, а також застосування систем моніторингу подій безпеки є необхідною умовою забезпечення стійкості та надійності корпоративних інформаційних ресурсів. Тому тема кваліфікаційної роботи є актуальною та своєчасною.

Позитивні сторони:

1. На основі проведеного аналізу, в роботі було встановлено зміст проблеми виявлення скомпрометованих ідентифікаційних даних.
2. Досліджено методи та засоби виявлення скомпрометованих ідентифікаційних даних на базі Splunk.
3. Розглянуто зміст технології виявлення скомпрометованих ідентифікаційних даних на базі Splunk та рекомендації щодо її застосування.
4. Текст викладено достатньо грамотно, послідовно. Сформульовано чіткі та змістовні висновки. Графічний матеріал оформлено якісно. Список науково-технічної літератури свідчить про вміння користуватись матеріалами за темою кваліфікаційної роботи.

Недоліки:

1. У кваліфікаційній роботі бажано було б провести аналіз умов впроваджень SIEM систем в поєднанні з UEBA на прикладі конкретної організації.
2. Запропонований порядок застосування технології виявлення скомпрометованих ідентифікаційних даних бажано було б показати на прикладі конкретної організації.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **"відмінно"**, а здобувачка **СПІВАК ІЛЛЯ** – присвоєння кваліфікації магістр з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Рецензент:

_____	_____	_____
(науковий ступінь, вчене звання)	*(підпис)*	*(ім'я, прізвище)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач СПІВАК Ілля до захисту кваліфікаційної роботи
(прізвище, ім'я)
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)
на тему: «Технологія виявлення скомпрометованих ідентифікаційних даних в корпоративній мережі на базі Splunk».
Кваліфікаційна робота і рецензія додаються.

Директор інституту Євгенія ІВАНЧЕНКО
(підпис) *(ім'я, прізвище)*

Висновок керівника кваліфікаційної роботи

Здобувачка ***СПІВАК Ілля*** обрала тему роботи, метою якої було дослідити технологію виявлення скомпрометованих ідентифікаційних даних в корпоративній мережі на базі Splunk та розробити рекомендації щодо її впровадження. Перелік використаних джерел свідчить про вміння здобувача розбиратися у сучасних наукових підходах до виявлення шкідливого ПЗ та успішно застосовувати їх у дослідженнях. Під час виконання кваліфікаційної роботи ***СПІВАК Ілля*** показав добру теоретичну та практичну підготовку, вміння самостійно вирішувати поставлені завдання й робити обґрунтовані висновки. Роботу виконувала сумлінно, акуратно та вчасно відповідно до затвердженого плану.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***СПІВАКА Ілля*** на оцінку **"відмінно"** та присвоїти їй кваліфікацію магістр з кібербезпеки за освітньою програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи Андрій СОБЧУК
(підпис) *(ім'я, прізвище)*
"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **СПІВАК Ілля** допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
(назва)

Галина ГАЙДУР
(підпис) *(ім'я, прізвище)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 60 сторінок, 17 рисунків, 2 таблиць, 19 джерел.

Об’єкт дослідження: процес забезпечення кібербезпеки корпоративних інформаційних ресурсів організації.

Предмет дослідження: методи та засоби виявлення скомпрометованих облікових даних у корпоративних мережах на основі систем моніторингу подій безпеки.

Мета роботи: дослідити та проаналізувати підходи до виявлення скомпрометованих облікових даних у корпоративних мережах, а також оцінити ефективність систем моніторингу подій за показниками часу реагування на інциденти.

Методи дослідження: аналіз науково-технічної літератури за тематикою роботи, аналіз звітів з кібербезпеки, порівняння функціональних можливостей систем моніторингу подій, узагальнення результатів досліджень та аналітичних даних.

Короткий зміст роботи: в роботі розглянуто проблему компрометації облікових даних як одного з основних векторів сучасних кібератак. Проаналізовано роль систем моніторингу подій безпеки у виявленні несанкціонованого доступу та підозрілої активності користувачів.

На основі проведеного аналізу сформульовано висновки щодо доцільності використання систем моніторингу подій безпеки для своєчасного виявлення компрометації облікових даних.

Галузь використання: кібербезпека корпоративних інформаційних систем та мереж.

СКОМПРОМЕТОВАНІ ОБЛІКОВІ ДАНІ, МОНІТОРИНГ ПОДІЙ БЕЗПЕКИ, SIEM, SOC, MTTR, ВИЯВЛЕННЯ ІНЦИДЕНТІВ

ABSTRACT

Text part of the qualification work: 60 pages, 17 figures, 2 tables, 19 sources.

Object of research: the process of ensuring cybersecurity of corporate information resources of an organization.

Subject of research: methods and tools for detecting compromised credentials in corporate networks based on security event monitoring systems.

The aim of research: to study and analyze approaches to detecting compromised credentials in corporate networks, as well as to evaluate the effectiveness of security event monitoring systems using incident response time metrics.

Research methods: analysis of scientific and technical literature on the research topic, analysis of cybersecurity reports, comparison of functional capabilities of security event monitoring systems, and generalization of research results and analytical data.

Summary of the work: the paper considers the problem of credential compromise as one of the main vectors of modern cyberattacks.

The role of security event monitoring systems in detecting unauthorized access and suspicious user activity is analyzed. A comparative analysis of security event monitoring systems is carried out in terms of their impact on the speed of detection and handling of incidents related to the use of compromised credentials. The features of operation and limitations of various approaches to event monitoring, as well as the factors affecting the overall incident response time of the SOC, are considered.

Based on the analysis conducted in the work, conclusions are formulated regarding the feasibility of using security event monitoring systems for timely detection of compromised credentials and improving the overall level of cybersecurity of corporate information resources.

Field of application: cybersecurity of corporate information systems and networks.

COMPROMISED CREDENTIALS, SECURITY EVENT MONITORING, SIEM, SOC, MTTR, INCIDENT DETECT

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

SOC	-	Security Operations Center
SIEM	-	Security Information and Event Management
SOAR	-	Security Orchestration Automation and Response
C3	-	Compromised Credential Checking
PSI	-	Private Set Intersection
MFA	-	Multi-Factor Authentication
UEBA	-	User and Entity Behavior Analytics
LSTM	-	Long Short-Term Memory
MTTR	-	Mean Time to Resolution
MTTA	-	Mean time to Acknowledge
LSTM	-	Long Short-Term Memory
MTTI	-	Mean time to Investigate
MTTD	-	Mean time to Detect
GRU	-	Gated Recurrent Unit
ISMS	-	Information Security Management System
SSH	-	Secure Shell
ASN	-	Autonomous System Number

ВСТУП

Актуальність дослідження. Сучасні процеси цифрової трансформації суттєво змінюють підходи до побудови та захисту корпоративних інформаційних систем. Широке впровадження хмарних сервісів, віддаленого доступу, гібридних робочих моделей, систем єдиного входу та мобільних платформ призводить до зростання складності IT-інфраструктури та розширення поверхні атаки.

У таких умовах традиційні підходи до забезпечення інформаційної безпеки, що ґрунтуються на периметровому захисті, виявляються недостатньо ефективними. Однією з найбільш критичних загроз для корпоративних мереж є компрометація облікових даних користувачів. Використання валідних облікових записів дозволяє зловмисникам обходити механізми периметрового захисту та маскувати свою діяльність під легітимну поведінку користувачів. Отримавши доступ до облікових даних, зловмисники можуть здійснювати ескалацію привілеїв, переміщення між системами та тривалий час залишатися непоміченими, що значно підвищує ризик масштабних інцидентів інформаційної безпеки.

Сучасні тенденції розвитку кіберзагроз свідчать про стале зростання атак, пов’язаних із викраденням або компрометацією ідентифікаційних даних. У більшості випадків саме скомпрометовані облікові записи використовуються як початковий вектор доступу до корпоративних систем і стають основою для подальших багатоступеневих атак. Автоматизовані засоби збору облікових даних, повторне використання паролів та експлуатація витоків баз даних сторонніх сервісів значно підвищують ефективність таких атак і збільшують потенційні фінансові та репутаційні втрати організацій.

У зв’язку з цим особливої актуальності набуває завдання своєчасного виявлення скомпрометованих облікових даних та впровадження ефективних систем моніторингу подій безпеки в корпоративних мережах. Традиційні механізми автентифікації без додаткових заходів захисту вже не забезпечують належного рівня безпеки. Виникає потреба у застосуванні комплексних підходів, що включають аналіз поведінкових патернів доступу, контекстну оцінку ризику, моніторинг витоків баз даних, а також кореляцію подій безпеки.

Використання систем класу SIEM та функціонування центрів реагування на інциденти безпеки дозволяє реалізувати централізований підхід до збору, аналізу та кореляції подій, а також скоротити час виявлення й реагування на інциденти. Зменшення часу, протягом якого зловмисник може експлуатувати скомпрометовані облікові дані, є одним із ключових факторів мінімізації наслідків атак та підвищення загального рівня кібербезпеки корпоративних інформаційних ресурсів. Вищезазначене визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої присвячено дослідженню методів і засобів виявлення скомпрометованих облікових даних у корпоративних мережах на основі систем моніторингу подій безпеки.

Об’єкт дослідження – процес забезпечення кібербезпеки корпоративних інформаційних ресурсів організації.

Предмет дослідження – методи та засоби виявлення скомпрометованих облікових даних у корпоративних мережах на основі систем моніторингу подій безпеки.

Мета роботи – дослідити та проаналізувати підходи до виявлення скомпрометованих облікових даних у корпоративних мережах, а також оцінити ефективність систем моніторингу подій безпеки за показниками часу реагування на інциденти.

Наукові завдання:

дослідити сутність проблеми компрометації облікових даних у корпоративних інформаційних системах;

проаналізувати сучасні тенденції та вектори атак, пов’язані з використанням скомпрометованих облікових записів;

проаналізувати підходи до виявлення компрометації облікових даних на основі моніторингу подій безпеки;

дослідити функціональні можливості SIEM-систем щодо виявлення та реагування на інциденти безпеки; оцінити вплив систем моніторингу подій на показники часу виявлення та реагування на інциденти.

Методи дослідження – аналіз науково-технічної літератури та звітів з кібербезпеки, порівняльний аналіз функціональних можливостей систем моніторингу подій безпеки, узагальнення аналітичних даних та результатів досліджень.

Практичне значення одержаних результатів полягає у можливості використання отриманих висновків і рекомендацій фахівцями з кібербезпеки для підвищення ефективності виявлення скомпрометованих облікових даних та зменшення часу реагування на інциденти у корпоративних мережах.

1 МОНІТОРИНГ ПОДІЙ ТА ВИЯВЛЕННЯ АНОМАЛІЙ У КОРПОРАТИВНІЙ МЕРЕЖІ

1.1 Теоретичні основи моніторингу подій у корпоративних мережах

В сучасних умовах цифрової розвитку державні установи та комерційні організації все частіше стикаються зі зростанням кількості та складності кіберзагроз. Це особливо помітно в умовах розширення мережевої інфраструктури та впровадження віддаленого доступу, коли збільшується кількість підключень поза межами корпоративного чи державного периметру, що підвищує ризики несанкціонованого доступу до інформаційних систем.

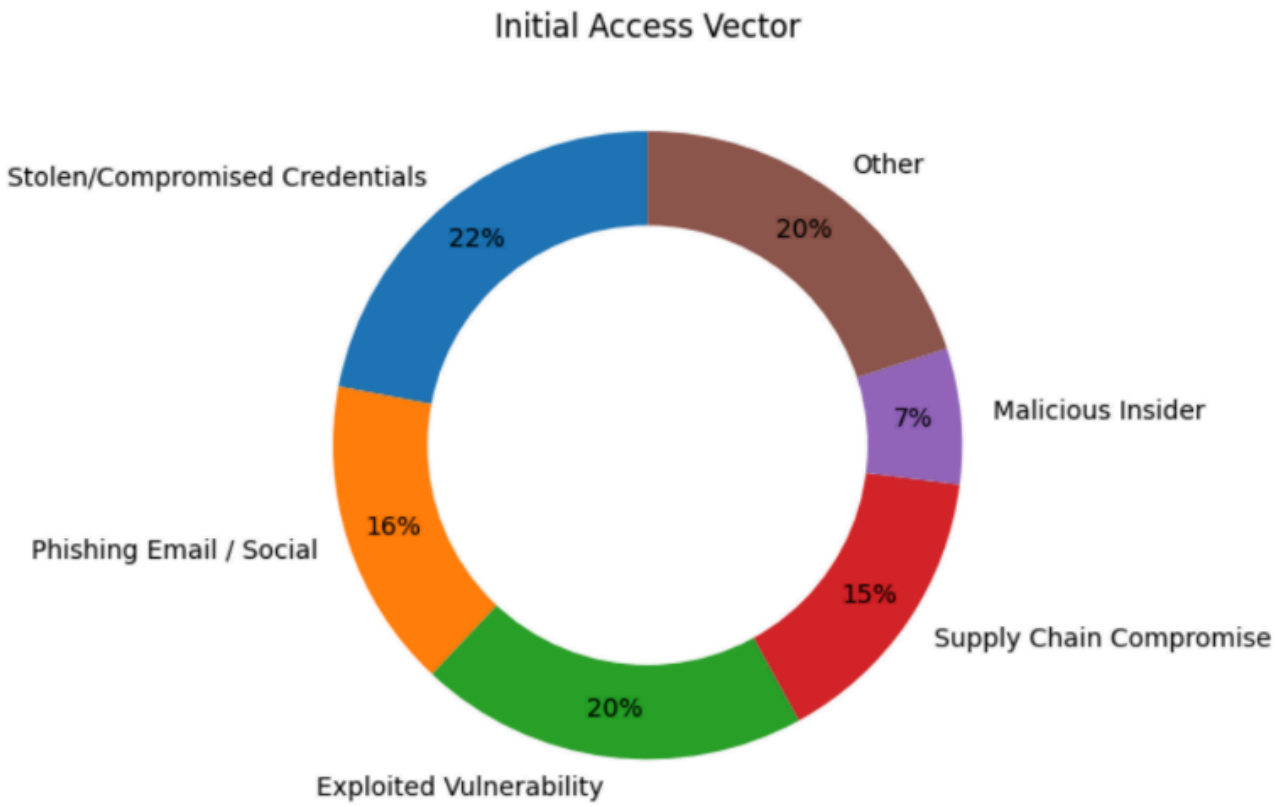
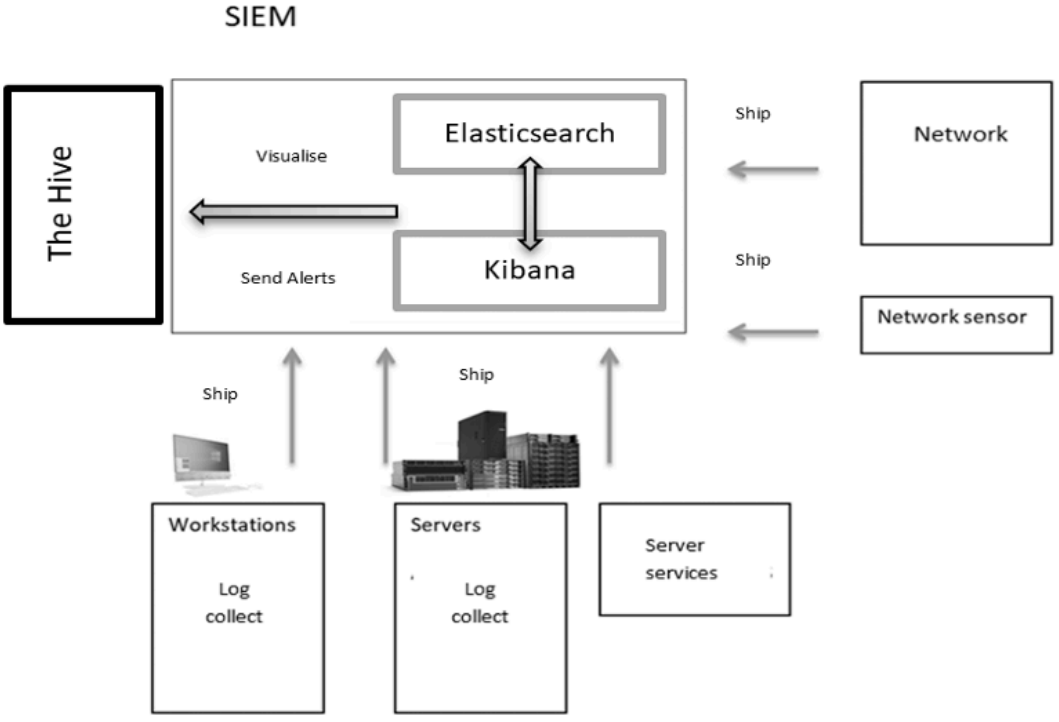


Рис. 1.1 Відсоткове співвідношення кількості векторів отримання доступу [8]

Для забезпечення належного рівня кібербезпеки необхідно впроваджувати комплексні технічні, адміністративні та організаційні заходи, які дозволяють вчасно виявляти та запобігати потенційним інцидентам. Недостатня організація інформаційної безпеки призводить до порушення цілісності систем та втрати даних, що безпосередньо впливає на стабільність роботи установи або підприємства.

Одним із елементів забезпечення інформаційної безпеки в корпоративних або державних мережах є впровадження систем централізованого моніторингу подій. Такі системи зазвичай реалізуються у форматі оперативного центра безпеки - SOC, який об’єднує фахівців, технології та процеси для безперервного контролю стану кіберзахисту. Основним інструментом SOC виступає система управління інформаційними та подіями - SIEM, що здійснює збір і кореляцію логів з різних джерел, таких як сервери, мережеві пристрої, бази даних і сервіси керування обліковими записами. Це дозволяє виявляти потенційно небезпечну активність у режимі реального часу, оперативно реагувати на інциденти та зменшувати наслідки компрометації облікових даних. [15]



\

Рис. 1.1 Приклад схеми потоку даних в SIEM системі

Логування є основою будь якої системи моніторингу безпеки. Це процес фіксації усіх значущих дій користувачів, системних процесів і мережевих подій у вигляді структурованих записів. Кожен запис містить відомості про час події, її джерело, тип, ідентифікатор користувача, результат виконання дії та інші атрибути, що дозволяють відтворити контекст події. У сучасних корпоративних мережах генерується величезний обсяг таких даних, тому для ефективної роботи необхідна їхня автоматизована обробка. SIEM системи виконують функції збору логів із різних джерел, перетворюючи їх у єдиний уніфікований формат, що дає змогу проводити пошук, фільтрацію та аналітику на основі отриманих даних.

Ефективність логування також залежить від дотримання політик зберігання, доступу та аудиту даних. Згідно з рекомендаціями NIST SP 800-92 та ISO/IEC 27001, журнали подій мають зберігатися у захищеному середовищі з контрольованим доступом, а час їхнього зберігання повинен відповідати вимогам внутрішніх регламентів і нормативних актів. Це дозволяє проводити ретроспективний аналіз у разі інцидентів, забезпечуючи доказову базу для форензічного розслідування.[10,3]

Наступним етапом після збору й нормалізації логів є аналітика подій, яка включає створення кореляційних правил і поведінкових моделей для виявлення аномалій. Сучасні SIEM системи не обмежуються статичними правилами, в них також інтегрують алгоритми машинного навчання, що дозволяють будувати профілі “нормальної” активності користувачів і систем. Завдяки цьому стає можливим виявлення нових, раніше невідомих типів атак, які не мають чітких сигнатур.

Окрім цього важливим аспектом аналітики є кореляція подій з різних джерел. Це дозволяє поєднувати інформацію з систем автентифікації, мережевих пристроїв, серверів додатків та засобів контролю доступу в єдиний контекст подій. Для підвищення точності аналізу застосовуються методи статистичної обробки, часових рядів і кластеризації, що допомагає відокремити випадкові

відхилення від дійсно загрозливих подій. [10,3]

Таким чином, процес логування виступає не лише технічним інструментом збору інформації, а є основою системи аналітики подій безпеки. Правильна організація цього процесу дозволяє своєчасно виявляти аномальну поведінку користувачів, спроби несанкціонованого доступу, компрометацію облікових даних і внутрішні загрози. У результаті централізоване логування та аналітика даних у SIEM формують єдине середовище для моніторингу, реагування та мінімізацію наслідків потенційних інцидентів.

1.2 Актуальні проблеми та приклади компрометації облікових даних у корпоративних мережах

Однією з загроз у сучасних корпоративних мережах є використання скомпрометованих облікових даних, отриманих внаслідок витоків із баз даних, фішингових кампаній або шкідливих програм. Зловмисники активно застосовують такі дані для реальних атак, а не лише для продажу.

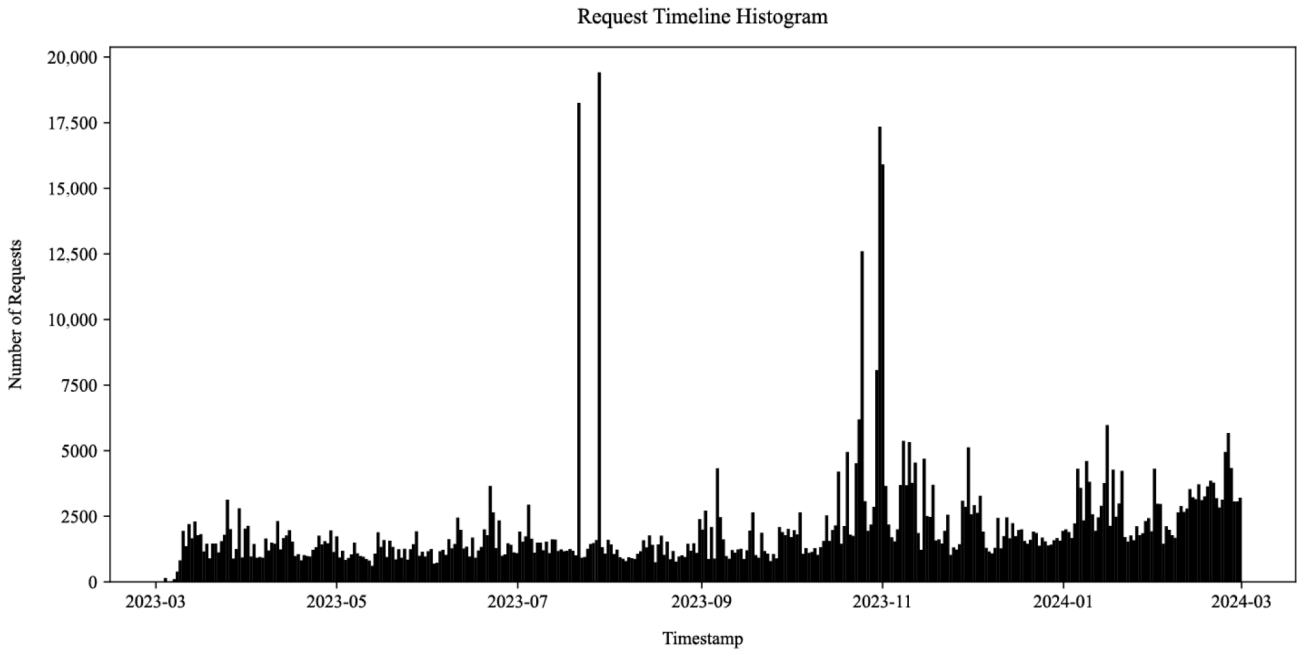


Рис. 1.2 Графік кількості використання скомпрометованих даних після їх витоку

Вже протягом кількох годин після оприлюднення бази витоку починається автоматизоване сканування та спроби входу в системи з використанням викрадених логінів і паролів. Близько 70 % виявлених спроб використовували звичайні протоколи аутентифікації SSH, RDP або HTTP форми входу. Це свідчить, що кіберзлочинці дедалі частіше використовують викрадені облікові дані як основний вектор проникнення до корпоративних систем, оминаючи складні технічні експлойти.

Також значна частина скомпрометованих облікових даних є повторно використаними паролями для кількох сервісів. У корпоративному контексті це створює критичну загрозу, коли зловмисник, що отримавши доступ до облікового запису на зовнішньому ресурсі , може скористатися тими ж даними для входу до внутрішньої мережі компанії. Такий тип атак називається credential stuffing і є однією з найчастіших причин компрометації корпоративних облікових записів.[13]

Згідно з аналітичним звітом ENISA Threat Landscape 2024, дедалі більше атак базуються на поєднанні викрадених облікових даних із соціальною інженерією або внутрішніми зловживаннями. Співробітники або підрядники, які мають легітимний доступ до корпоративної мережі, можуть свідомо або випадково сприяти витоку конфіденційних даних, обходячи більшість механізмів контролю доступу. Ще одним вектором загрози стають ланцюги постачання, коли компрометація одного партнера або інтегрованого зовнішнього сервісу призводить до витоку облікових даних і компрометації всієї екосистеми. Прикладом є інциденти, коли через доступ постачальників IT послуг зловмисники отримували контроль над внутрішніми серверами організацій замовника.[5]

Таким чином компрометація облікових даних у корпоративних мережах є комплексною проблемою, що поєднує технічні, організаційні та людські чинники.

1.3 Методи виявлення скомпрометованих ідентифікаційних даних

Для організації ефективного виявлення скомпрометованих облікових даних необхідно розробити класифікацію методів, що дозволяє систематизувати підходи за типом джерел інформації та характером аналітичних дій.

На мою думку класифікація підходів до детекції базується на принципі різноспрямованості джерел інформації:

- зовнішні дані - витоки даних на зовні
- внутрішні поведінкові сигнали - аномалії в діях користувачів
- активні методи протидії - обманні механізми

Моніторинг витоків облікових даних

Моніторинг витоків облікових даних є одним із методів виявлення використання скомпрометованих пар логінів і паролів до моменту їх експлуатації зловмисниками. Основною ідеєю таких систем є перевірка ідентифікаційних\облікових даних користувача на наявність у базах викрадених записів без розкриття самих паролів або іншої конфіденційної інформації.

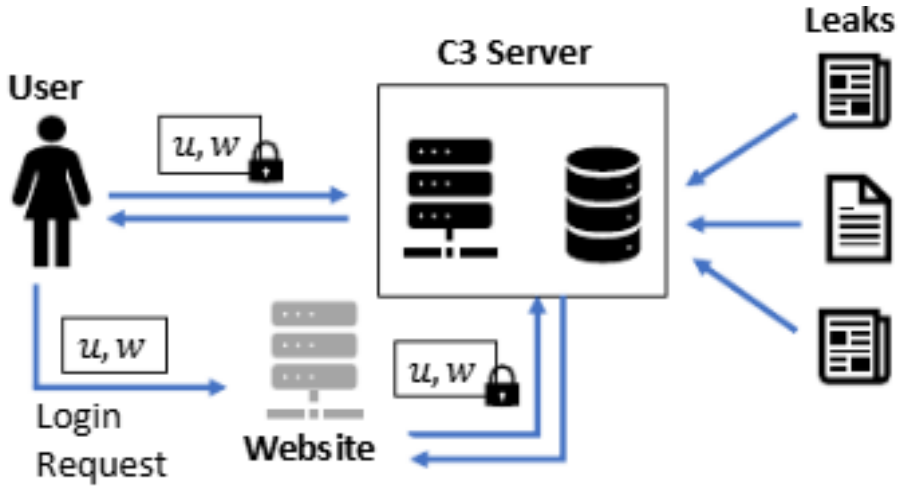


Рис. 1.3 Схема роботи С3 сервера

Для цього використовуються криптографічні протоколи перевірки компрометації С3, що дозволяють користувачеві або сервісу підтвердити безпеку

облікових даних. В порівнянні з С3 інші механізми перевірки, що використовують хеші своїх паролів для відправки на сервер перевірки, створюють ризик повторної компрометації, оскільки навіть хешовані значення можуть бути використані для атак з попереднім обчисленням. Для вирішення цієї проблеми дослідники запропонували низку протоколів приватної перевірки, заснованих на технологіях Private Set Intersection (PSI), гомоморфному шифруванні, які дозволяють зіставляти дані між користувачем і сервером без розкриття їхнього вмісту. [12]

З практичної точки зору, системи моніторингу витоків можуть працювати у двох режимах пасивний та активний. Перший - це тип моніторингу, коли безпекова команда або SIEM система періодично перевіряє облікові дані користувачів на наявність у відомих витоках, використовуючи захищені API або локальні копії баз. Інший тип моніторингу, коли система в реальному часі аналізує події аутентифікації і здійснює автоматичну перевірку під час входу користувача. Поєднання таких перевірок з політиками ротації паролів, багатофакторною аутентифікацією - MFA та централізованим управлінням обліковими записами істотно знижує ризик компрометації корпоративних систем. Таким чином, моніторинг витоків на основі С3-протоколів є перспективним напрямом розвитку кіберзахисту організацій, який забезпечує баланс між проактивним виявленням компрометації та збереженням приватності користувачів. Його впровадження дозволяє значно скоротити час реагування на інциденти, запобігти несанкціонованому доступу та підвищити довіру до корпоративних систем аутентифікації.[12]

Поведінковий аналіз користувачів та сутностей

Поведінковий аналіз користувачів та сутностей є одним із інструментів виявлення компрометації облікових даних та внутрішніх загроз у корпоративних середовищах. Його основна мета полягає у виявленні відхилень від усталених моделей поведінки користувачів, системних процесів і мережевих об’єктів, що може свідчити про порушення безпеки навіть у разі відсутності явних сигнатур.

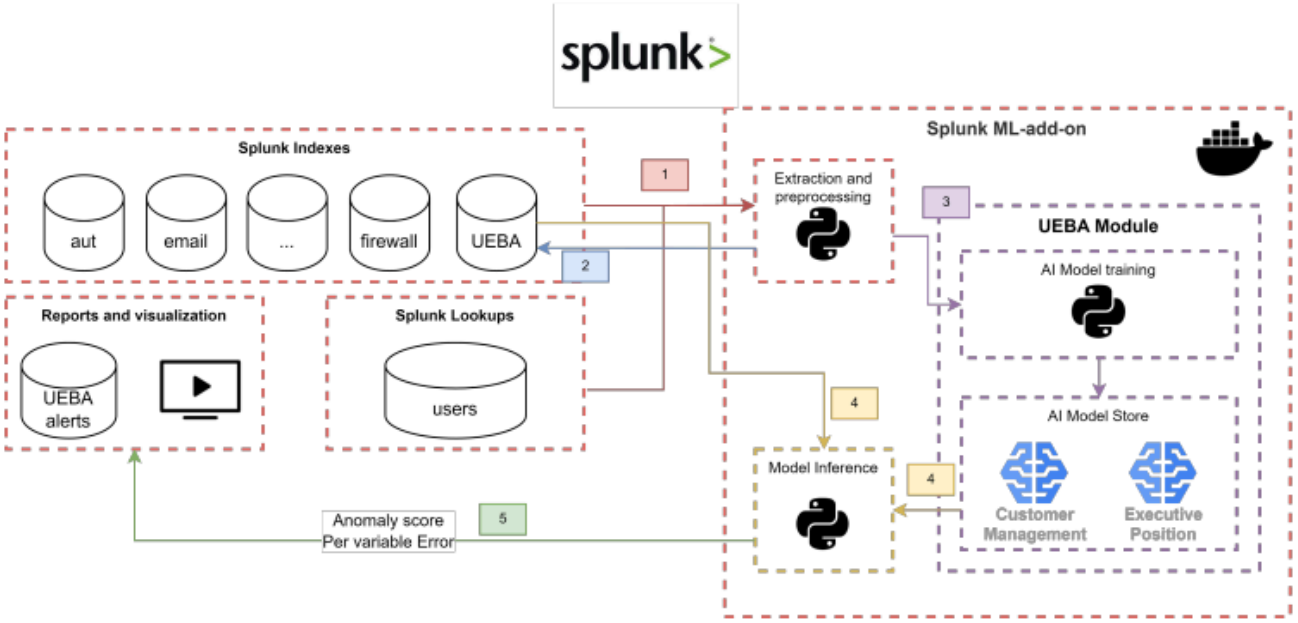


Рис. 1.4 Архітектура системи виявлення аномалій на базі UEBA

Системи UEBA функціонують на основі алгоритмів машинного навчання, які формують профіль “нормальної” поведінки кожного користувача чи пристрою, використовуючи історичні дані з журналів аутентифікації, мережевого трафіку, дій з файлами, системних викликів та інших джерел. Виявлення аномалій здійснюється через порівняння поточних дій з еталонними поведінковими шаблонами. Значне відхилення від сформованої моделі інтерпретується як потенційна загроза, що може бути результатом викрадення облікових даних або зловживання доступом.[1]

Ефективність сучасних UEBA значно підвищується завдяки застосуванню глибинних автоенкодерів, які дозволяють виявляти приховані закономірності та нелінійні залежності між поведінковими ознаками. Такі моделі аналізують багатовимірні вектори активності користувачів і обчислюють похибку реконструкції, що виступає індикатором рівня відхилення поточної поведінки від звичної. Визначення аномалій у рамках UEBA не обмежується аналізом окремих подій, а враховує контекст дій користувача - час входу в систему, географічне розташування, послідовність виконаних операцій, типи звернень до ресурсів, інтенсивність роботи з файлами або сервісами. Такий багаторівневий підхід забезпечує високу точність розпізнавання нетипової активності, знижуючи

кількість хибнопозитивних спрацьовувань.[1]

Результати аналізу в системах UEBA можуть бути інтегровані з платформами SIEM або SOAR для подальшої кореляції подій та автоматизованого реагування. Це дозволяє оперативно блокувати підозрілу активність, проводити розслідування інцидентів та підвищувати рівень ситуаційної обізнаності в межах центру кіберзахисту. Застосування UEBA сприяє переходу від заходів реагування до проактивної моделі кіберзахисту, у якій акцент робиться не на фіксації інцидентів після їх виникнення, а на своєчасному виявленні поведінкових відхилень, що передують атаці. Таким чином, поведінковий аналіз користувачів виступає критично важливим елементом сучасної архітектури безпеки корпоративних мереж, підвищуючи стійкість організацій до внутрішніх загроз та цілеспрямованих атак.[1]

Honeytokens - введення в оману

Введення в оману - це стратегія активного захисту, що передбачає створення фіктивних об’єктів у цифровому середовищі з метою виявлення зловмисників або зміщення їхньої діяльності зі справжніх цілей. До таких об’єктів належать honeytokens - фальшиві ресурси, які не використовуються легітимними користувачами, а також decoy-облікові записи, які імітують справжні акаунти із правами доступу. При спробі взаємодії з такими об’єктами генерується подія про несанкціоновану активність. Перевагою такого підходу є низький рівень помилкових спрацювань, оскільки легітимні користувачі зазвичай не мають причин взаємодіяти з подібними об’єктами. Інтеграція механізмів введення в оману з SIEM та UEBA-системами дозволяє корелювати події доступу до decoy-ресурсів з поведінковими індикаторами та швидко ініціювати процес реагування на інцидент.[18]

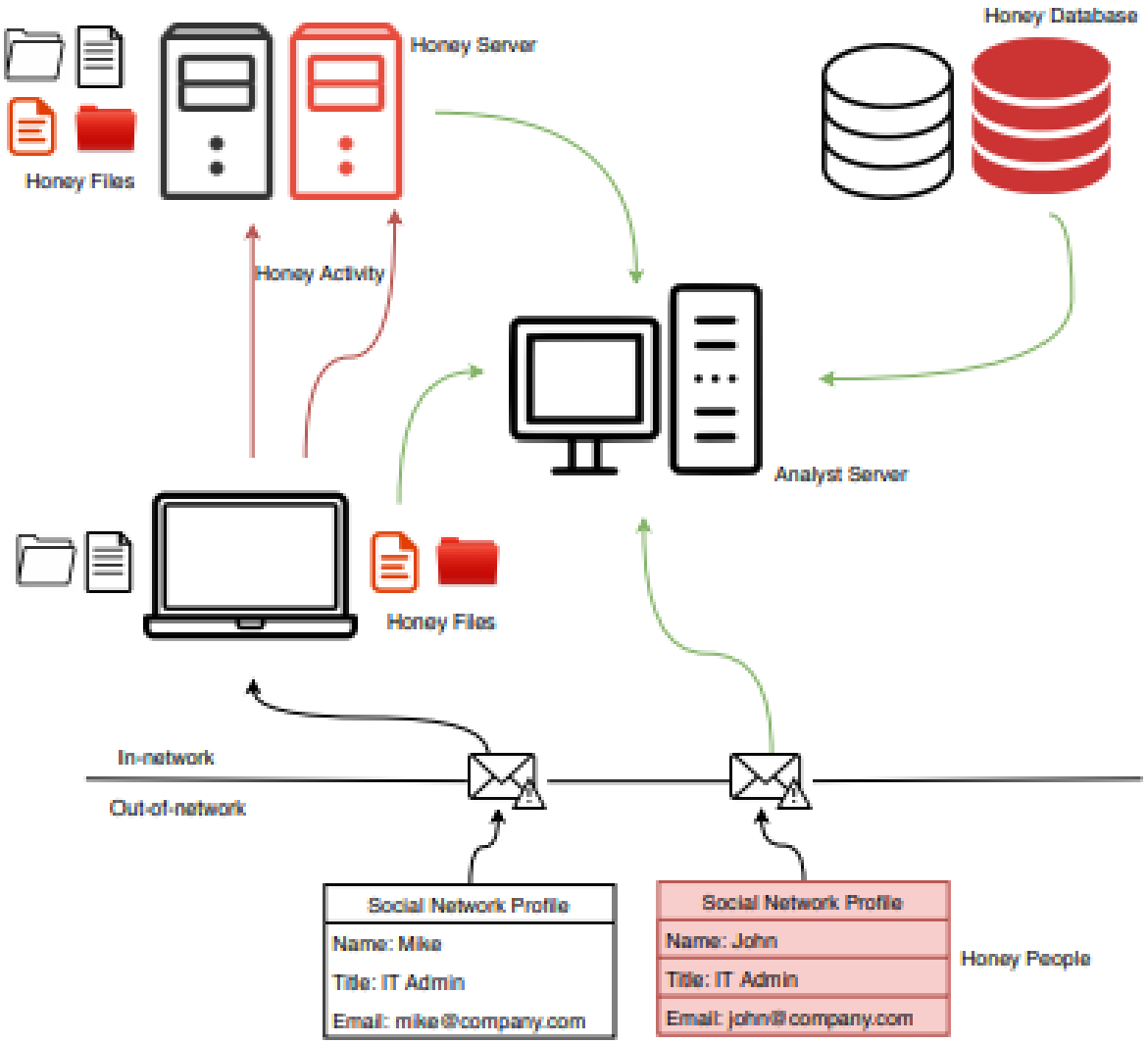


Рис. 1.5 Приклад системи з застосуванням honeypots

Для практичної імплементації таких технологій у корпоративній мережі рекомендується:

- Впровадження фальшивих облікових записів із видимими правами, але без реального завдання, розміщених поряд із легітимними обліковими записами;
- Створення файлів-приманок або документів із унікальними ідентифікаторами, які ніколи не використовуються легітимно, тому кожний доступ до них є підозрілим;
- Інтеграція сигналів з honeytokens до систем SIEM чи UEBA, щоб подія активації фальшивого об’єкта автоматично створювала інцидент або підвищувала ризик облікового запису.

Основна перевага таких методів полягає в тому, що вони дають високу довіру до того, що атака відбулася або знаходиться в процесі. Спроби доступу до “пастки” є прямим сигналом про присутність зловмисника, що дозволяє скоротити час виявлення та почати реагування до масштабного поширення.[18]

Однак ефективність deception-технологій залежить не лише від їх розгортання, а й від життєвого циклу та глибини застосування цих “пасток”. Інтеграція honeytokens і decoy-облікових записів у стратегічну архітектуру кібербезпеки сприяє виявленню скомпрометованих облікових даних, особливо коли традиційні системи моніторингу ще не зафіксували активність зловмисників. Deception-технології може доповнювати SIEM системи та створюють додатковий рівень захисту шляхом активного введення в оману атакуючих і збору інформації про їхні дії.[18]

Ефективне виявлення скомпрометованих облікових даних у корпоративних мережах базується не лише на технічних інструментах, а й на відповідності міжнародним стандартам кібербезпеки. ISO та NIST визначають комплекс рекомендацій, що охоплює вимоги до журналювання подій, моніторингу активності користувачів, управління інцидентами, контролю доступу та реагування на порушення безпеки. Ці стандарти задають фундаментальні принципи, які організації повинні інтегрувати у власні політики та технічні процеси, щоб забезпечити своєчасне виявлення несанкціонованого доступу та зниження ризиків, пов’язаних із компрометацією облікових записів.

У рамках стандарту ISO/IEC 27001 ключові вимоги зосереджені в Annex A, де визначено необхідність журналювання подій (A.12.4), моніторингу системної активності (A.12.4.3), контролю доступу (A.9) та організації процесів управління інцидентами (A.16). Допоміжні стандарти, зокрема ISO/IEC 27002 і ISO/IEC 27035, деталізують вимоги щодо змісту логів, їхнього захищеного зберігання, механізмів аналізу та процедур реагування на інциденти, включно з випадками використання викрадених або підроблених облікових даних.[5,6]

Зі іншого боку, інститут NIST пропонує систему вимог та рекомендацій, орієнтованих на практичну реалізацію моніторингу безпеки. Документ NIST SP 800-53 формує перелік контролів, необхідних для виявлення аномальних дій користувачів (AU-6, AC-7, AC-17, SI-4), а NIST SP 800-92 визначає принципи збору, кореляції та аналізу журналів подій, включно з вимогами до джерел логів і методів їхньої обробки. Стандарт NIST SP 800-61 описує життєвий цикл реагування на інциденти та визначає, які саме події повинні спричиняти ескалацію або ініціювати процес розслідування, що охоплює й випадки підозри на компрометацію облікових записів.[10,9]

Незалежно від конкретної технології чи продукту, стандарти ISO та NIST узгоджено наголошують на важливості побудови системи раннього виявлення підозрілої активності. Це включає аналіз невдалих та успішних автентифікацій, визначення нетипових шаблонів поведінки, контроль доступу до критичних ресурсів і забезпечення неупередженості журналів подій. Таким чином, нормативні вимоги формують основу для створення цілісної системи моніторингу, яка здатна забезпечувати своєчасне виявлення компрометації навіть за умови використання складних векторів атак або спроб приховування слідів зловмисника.

2 МЕТОДИ ВИЯВЛЕННЯ СКОМПРОМЕТОВАНИХ ІДЕНТИФІКАЦІЙНИХ ДАНИХ НА ОСНОВІ АНОМАЛІЙ

2.1 Виявлення аномальної поведінки

Виявлення аномальної поведінки користувачів і аналіз віддалених підключень, це завдання що спрямоване на ідентифікацію дій, які відхиляються від усталених моделей роботи суб’єктів або характеризуються підозрілими віддаленими сесіями. Це дозволяє виявляти компрометацію облікових записів, автоматизовані атаки підбору паролів, та коли зловмисник після початкового входу поширює доступ у мережі.[7]

Класифікація аномальної поведінки користувачів

Класифікація аномалій:

- Точкові аномалії - тип відхилення\аномалії в поведінці, який характеризується одиничною подією, що різко вибивається з нормальної статистики. Це може бути разовий вхід у систему з IP-адреси,що позначена як зломисна, або аутентифікація з пристрою, який раніше не використовувався конкретним користувачем. У контексті систем безпеки точкові аномалії часто є першим сигналом компрометації, який надалі аналізується за допомогою поведінкових чи контекстних моделей.[17]
- Контекстні аномалії - такі аномалії проявляються тоді, коли певна дія є нормальною в одному контексті, але стає підозрілою в іншому. До прикладу, користувач систематично входить у корпоративну мережу з однієї локації, але одного дня з іншої країни у позаробочий час. Контекстні аномалії враховують часові, географічні та поведінкові параметри, що дозволяє уникнути помилкових спрацьовувань і точніше визначати підозрілі дії.[17]
- Колективні/послідовні аномалії - цей тип охоплює послідовність подій, які

окремо можуть бути нормальними, але разом утворюють підозрілу поведінкову модель. Як приклад, серія невдалих входів до системи з подальшим успішним доступом і запитом до конфіденційних ресурсів. Для їх виявлення часто використовуються рекурентні нейронні мережі LSTM, які аналізують послідовності логів у часовому розрізі.[17]

- Часові аномалії - їх суть полягає у відхиленні в часових інтервалах між подіями. Коли звичайна сесія користувача триває 10 хвилин, а зафіксована нова вже понад годину або навпаки, складається з численних коротких з'єднань у нетиповий час. Такі аномалії важко виявити класичними методами статистичного аналізу, але вони добре ідентифікуються моделями з пам'яттю часу.[17]
- Аномалії в траєкторії виконання - цей тип базується на аналізі логів і траєкторій дій користувачів у системі. Якщо звичайна послідовність дій адміністратора це аутентифікація, запуск системного журналу та перевірка стану серверів, то відхилення може бути сигналом компрометації. Аномалії такого типу описуються як порушення очікуваного графу подій, тобто зміна структури послідовностей, що зазвичай спостерігаються у логах.[17]

Підходи виявлення аномальної поведінки

Виявлення аномальної активності в логах користувачів базується на поєднанні статистичних, поведінкових, машинних і кореляційних методів аналізу, які разом формують багаторівневий підхід до ідентифікації потенційно скомпрометованих облікових записів. Сучасні системи UEBA та SIEM поєднують одразу кілька класів алгоритмів, що дозволяє отримати комплексне уявлення про поведінку користувачів у динаміці.

Одним з підходів до виявлення відхилень є статистичний аналіз. У таких системах формується базова лінія нормальної поведінки, що описує типові значення для кожного користувача або групи.Їх частоту логінів, години активності, обсяг запитів до ресурсів. Будь-яке значне відхилення від цих параметрів може трактуватися як потенційно підозріле. Статистичні моделі прості у впровадженні,

проте їхня ефективність знижується в умовах складної, динамічної поведінки користувачів, що характерно для великих корпоративних середовищ. Тому в практиці UEBA домінує застосування методів машинного навчання, здатних автоматично формувати моделі нормальної активності та виявляти багатовимірні відхилення. Неконтрольоване навчання особливо поширене, оскільки аномалії трапляються рідко й важко маркуються вручну. Алгоритми по типу Isolation Forest, автоенкодерів або кластеризації дозволяють будувати багатовимірний простір ознак і визначати події, що статистично вибиваються зі звичних кластерів поведінки. Такий підхід ефективний для виявлення точкових і контекстних аномалій, де важливими є не окремі події, а їхня віддаленість від “нормальної” структури даних.[11]

Для складніших сценаріїв, застосовуються моделі, здатні аналізувати логічні зв’язки між подіями у часовій послідовності. Глибокі нейронні мережі, зокрема LSTM, GRU та їх гібридні варіанти, дозволяють виявляти відхилення у маршрутах користувацької активності, де аномалія виникає не у самій події, а її місце в загальній структурі поведінки. Аналогічно працюють і приховані марковські моделі, здатні оцінювати ймовірність переходів між станами та виявляти ті траєкторії, що практично ніколи не зустрічаються у звичайному робочому процесі.[19]

Важливим елементом сучасних SIEM і UEBA є кореляційний аналіз. На відміну від класичних сигнатурних правил, кореляційні моделі дозволяють оцінювати події у взаємозв’язку. Кореляція дозволяє виявляти складні атаки, де зловмисник поступово пересувається в мережі, комбінуючи різні тактики. Також суттєву роль у виявленні аномалій відіграє побудова поведінкових профілів. UEBA системи формують унікальні моделі для кожного користувача, враховуючи типові робочі години, місця входу, частоту використання окремих систем, характер доступу до файлів і сервісів. Відхилення від цього профілю накопичуються та впливають на ризиковий рейтинг користувача, забезпечуючи довготривалу оцінку його поведінки навіть у випадках, коли одиничні події не є критичними.

У практиці інформаційної безпеки найкращі результати дають гібридні підходи, що поєднують машинне навчання, статистичний аналіз, кореляційні правила та контекстні ознаки. Таким чином, сучасне виявлення аномалій базується на багаторівневій моделі, де кожна технологія компенсує обмеження іншої, забезпечуючи точніше виявлення загроз у багатовимірному середовищі корпоративних логів.

Застосування машинного навчання в виявленні аномальної поведінки

Як і більшості аспектів кібербезпеки, машинне навчання(ML) застосовується і в виявлення аномальної поведінки користувачів та потенційно скомпрометованих облікових записів. Алгоритми ML дозволяють аналізувати великі об’єми логів і телеметрії, виявляючи складні патерни активності, які важко формалізувати традиційними правилами. Наприклад, супервізовані моделі можуть класифікувати сеанси доступу як типові або аномальні на основі набору ознак, що включають джерело підключення, час автентифікації, цільові ресурси та попередню поведінку користувача

Основні підходи включають:

- Створення поведінкових профілів користувачів на основі історичних даних і багатовимірної агрегації подій.
- Класифікацію сесій доступу та подій із застосуванням алгоритмів ML для визначення нетипових чи потенційно зловмисних дій.
- Використання LLM або трансформерних моделей для аналізу текстових логів та побудови семантичних ембедінгів, що дозволяє виявляти приховані відхилення у поведінці користувачів.
- Інтеграцію моделей із системами SIEM/UEBA, щоб автоматично генерувати попередження, оцінювати пріоритетність інцидентів та підтримувати «людину в циклі» для перевірки хибних спрацювань.

Ці методи дозволяють значно підвищити ефективність детекції аномалій, зменшити навантаження на аналітиків та скоротити час реагування на потенційно

шкідливі дії в мережі. Водночас слід враховувати виклики, пов’язані з потребою великих наборів даних із мітками, потенційною вразливістю моделей до атак на дані та необхідністю пояснюваності рішень.[4]

2.2 Splunk Enterprise Security: Архітектура та функціональні можливості

Splunk Enterprise є однію з платформ типу SIEM, призначеною для збору, індексації та аналітичної обробки машинних даних з системних журналів, мережевого трафіку, пристроїв безпеки, серверів і прикладних систем. Основна концепція роботи полягає у створенні централізованого репозиторію подій, що дозволяє проводити кореляцію даних, аналіз інцидентів та побудову поведінкових моделей у реальному часі.

Splunk Enterprise використовує власний рушій індексації, що забезпечує швидке пошукове оброблення великих обсягів журналів подій. Система підтримує реальний моніторинг активності, створює дашборди та звіти для візуалізації даних, а також застосовує кореляційні пошуки для виявлення складних загроз. Гнучкість Splunk Enterprise дозволяє налаштовувати власні правила детекції, панелі моніторингу та звітність, що робить платформу придатною для застосування в підприємствах різного розміру та напрямку роботи. У практичних кейсах Splunk ES демонструє ефективність у виявленні APT-атак, внутрішніх загроз і т.п, що свідчить про його важливу роль у побудові сучасних стратегій кіберзахисту.

Архітектура Splunk Enterprise побудована з урахуванням принципів масштабованості, гнучкості та централізованого управління безпековими подіями. Система складається з кількох ключових компонентів, кожен з яких виконує специфічну роль у зборі, нормалізації, зберіганні та аналітиці даних.

Архітектура Splunk Enterprise:

- **Рівень збору даних** - відповідає за прийом потоків інформації з різних джерел, таких як серверні журнали, мережеві пристрої, фаєрволи, антивірусні системи, системи контролю доступу, IoT-пристрої тощо. Завдяки конекторам (Forwarders), які транспортують дані у стиснутому та безпечному вигляді до центрального сховища, Splunk може отримувати інформації різного формату.
- **Рівень індексації та зберігання** - отримані події обробляються і зберігаються в оптимізованому вигляді індексів. Splunk застосовує власний механізм колонкової індексації, який дозволяє здійснювати пошук за часовими мітками, полями та ключовими словами з мінімальною затримкою. Індекси зберігаються у вигляді bucket структур, які забезпечують баланс між швидкістю пошуку та ефективним використанням дискового простору.
- **Аналітичний рівень** - центральна складова платформи, яка дозволяє аналітикам використовувати Search Processing Language (SPL) для створення запитів, побудови дашбордів, створення попереджень і кореляційних правил. У цьому шарі реалізовано модулі Splunk, що забезпечують можливість моніторинг, аналітику інцидентів, керування доступами.

Рис. 2.1 Схема потоку даних в Splunk Enterprise

Серед всіх функцій Splunk Enterprise можна виділити декілька ключевих:

- Кореляція подій та пошук загроз. Splunk Enterpris надає користувачам набір кореляційних пошуків, що дозволяє виявляти зв’язки між подіями з різних джерел. Система може об’єднувати події входу до системи, зміну прав користувача та спроби доступу до конфіденційних файлів у єдиний інцидент. Ці пошуки базуються на SPL-запитах і можуть бути адаптовані до специфіки організації.
- Набір інструментів з машинним навчанням. Однією з ключових особливостей Splunk Enterpris є модуль моніторингу безпеки, який дозволяє створювати моделі поведінкової аналітики. Його також можна застосовувати для прогнозування навантаження, виявлення зловмисних процесів та класифікації подій на основі історичних даних.
- Адаптивне реагування на події. Цей підхід значно скорочує час від моменту виявлення до реагування. Якщо система виявить підозрілу активність, вона може тимчасово заблокувати користувача,ip-адресу або надіслати запит у систему керування доступами.

Для оцінювання ефективності різних систем моніторингу подій застосовують низку критеріїв, зокрема MTTR, зручність інтерфейсу, масштабованість, інтеграцію з іншими системами, гнучкість налаштувань кореляційних правил та рівень автоматизації реагування. MTTR (Mean Time to Resolution) - це середній час, необхідний для виявлення, аналізу та усунення інциденту безпеки. Він є ключовим показником ефективності роботи SOC та якості аналітичних інструментів SIEM-рішення. Менше значення MTTR вказує на швидше виявлення й вирішення інцидентів, що безпосередньо знижує ризик ескалації атак або тривалого простою систем.[2]

MTTR є узагальненим індикатором, що складається з кількох ключових метрик, які відображають різні етапи обробки інциденту. До складових MTTR належать MTTD, MTTA, MTTI. [2]

MTTA характеризує проміжок часу від моменту появи сповіщення в системі

до того, як аналітик SOC офіційно бере інцидент у роботу. На цей показник впливають організаційні процеси, якість системи оповіщення, кількість хибних спрацювань та загальне навантаження на команду.[2]

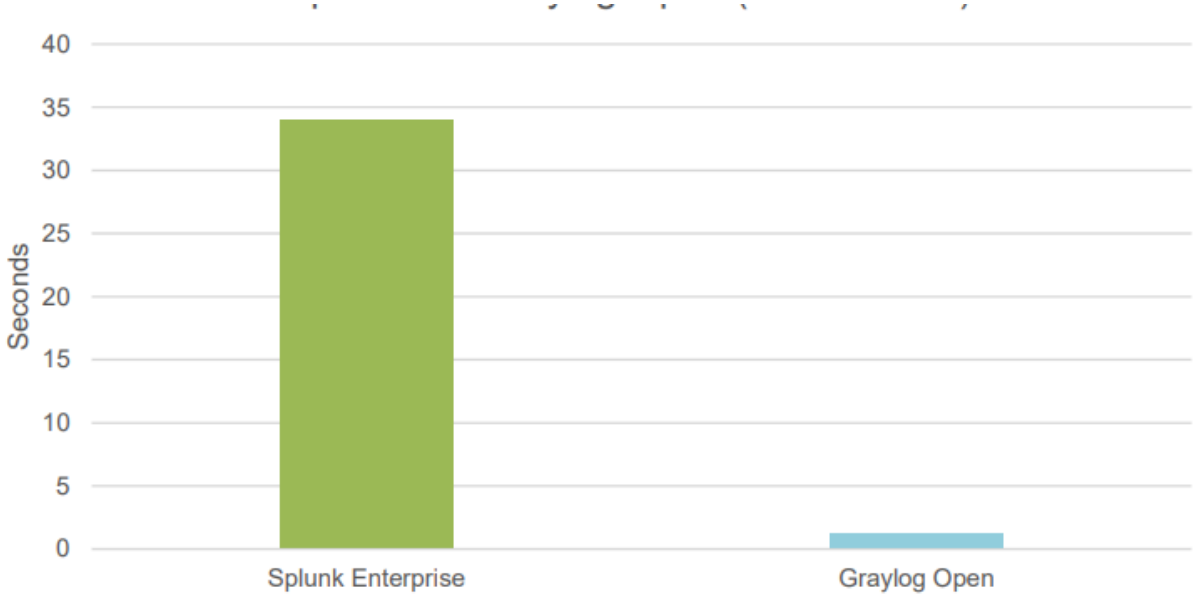


Рис. 2.2 Середнє значення MTTA для Splunk та Graylog

MTTD визначає, скільки часу минає від фактичного початку шкідливої активності до моменту, коли система класифікує її як загрозу. Ця метрика залежить від якості логування, алгоритмів аналізу, налаштування кореляційних правил, а також можливостей поведінкової аналітики. Чим нижче MTTD, тим швидше організація помічає потенційний інцидент і тим менше часу залишається зловмиснику для розвитку атаки.[2]

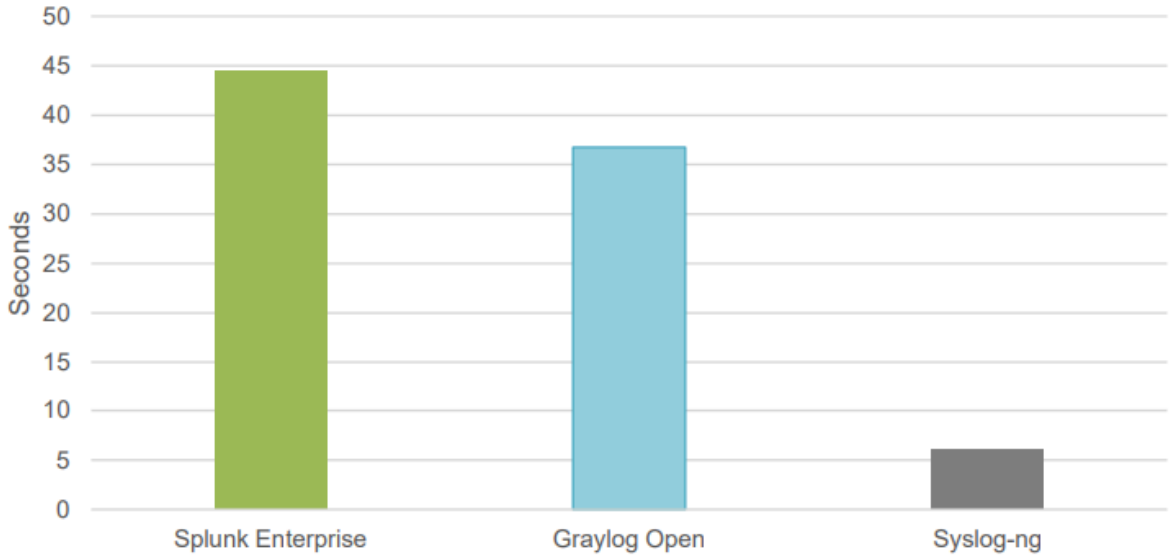


Рис. 2.3 Середнє значення MTTD для Splunk, Graylog та Syslog

MTTI охоплює процес аналізу інциденту після його виявлення: вивчення логів, співставлення подій, визначення масштабу та рівня ризику. На величину MTTI може впливати зручність інтерфейсу системи моніторингу, можливості фільтрації даних, наявність аналітичних інструментів і швидкість доступу до контекстної інформації. Оптимізація цього етапу дозволяє оперативніше приймати рішення про подальші дії щодо нейтралізації загрози.[2]

У сукупності MTTA, MTTD і MTTI формують повний час реагування на інцидент, тобто MTTR.

Таблиця 2.1

Порівняльна таблиця систем моніторингу подій

Критерії	Splunk Enterprise	Graylog Open	Syslog-ng
Архітектура та масштабування	Гнучка розподілена архітектура з можливістю горизонтального масштабування; підтримує багаторівневі індекси та кластеризацію даних	Підтримує горизонтальне масштабування через Elasticsearch; менш оптимізована при великих обсягах даних	Орієнтована на централізований збір логів; масштабування обмежене продуктивністю сервера
Інтерфейс та аналітика	Інтуїтивний веб-інтерфейс; розвинена аналітика, візуалізації та дашборди	Простий інтерфейс із базовою аналітикою; вимагає додаткових плагінів для	Відсутній графічний інтерфейс; аналітика реалізується зовнішніми засобами

		візуалізації	
Кореляція подій та автоматизація	Наявний механізм кореляційних правил, підтримка машинного навчання; інтеграція з SOAR	Підтримує власну мову запитів Graylog Pipeline Rules; обмежена автоматизація реагування	Переважно функція збору та маршрутизації; відсутність механізмів кореляції
Інтеграції	Можливість отримання інформацію з різних лжерел	Можливість отримання інформацію з різних лжерел	Сфокусована на syslog джерелах
Продуктивність при великих обсягах логів	Висока ефективність за рахунок індексації та розподілу навантаження; оптимізована для великих SOC	Середня продуктивність; можливе зниження швидкодії при великих потока	Висока швидкість збору логів, але без можливості складного аналізу
Середній MTTD	44.5 секунд	36.75 секунд	6 секунд
Середній MTTA	34,9 секунд	2 секунд	-

2.3 Splunk UBA: Аналіз поведінки користувачів

Splunk User Behavior Analytics (UBA) - це рішення, що спрямоване на виявлення загроз через моделювання та аналіз поведінки користувачів і сутностей. UBA доповнює збір та індексацію журналів алгоритмами машинного навчання, профілюванням, скормленими моделями послідовностей та механізмами ризикової оцінки, що дає можливість ідентифікувати аномалії, які пропускають сигнатурні системи. Splunk UBA поєднує поведінковий контекст із кореляцією подій, і це дозволяє перетворювати розрізнені індикатори у цілісні інцидентні ланцюжки, які потім ранжуються за ризиком.

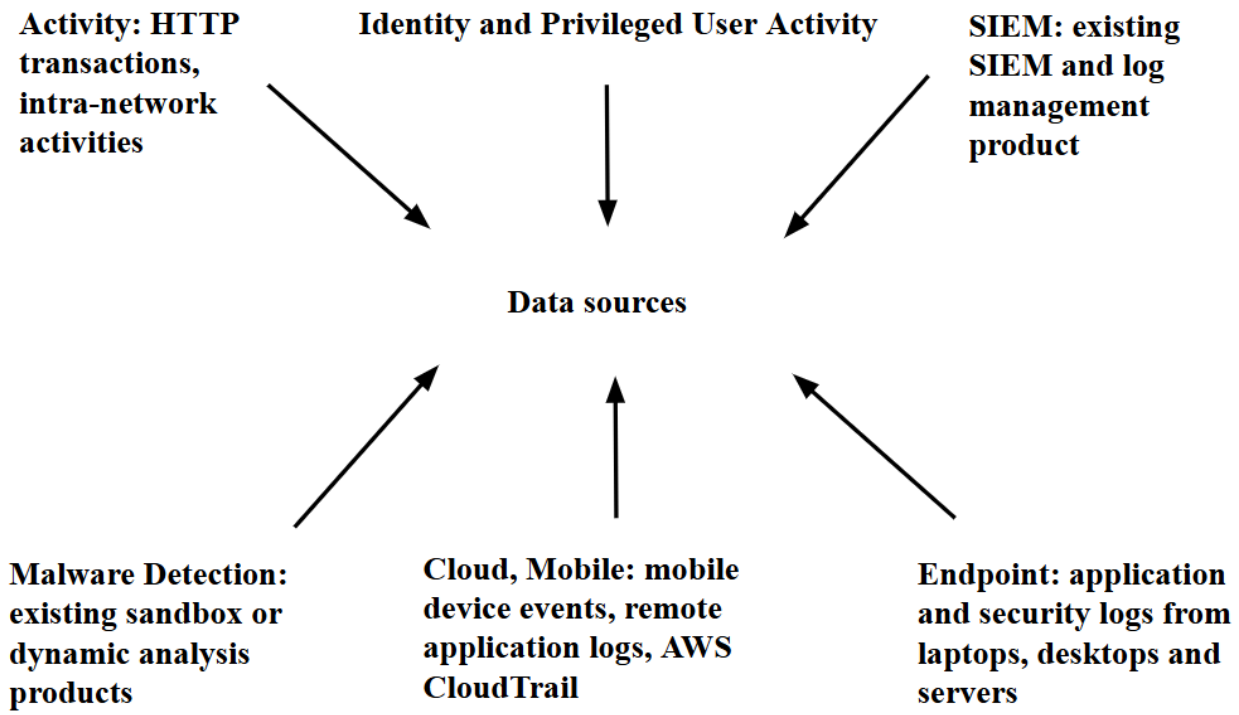


Рис. 2.4 Джерела отримання інформації для Splunk UBA

Splunk UBA може отримувати дані від таких джерел, як: журнали автентифікації , мережеві логи, телеметрія кінцевих пристроїв та журнали додатків. На рівні прийому даних відбувається нормалізація та збагачення подій. Далі поведінкові модулі будують індивідуальні профілі для кожного користувача/сутності і групують подібних користувачів у групи, що служать базою для подальшого виявлення контекстних аномалій.

Splunk UBA застосовує кілька взаємодоповнювальних підходів до аналітики

поведінки. Насамперед система формує базові лінії активності, тобто визначає, якими є типові дії конкретного користувача в різних контекстах його звичний час роботи, характер доступу до ресурсів, інтенсивність операцій. Після формування такого профілю будь яке відхилення, що суттєво вибивається із загальної картини, інтерпретується як потенційний індикатор компрометації. Також використовується аналіз “peer-group”, який дозволяє оцінювати поведінку користувача не лише відносно його власної історії, а й у порівнянні з типовою поведінкою групи співробітників зі схожими функціями або ролями в організації. Якщо дії користувача не відповідають очікуваним моделям, система позначає такі відхилення як нетипові.

Важливою складовою є також моделі, що враховують послідовність та часову логіку подій. У цьому випадку аналізується не окрема подія, а її місце в ланцюжку дій, включно з тим, наскільки природними є проміжки між ними. Завдяки цьому Splunk UBA може виявляти як порушення типової послідовності дій, так і часові відхилення, коли події відбуваються у нетиповий для користувача момент. Доповнює ці можливості використання алгоритмів машинного навчання зокрема автоенкодерів та інших нейронних підходів, що дають змогу аналізувати багатовимірні простори ознак. Такі моделі здатні фіксувати складні та слабко виражені відхилення, які не виявляються традиційними статистичними або порівняльними методами. [16]

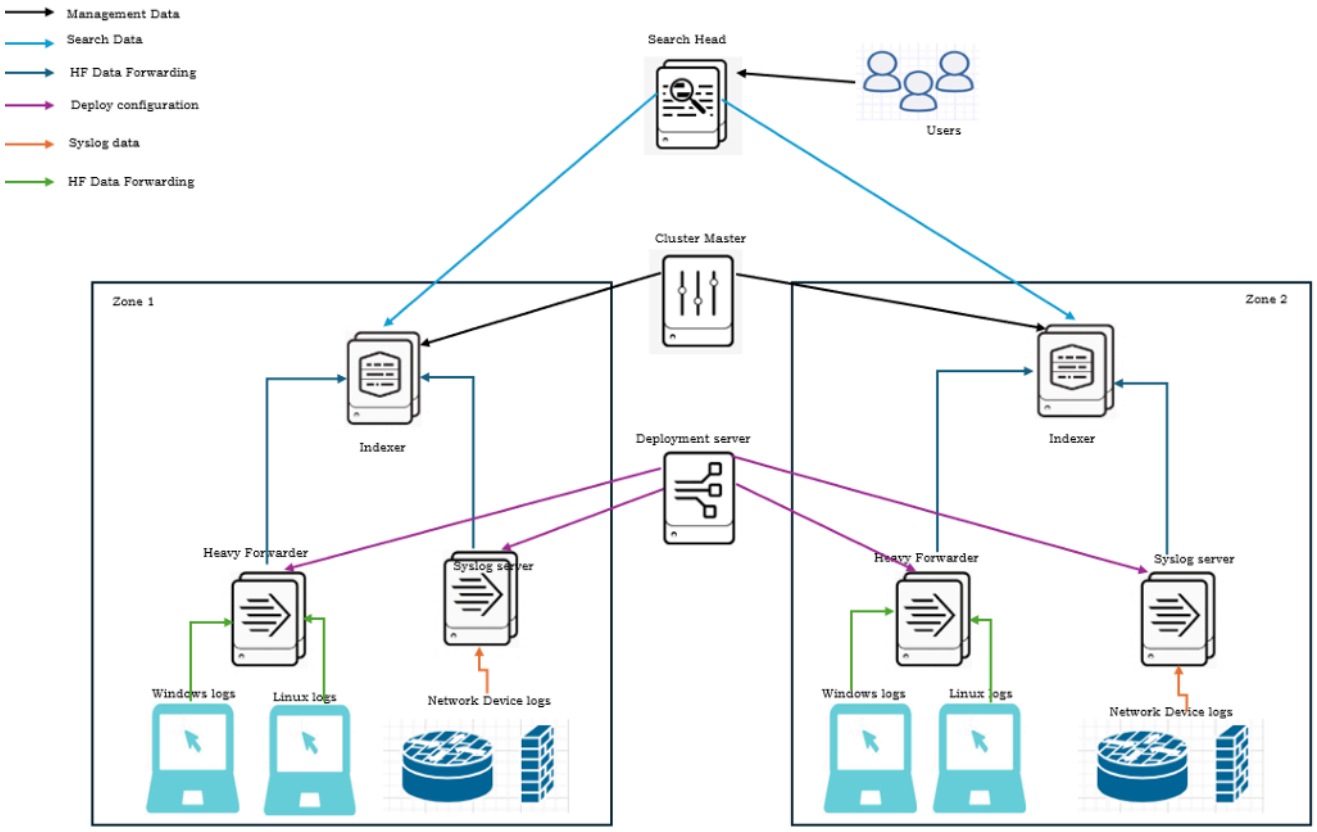


Рис. 2.5 Архітектурний дизайн Splunk Enterprise

У практичному застосуванні Splunk UBA ключовими є два аспекти: якісна побудова ознак та контроль над помилковими спрацюваннями. Хоча платформа містить набір готових кореляційних правил і поведінкових шаблонів, ефективність виявлення значною мірою залежить від коректного налаштування порогів ризику, часових інтервалів та логіки поділу користувачів на peer-групи. Таке налаштування зменшує рівень хибних сигналів і забезпечує більш релевантні сповіщення. Для надання ширшого контексту кожному інциденту Splunk UBA автоматично збагачує події додатковими відомостями: останніми діями користувача, пов’язаними мережевими подіями, змінами ролей і дозволів. Це спрощує роботу аналітиків на етапі первинного сортування інцидентів і прискорює перехід до детального розслідування.[14]

Splunk Enterprise Security та SOAR-платформами дозволяє реалізовувати автоматизовані сценарії реагування. Після досягнення певного рівня ризику система може автоматично створити інцидент у сервісних системах ITSM, виконати ескалацію, ізолювати підозрілу сесію або запустити багатокрокове

розслідування за заздалегідь визначеним алгоритмом. Завдяки цьому час реагування на інциденти суттєво скорочується, а моніторинг переходить від пасивного спостереження до активних оборонних дій. Водночас перед увімкненням автоматизації важливо оцінити рівень хибнопозитивних сповіщень, щоб уникнути надмірного або некоректного втручання.[14]

Повноцінна робота Splunk UBA потребує якісного та достатнього обсягу телеметрії - відсутність окремих типів логів або слабке покриття інфраструктури значно знижує ефективність виявлення аномалій. Поведінкові моделі вимагають періодичного оновлення, особливо коли змінюються бізнес-процеси, сезонні тенденції, ролі користувачів чи організаційна структура. Ефективне впровадження UEBA у великих інфраструктурах також потребує політик щодо управління даними, контролю доступу до журналів, а також незалежного аудиту коректності використання поведінкових профілів, щоб уникнути зловживань.

2.4 Відповідність технології SIEM вимогам ISO/NIST

Використання SIEM дозволяє створити багаторівневий підхід до моніторингу подій безпеки, що відповідає ключовим контролям ISO/IEC 27001 та рекомендаціям NIST. UEBA забезпечує поведінкову аналітику, формує профілі користувачів і виявляє аномалії, тоді як SIEM виконує централізований збір журналів, кореляцію подій і ініціює процес реагування на інциденти.

У сукупності ці технології повністю покривають вимоги контролів до журналювання, моніторингу, управління інцидентами, контролю доступу, а також виявлення скомпрометованих облікових записів.

У контексті NIST Cybersecurity Framework рішення SIEM одночасно охоплює етапи Identify, Detect і Respond:

● Identify - ідентифікація активів, критичних облікових записів та ризикових поведінкових патернів.

● Detect - побудова поведінкових моделей, лог-аналітика, кореляційні правила, машинне навчання.

● Respond - автоматичні дії, ескалація інцидентів, блокування сесій, виконання playbooks.

У контексті стандарту ISO/IEC 27001 використання SIEM забезпечує виконання ключових вимог щодо управління інформаційною безпекою, зокрема в частині контролю доступу, журналювання подій та управління інцидентами безпеки:

● Управління активами та доступом – ідентифікація інформаційних активів, критичних облікових записів, ролей користувачів і ризикових поведінкових патернів, що відповідає вимогам контролів щодо управління активами та контролю доступу.

● Моніторинг та журналювання подій безпеки – централізований збір журналів, побудова поведінкових моделей, лог-аналітика, застосування кореляційних правил і методів машинного навчання для виявлення аномалій та ознак компрометації облікових даних, що відповідає вимогам контролів щодо журналювання та моніторингу.

● Управління інцидентами інформаційної безпеки – автоматизація реагування, ескалація інцидентів, блокування сесій або облікових записів, а також виконання попередньо визначених сценаріїв реагування (playbooks), що відповідає вимогам стандарту щодо своєчасного реагування та обробки інцидентів.

Таблиця 2.2

Картка контролю Splunk Enterprise

Стандарт	Вимоги	Реалізація в Splunk Enterprise	Практична реалізація
ISO/IEC 27001	Реєстрація подій; моніторинг активності; захист журналів; виявлення інцидентів та реагування	Централізований збір та нормалізація логів; кореляційні правила; зберігання й захист журналів; створення алертів	Аналіз логів, кореляція; профілювання поведінки
NIST SP 800-92	Організація процесів логування; забезпечення цілісності журналів; визначення відповідальних	Парсинг; ротація; контроль цілісності; політики зберігання та агрегування журналів	Побудова передачі та нормалізація логів; контроль структур та цілісності журналів
NIST SP 800-53 AU	Повний аудит дій користувачів; журналювання критичних змін; аудит доступу; контроль привілеїв	Аудит логів; моніторинг адміністративних подій; контроль доступу до журналів, аудит змін у системах	Виявлення аномалій; контроль доступу до критичних систем

NIST SP 800-53 IA	Моніторинг автентифікації; виявлення підозрілих входів; управління обліковими записами	Кореляція подій; автоматизовані правила блокування; перевірка узгодженості даних	Моделювання профілів входу; виявлення аномалії; аналіз послідовностей підозрілих дій
NIST SP 800-53 IR	Виявлення інцидентів; збір контексту; документування; підтримка процесу реагування	Автоматичне створення інцидентів;інтеграція з SOAR/ITSM-процесами; кореляція подій	UEBA-тригери інцидентів; формування подій; аналітика для етапу розслідування
NIST CSF (Identify, Detect, Respond)	Виявлення аномалій; реагування на інциденти	Кореляція правил; створення алертів; запуск робочих процесів реагування	Кореляційні правила; поведінкові моделі

3 РОЗРОБКА ТА ОЦІНКА ТЕХНОЛОГІЇ ВИЯВЛЕННЯ СКОМПРОМЕТОВАНИХ ІДЕНТИФІКАЦІЙНИХ ДАНИХ

3.1 Практичне впровадження Splunk

В межах практичної частини роботи було реалізовано прототип технології виявлення скомпрометованих ідентифікаційних даних на основі аналізу аномальної поведінки користувачів із використанням платформи Splunk Enterprise. Система включає в себе:

- Linux сервер, на якому розгорнуто Splunk Enterprise для аналізу логів та Splunk Universal Forwarder для збору логів.
- Користувач Linux в одній підмережі з Linux сервер.
- Користувач Windows, що знаходиться в іншій підмережі.

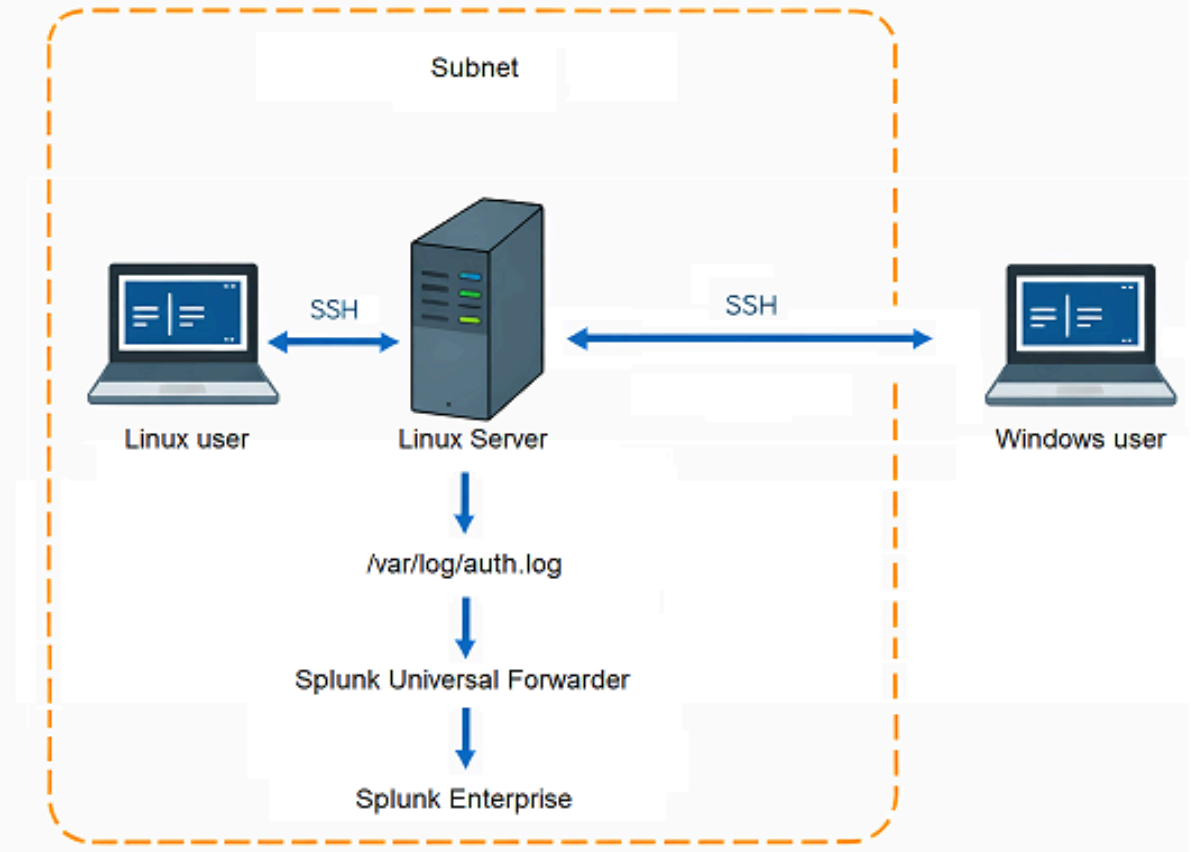


Рис. 3.1 Схема розгорнутої системи з Splunk Enterprise

Splunk Enterprise було розгорнуто у вигляді контейнера Docker, що забезпечило швидке встановлення, керованість сервісу та спрощене адміністрування.

Для збору подій із операційної системи Linux застосовувався Splunk Universal Forwarder, який було встановлено на сервері та налаштовано для автоматичного запуску разом із системою. Forwarder здійснював збір журналів аутентифікації, зокрема файлу /var/log/auth.log, та передавав їх до Splunk Enterprise через виділений порт 9997.

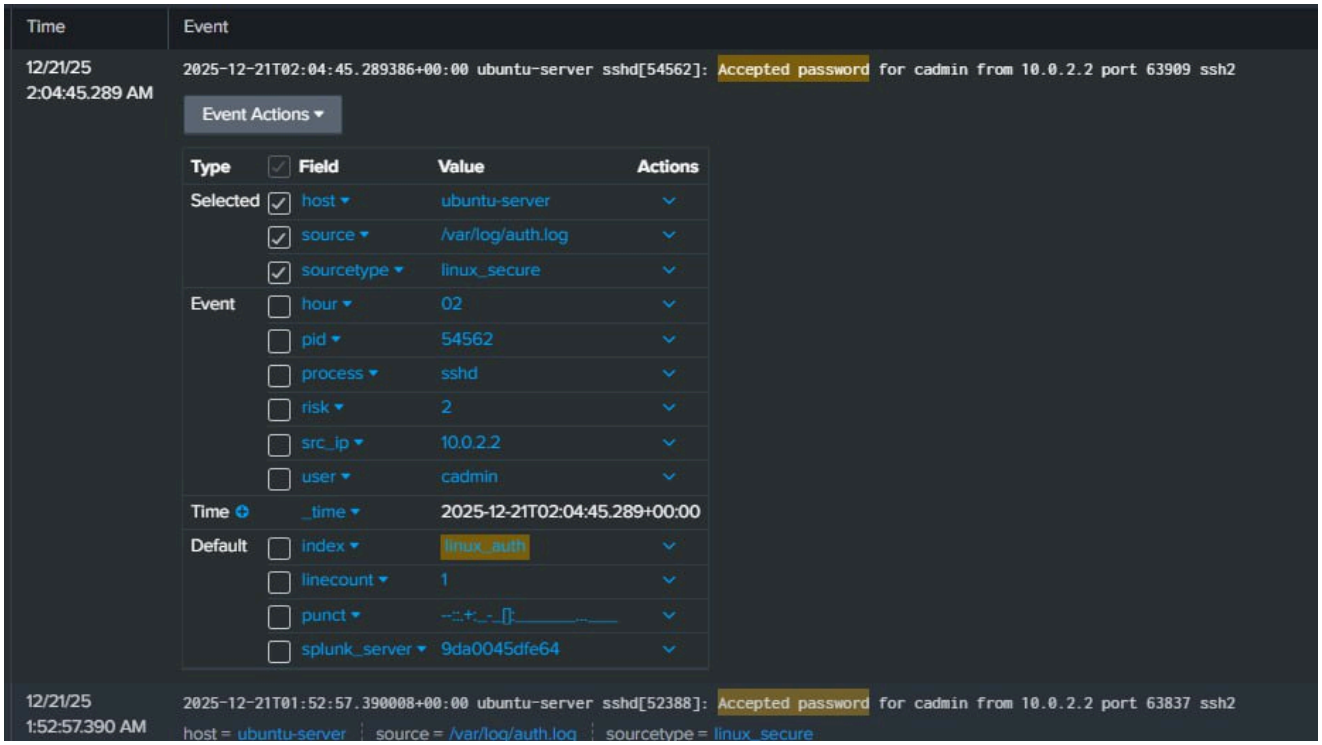


Рис. 3.2 Приклад звичайного підключення в auth.log

Для збереження та обробки подій було створено окремий індекс linux_auth для відокремлення журналу автентифікації від інших типів даних та оптимізувати подальший пошук і кореляцію. На основі зібраних логів реалізовано пошукові запити, спрямовані на виявлення успішних SSH-підключень та витяг ключових атрибутів подій, таких як ім’я користувача, джерельна IP-адреса та час входу.

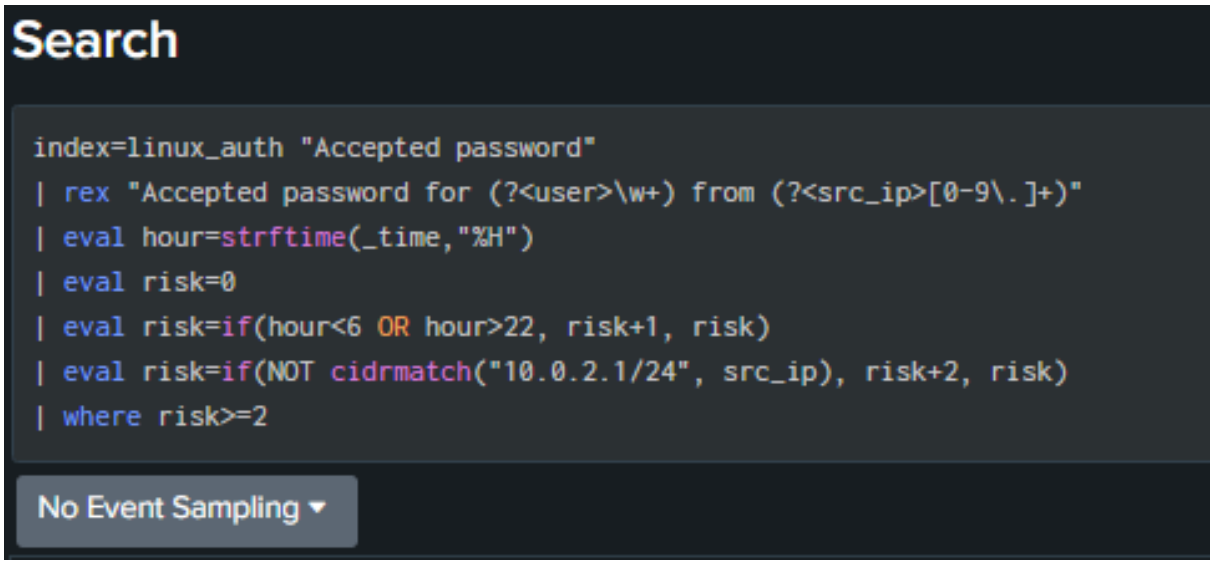


Рис. 3.3 Запиту для пошуку підключень по ssh, що підпадають під умови

У межах практичного сценарію було реалізовано механізм оцінювання ризику поведінки користувача. Для цього використовувався підхід накопичення ризикових ознак, зокрема входи у нетиповий час, підключення з незвичних IP-адрес. На основі сукупності цих факторів формувався інтегральний показник ризику(risk), який дозволяв відокремлювати стандартну поведінку користувача від потенційно скомпрометованої.

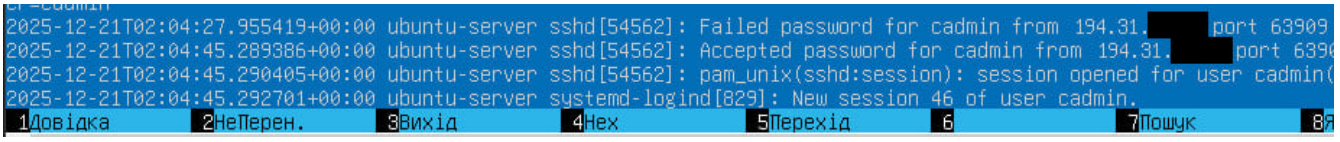


Рис. 3.4 Інформація про підключення в auth.log

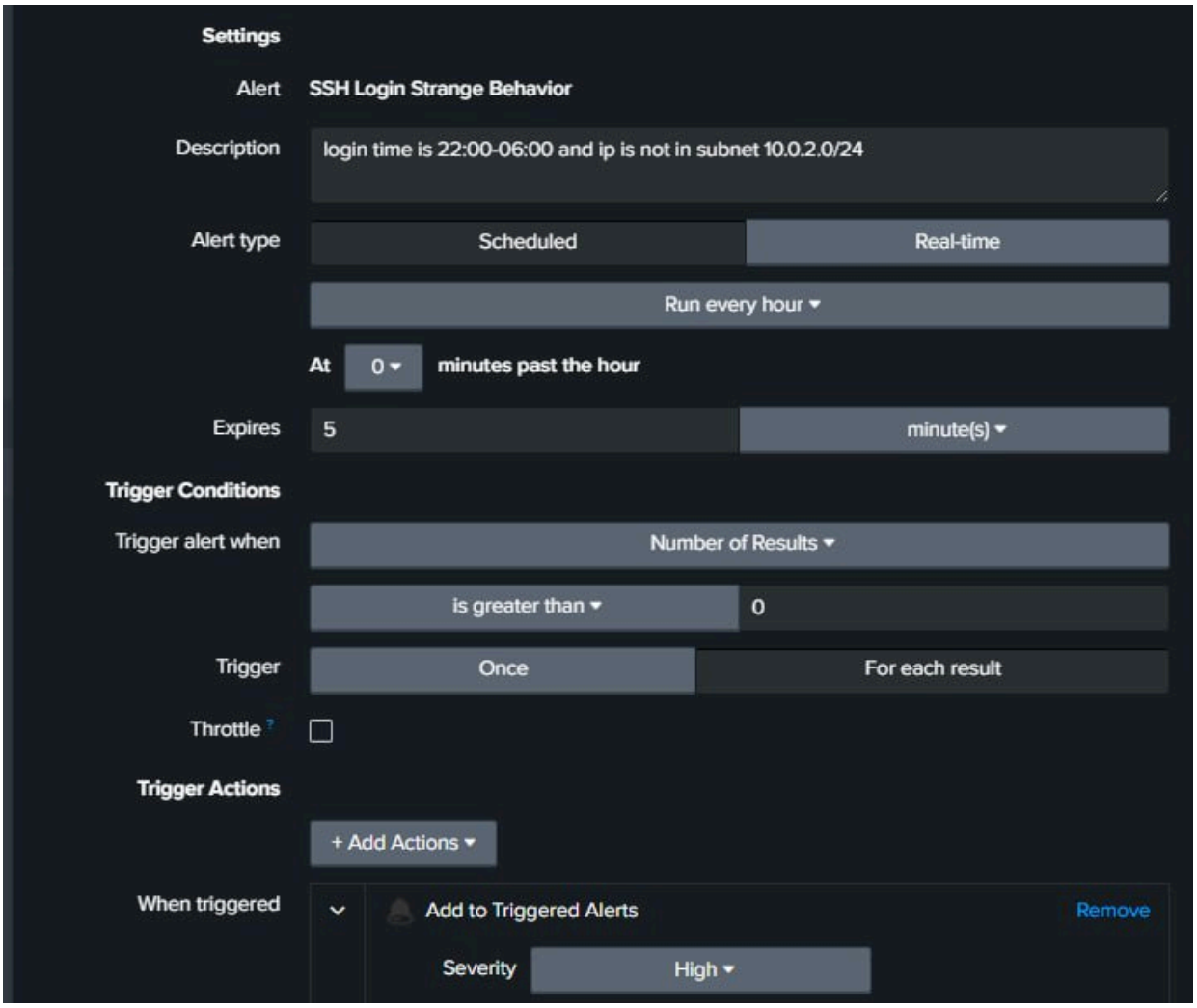


Рис. 3.5 Налаштування сповіщення

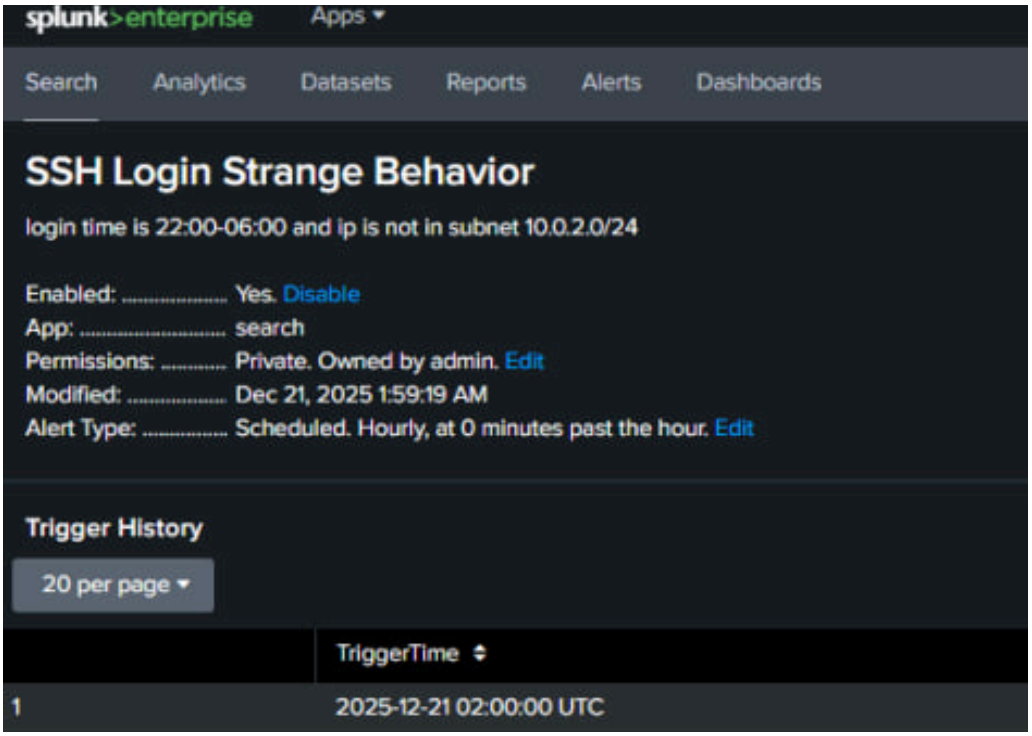


Рис. 3.6 Спрацювання сповіщення на основі запиту

При перевищенні заданого порогового значення ризику система генерує сповіщення у вигляді alert, що дозволяє оперативно реагувати на підозрілі події безпеки.

3.2 Оцінка результатів реагування на події

Ефективності впровадженої технології виявлення скомпрометованих ідентифікаційних даних визначалась на основі аналізу здатності системи своєчасно і коректно виявляти відхилення від типової поведінки користувачів, а також забезпечувати оперативне інформування про потенційні інциденти інформаційної безпеки.

У процесі тестування були змодельовані різні сценарії автентифікації, що охоплювали як легітимну активність користувачів, так і нетипові дії, характерні для компрометації облікових записів. Було розглянуто підключення по SSH у неробочий час, автентифікації з альтернативних або раніше нехарактерних IP-адрес. Результати експериментів засвідчили, що використання кореляційних правил у поєднанні з часовими вікнами та елементарними поведінковими моделями дозволяє ефективно виявляти аномальні патерни доступу без застосування жорстко фіксованих сигнатур.

На відміну від традиційних rule-based методів, де кожна подія розглядається ізольовано, реалізована логіка ризик-орієнтованого аналізу базується на накопиченні ознак та обчисленні сукупного ризикового показника. Це дає змогу гнучко налаштовувати чутливість системи та зменшувати кількість хибнопозитивних спрацювань.

Завдяки автоматичній генерації сповіщень після досягнення визначеного порогу ризику та коректності налаштування сповіщень значно скорочується часовий інтервал між появою підозрілої активності та її виявленням аналітиком. Це безпосередньо впливає на зменшення показника MTTR, який є одним із

ключових індикаторів ефективності процесів реагування на інциденти в сучасних SOC.

В порівнянні з ручним аналізом логів, автоматизований підхід дозволяє перейти від реактивної до проактивної моделі кіберзахисту. Водночас треба зауважити, що точність і повнота детекції значною мірою залежать від якості та різноманітності телеметрії. Обмеження аналізу виключно журналами автентифікації дозволяє виявляти лише початкові етапи компрометації, але не забезпечує достатнього контексту для ідентифікації складніших сценаріїв атак, зловживання привілеями і т.б.

Таким чином, результати експериментального впровадження підтверджують доцільність використання платформ SIEM для підвищення ефективності виявлення скомпрометованих облікових записів. Разом із тим вони є необхідність подальшого розвитку системи за рахунок розширення джерел даних і застосування складніших аналітичних моделей.

3.3 Відповідність впровадженої технології до стандартів ISO\NIST

Впровадження системи виявлення скомпрометованих ідентифікаційних даних на основі платформи Splunk Enterprise повинно оцінюватися не лише з точки зору технічної ефективності, але й з позиції відповідності міжнародним стандартам у сфері інформаційної безпеки.

Відповідність стандарту ISO/IEC 27001

Стандарт ISO/IEC 27001 визначає вимоги до системи управління інформаційною безпекою (ISMS) та орієнтований на ризик-орієнтований підхід до захисту інформаційних активів. Запропонована технологія безпосередньо підтримує низку контрольних заходів, визначених у додатку **A** стандарту.

Зокрема, у контексті контролів **A.5** - організаційні заходи безпеки та **A.8** - управління активами впроваджена система забезпечує централізований облік та моніторинг подій доступу до критичних ресурсів. Журнали автентифікації

користувачів розглядаються як інформаційні активи, для яких визначено правила збору, зберігання та аналізу.

Контроль **A.9** - управління доступом реалізується через моніторинг фактичного використання облікових записів. Поведінковий аналіз дозволяє виявляти ситуації, коли доступ формально дозволений, але контекст його використання відрізняється від нормального. Таким чином, система компенсує обмеження класичних механізмів контролю доступу, які не враховують поведінкові фактори.

Особливу роль відіграє відповідність контролям **A.12.4** - логування та моніторинг. Splunk Enterprise забезпечує централізований збір логів, їх кореляцію та довгострокове зберігання, що відповідає вимогам стандарту щодо трасованості подій і можливості проведення аудиту. Автоматизовані кореляційні правила та сповіщення реалізують вимогу постійного моніторингу безпеки інформаційних систем.

У межах контролів **A.16** - управління інцидентами інформаційної безпеки реалізована технологія підтримує раннє виявлення інцидентів та їх класифікацію на основі ризикового скорингу. Автоматичні сповіщення сприяють своєчасному реагуванню та документуванню інцидентів, що є ключовим елементом зрілої ISMS.

Таким чином, впроваджене рішення узгоджується з концепцією ISO/IEC 27001, оскільки не лише виявляє технічні події, а й інтегрується в загальний процес управління ризиками інформаційної безпеки.

Відповідність рекомендаціям NIST

У контексті функції Identify впроваджена система сприяє ідентифікації ризиків, пов’язаних із компрометацією облікових записів. Аналіз історичних даних автентифікації дозволяє формувати уявлення про нормальні шаблони поведінки користувачів і визначати потенційно вразливі облікові записи.

Функція Protect реалізується опосередковано через підвищення прозорості використання облікових даних. Хоча система не запобігає атаці безпосередньо,

вона створює умови для швидкого виявлення зловживань доступом, що зменшує потенційні наслідки компрометації.

Головна відповідність даної технології відповідно стандартам є Detect, яка є ключовою для UEBA-підходів. Згідно з NIST SP 800-92, ефективна система журналювання має забезпечувати не лише збір логів, але й їх аналітичну обробку. Реалізовані кореляційні запити, часові вікна та ризиковий скоринг відповідають цим вимогам і дозволяють виявляти аномальні події в режимі, близькому до реального часу.

Функції Respond та Recover підтримуються через механізми сповіщень і подальшого аналізу інцидентів. Автоматизовані сповіщення скорочують час реагування, а збереження історичних даних дозволяє виконувати ретроспективний аналіз та вдосконалювати правила детекції. Це відповідає рекомендаціям NIST SP 800-61 щодо управління інцидентами інформаційної безпеки.

Загалом можна зробити висновок, що впроваджена технологія виявлення скомпрометованих ідентифікаційних даних відповідає ключовим положенням міжнародних стандартів ISO/IEC 27001 та рекомендацій NIST. Вона забезпечує реалізацію принципів ризик-орієнтованого підходу, безперервного моніторингу та своєчасного реагування на інциденти.

Разом із тим варто зазначити, що повна відповідність стандартам досягається лише за умови поєднання технічних засобів із організаційними та процедурними заходами. Запропоноване рішення слід розглядати як складову загальної системи управління інформаційною безпекою, яка має бути доповнена політиками доступу, регламентами реагування та регулярним аудитом.

3.4 Рекомендації щодо застосування Splunk в корпоративну мережу

На основі отриманих результатів дослідження та практичного впровадження можна сформулювати низку рекомендацій щодо інтеграції підходів UEBA та SIEM у реальну корпоративну мережу. Першочерговим кроком має стати забезпечення централізованого збору телеметрії з різнорівневих джерел, включаючи системи

автентифікації, сервери прикладних сервісів, мережеві пристрої та кінцеві хости. Саме різноманітність і повнота даних дозволяють формувати багатовимірні поведінкові профілі користувачів, що є ключовою умовою ефективного виявлення аномалій.

Рекомендується впроваджувати ризико-орієнтований підхід до детекції інцидентів, за якого рішення про потенційну компрометацію приймається на основі сукупності ознак. Такий підхід відповідає сучасним концепціям NIST Cybersecurity Framework і стандарту ISO/IEC 27001, які наголошують на необхідності контекстного аналізу та адаптивного управління ризиками. Застосування поведінкових профілів дозволяє системі поступово адаптуватися до змін у робочих процесах і зменшувати кількість помилкових спрацювань.

Також важливим аспектом є управління хибно-позитивними спрацюваннями. Для цього доцільно налаштовувати часові вікна аналізу, пороги ризику та механізми peer-group аналізу, які дозволяють порівнювати поведінку користувача з групою подібних ролей або функцій. Перед впровадженням автоматизованих сценаріїв реагування рекомендовано проводити поетапне тестування, що дає змогу уникнути блокування легітимної активності та негативного впливу на внутрішні процеси.

Впровадження UEBA має супроводжуватися також організаційними та нормативними заходами. Зокрема, необхідно визначити політики доступу до журналів подій, регламентувати використання поведінкових профілів і забезпечити дотримання вимог щодо захисту персональних даних. Це особливо актуально в контексті аналізу активності користувачів, де важливо дотримуватися принципів мінімізації даних і прозорості обробки.

У комплексі зазначені рекомендації дозволяють інтегрувати UEBA та SIEM у загальну систему управління інформаційною безпекою організації для підвищення рівня захищеності ідентифікаційних і зменшити ризики, пов’язані з компрометацією ідентифікаційних даних.

ВИСНОВКИ

У роботі було досліджено проблему виявлення скомпрометованих ідентифікаційних даних у корпоративних мережах, яка є однією з загроз сучасної інформаційної безпеки. Аналіз теоретичних підходів і практичних рішень, а саме обмежену ефективність звичайних методів на основі сигнатурні та rule-based механізмів у випадку атак, які маскуються під легітимну активність користувачів.

У межах практичної частини було реалізовано технологію моніторингу та аналізу подій на основі платформи Splunk Enterprise з елементами поведінкової аналітики. Налаштований процес збору та аналізу журналів автентифікації, що дозволило сформувати базову модель нормальної поведінки користувачів і виявляти відхилення, пов’язані з нетиповими часами доступу та альтернативними джерелами підключення. Запроваджений ризик-орієнтований підхід до детекції інцидентів підтвердив свою ефективність у зменшенні кількості хибнопозитивних спрацювань.

Оцінка результатів реагування показала, що автоматизація процесів виявлення та сповіщення суттєво скорочує час реагування на інциденти і сприяє зниженню показника MTTR. Разом із тим треба зазначити про необхідність розширення набору джерел телеметрії та застосування більш складних моделей аналізу для виявлення багатоступеневих сценаріїв атак.

Отримані результати підтверджують доцільність використання SIEM-платформ для підвищення рівня захищеності облікових записів у корпоративних мережах. Запропоновані рекомендації можуть бути використані як основа для подальшого впровадження та розвитку систем моніторингу безпеки в реальних організаціях.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cybersecurity threat detection based on a UEBA framework using Deep Autoencoders / J. Fuentes et al. *AIMS mathematics*. 2025. Vol. 10, no. 10. P. 23496–23517. URL: https://doi.org/10.3934/math.20251043 (date of access: 22.11.2025).
2. Dahlberg G. Exploring incident management: A comparative study of splunk enterprise, graylog open and syslog-ng and their impact on mean time to resolution (MTTR). 2025. URL: https://su.diva-portal.org/smash/get/diva2:1970735/FULLTEXT01.pdf.
3. ENISA threat landscape 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
4. Eren M. E., Moore J. S., Alexandro B. S. Multi-Dimensional anomalous entity detection via poisson tensor factorization. *2020 IEEE international conference on intelligence and security informatics (ISI)*, Arlington, VA, USA, 9–10 November 2020. 2020. URL: https://doi.org/10.1109/isi49825.2020.9280524 (date of access: 22.11.2025).
5. ISO/IEC 27001. Системи керування інформаційною безпекою. Чинний від 2023-08-17. Вид. офіц. 2023
6. ISO/IEC 27002. Заходи забезпечення інформаційної безпеки. Чинний від 2024-01-09. Вид. офіц. 2024
7. Javed M. Detecting credential compromise in enterprise networks. 2016. URL: http://www2.eecs.berkeley.edu/Pubs/TechRpts/2016/EECS-2016-216.pdf.
8. Carlos Arcila Investigations Report: Alarming surge in cyberattacks through third-parties.2025. URL: https://www.verizon.com/about/news/2025-data-breach-investigations-report.
9. NIST SP 800-61. Computer security incident handling guide. Effective from 2012-07-01. Official edition.
10. NIST SP 800-92. Guide to computer security log management. Effective from 2006-09-01. Official edition.
11. Phillips J. A., McElwain C. M., Clemmer K. W. Metacognitive training in professional development can improve and sustain student achievement. URL: https://arxiv.org/pdf/1607.07856.
12. Protocols for checking compromised credentials / L. Li et al. *CCS '19: 2019 ACM SIGSAC conference on computer and communications security*, London United Kingdom. New York, NY, USA, 2019. URL: https://doi.org/10.1145/3319535.3354229 (date of access: 22.11.2025).
13. Rabzelj M., Sedlar U. Beyond the leak: analyzing the real-world exploitation of stolen credentials using honeypots. *Sensors*. 2025. Vol. 25, no. 12. P. 3676. URL: https://doi.org/10.3390/s25123676 (date of access: 22.11.2025).

14. Shelke P., Frantti T. Exploring the possibilities of splunk enterprise security in advanced cyber threat detection. *International conference on cyber warfare and security*. 2025. Vol. 20, no. 1. P. 605–613. URL: https://doi.org/10.34190/iccws.20.1.3326 (date of access: 22.11.2025).
15. Skendzic A., Kovacic B., Balon B. Management and monitoring security events in a business organization - SIEM system. *2022 45th jubilee international convention on information, communication and electronic technology (MIPRO)*, Opatija, Croatia, 23–27 May 2022. 2022. URL: https://doi.org/10.23919/mipro55190.2022.9803428 (date of access: 22.11.2025).
16. Splunk user behavior analytics. URL: https://www.splunk.com/en_us/pdfs/fact-sheets/splunk-user-behavior-analytics.pdf.
17. Anomaly detection in log-event sequences: A federated deep learning approach and open challenges / P. Himler et al. *EICC 2024: Austrian Institute of Technology, Giefinggasse 4, Vienna, 1220, Austria*, 2024. URL: https://www.skopik.at/ait/2024_mlwa.pdf (date of access: 22.11.2025).
18. Zhang L., Thing V. L. L. Three decades of deception techniques in active cyber defense - Retrospect and outlook. *Computers & security*. 2021. Vol. 106. P. 102288. URL: https://doi.org/10.1016/j.cose.2021.102288 (date of access: 22.11.2025).
19. Zhao Z., Xu C., Li B. A lstm-based anomaly detection model for log analysis. *Journal of signal processing systems*. 2021. Vol. 93, no. 7. P. 745–751. URL: https://doi.org/10.1007/s11265-021-01644-4 (date of access: 22.11.2025).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ

Кваліфікаційна робота
на тему:

«Технологія виявлення скомпрометованих ідентифікаційних даних в корпоративній мережі на базі Splunk»

Виконав: СПІВАК Ілля, БСДМ-63
Керівник: СОБЧУК Андрій д.ф., доцент

Об'єкт дослідження: процес забезпечення кібербезпеки корпоративних інформаційних ресурсів організації.

Предмет дослідження: методи та засоби виявлення скомпрометованих облікових даних у корпоративних мережах на основі систем моніторингу подій безпеки.

Мета роботи: дослідити та проаналізувати підходи до виявлення скомпрометованих облікових даних у корпоративних мережах.

Наукові завдання:

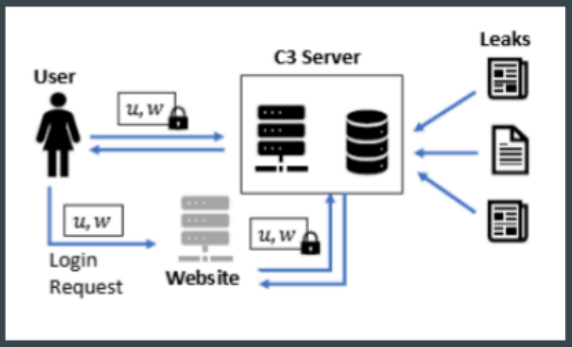
- дослідити сутність проблеми компрометації облікових даних у корпоративних інформаційних системах;
- проаналізувати сучасні тенденції та вектори атак, пов'язані з використанням скомпрометованих облікових записів;
- проаналізувати підходи до виявлення компрометації облікових даних на основі моніторингу подій безпеки;
- дослідити функціональні можливості SIEM-систем щодо виявлення та реагування на інциденти безпеки;

Дослідження проблеми виявлення скомпрометованих ідентифікаційних даних

Сучасні процеси цифрової трансформації суттєво змінюють підходи до побудови та захисту корпоративних інформаційних систем. Широке впровадження хмарних сервісів, віддаленого доступу, гібридних робочих моделей, систем єдиного входу та мобільних платформ призводить до зростання складності IT-інфраструктури та розширення поверхні атаки.

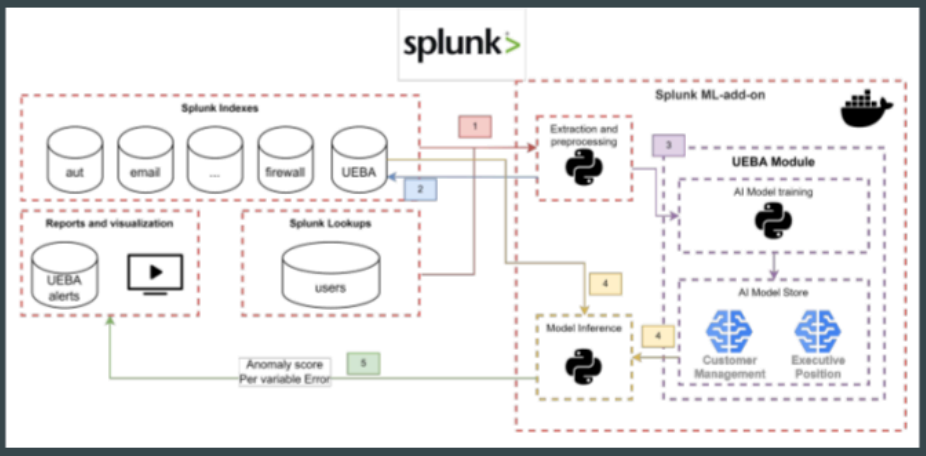
За даними компанії Verizon за 2025 рік найбільш розповсюдженим вектором атаки було використання скомпрометованих ідентифікаційних даних. Що є показником важливості проблеми виявлення та запобігання такій загрозі.

Методи виявлення скомпрометованих ідентифікаційних даних



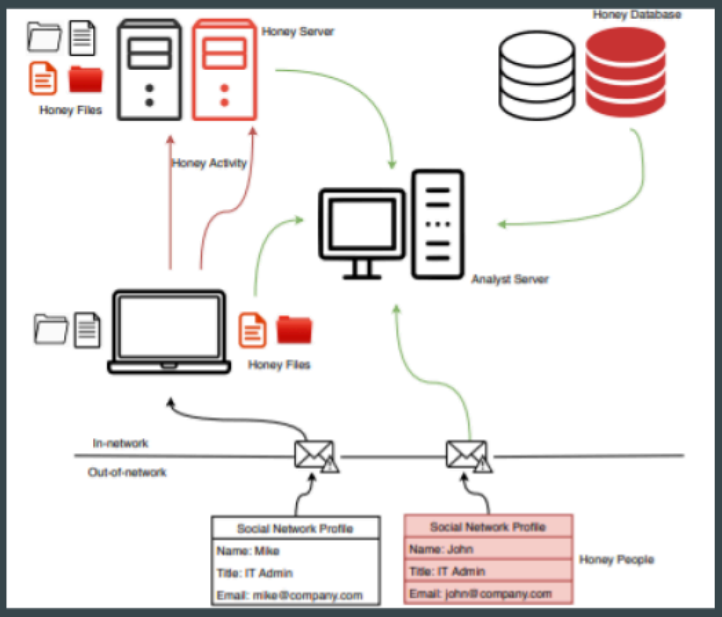
Моніторинг витоків облікових даних - це одним із методів виявлення використання скомпрометованих пар логінів і паролів до моменту їх експлуатації зловмисниками.

Основною ідеєю таких систем є перевірка ідентифікаційних\облікових даних користувача на наявність у базах викрадених записів без розкриття самих паролів або іншої конфіденційної інформації.



Поведінковий аналіз користувачів та сутностей. Його основна мета полягає у виявленні відхилень від усталених моделей поведінки користувачів, системних процесів і мережевих об'єктів, що може свідчити про порушення безпеки навіть у разі відсутності явних сигнатур

Введення в оману - це стратегія активного захисту, що передбачає створення фіктивних об'єктів у цифровому середовищі з метою виявлення зловмисників або зміщення їхньої діяльності зі справжніх цілей. До таких об' єктів належать honeytokens - фальшиві ресурси, які не використовуються легітимними користувачами, а також decoy-облікові записи, які імітують справжні акаунти із правами доступу.



Аналіз існуючих рішень

Splunk Enterprise - комерційне SIEM-рішення, що забезпечує збір, нормалізацію, кореляцію та розширений аналіз подій безпеки з використанням машинного навчання. Платформа підтримує розвинуті механізми виявлення інцидентів, автоматизацію реагування та поведінкову аналітику користувачів, що робить її ефективним інструментом для SOC.

Graylog Open - відкрита платформа для централізованого збору, зберігання та пошуку журналів подій, яка надає базові можливості аналізу та візуалізації даних. Система підтримує створення правил сповіщень і дашбордів, проте не має вбудованих повноцінних механізмів UEBA та розширеної кореляції

Syslog-ng - система збору та маршрутизації журналів подій, призначена для централізованого прийому, фільтрації та зберігання логів з різних джерел. Рішення забезпечує високу продуктивність і гнучке налаштування потоків журналів, однак має обмежені можливості аналітики та кореляції подій без додаткових інструментів.

SIEM System	Mean MTTD (sec)	Median MTTD (sec)	Standard Deviation MTTD (sec)
Splunk Enterprise	60	62	7
	45	41	11
	30	29	14
	43	44	21
	44.5	44	13.25
Graylog Open	56	57	7
	24	21	21
	33	27	23
	34	26	20
	36.75	32.75	17.75
Syslog-ng	17	17	0
	3	2	2
	3	2	1
	1	1	0
Average	6	5.5	0.75

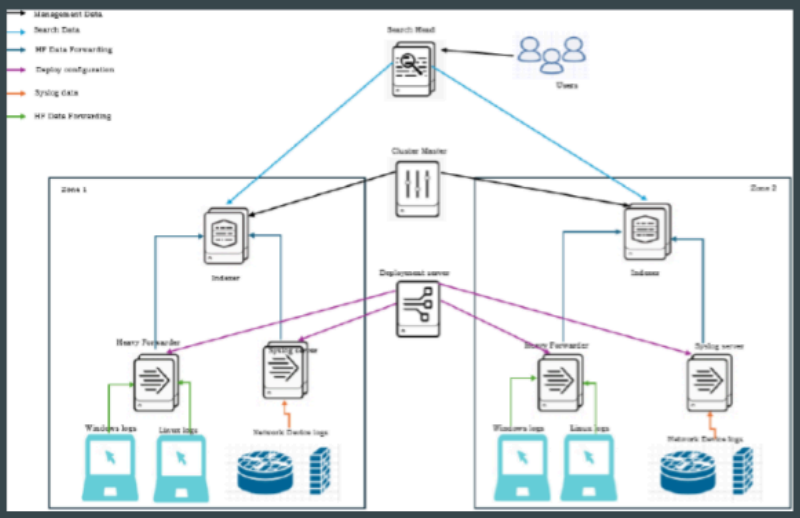
Також для більш детального порівняння цих рішень можна використати показник MTTR, що відображає мінімальний час потрібний на вирішення одного окремого інцидента.
MTTR складається з:

- MTTD - мінімальний час для виявлення
- MTTA - мінімальний час для усвідомлення
- MTTI - мінімальний час для розслідування

Призначення та основні функції Splunk Enterprise

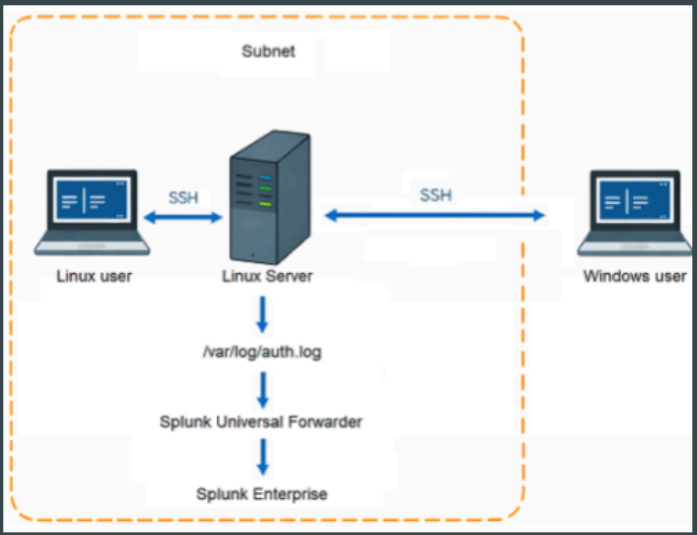
Splunk Enterprise є платформою призначеною для збору, індексації та аналітичної обробки машинних даних з системних журналів, мережевого трафіку, пристроїв безпеки, серверів і прикладних систем.
Основна концепція роботи полягає у створенні централізованого репозиторію подій, що дозволяє проводити кореляцію даних, аналіз інцидентів та побудову поведінкових моделей у реальному часі.

Архітектура Splunk Enterprise



- Рівень збору даних - відповідає за прийом потоків інформації з різних джерел.
- Рівень індексації та зберігання - отримані події обробляються і зберігаються в оптимізованому вигляді індексів.
- Аналітичний рівень - центральна складова платформи, яка дозволяє аналітикам використовувати Search Processing Language (SPL) для створення запитів, побудови дашбордів, створення попереджень і кореляційних правил.

Технологія застосування Splunk Enterprise



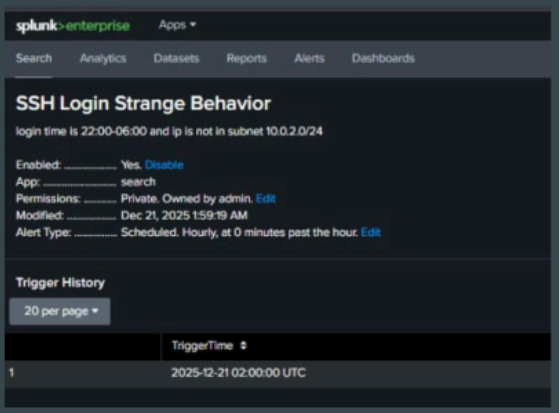
В межах практичної частини роботи було реалізовано прототип технології виявлення скомпрометованих ідентифікаційних даних на основі аналізу аномальної поведінки користувачів із використанням платформи Splunk Enterprise.
Система включає в себе:

- Linux сервер, на якому розгорнуто Splunk Enterprise для аналізу логів та Splunk Universal Forwarder для збору логів.
- Користувач Linux в одній підмережі з Linux сервер.
- Користувач Windows, що знаходиться в іншій підмережі.

Search

```
index=linux_auth "Accepted password"
| rex "Accepted password for (?<user>\w+) from (?<src_ip>[0-9\.]+)"
| eval hour=strftime(_time,"%H")
| eval risk=0
| eval risk=if(hour<6 OR hour>22, risk+1, risk)
| eval risk=if(NOT cidrmatch("10.0.2.1/24", src_ip), risk+2, risk)
| where risk>=2
```

На основі зібраних логів реалізовано пошукові запити, спрямовані на виявлення успішних SSH-підключень та витяг ключових атрибутів подій, таких як ім'я користувача, джерельна IP-адреса та час входу.
Також в запиті реалізовано механізм оцінювання ризику поведінки користувача. Для цього використовувався підхід накопичення ризикових ознак, зокрема входи у нетиповий час, підключення з незвичних IP-адрес.



На основі сукупності цих факторів формувався інтегральний показник ризику(risk), який дозволяв відокремлювати стандартну поведінку користувача від потенційно скомпрометованої. При перевищенні заданого порогового значення ризику система генерує сповіщення у вигляді alert, що дозволяє оперативно реагувати на підозрілі події безпеки.

Рекомендації щодо застосування Splunk Enterprise

Основними рекомендаціями щодо виявлення скомпрометованих ідентифікаційних даних є:

- Застосування більш ніж одного метода виявлення. Використання лише одного механізму контролюне забезпечує достатнього рівня надійності виявлення компрометації облікових даних. Тому доцільним є комбінування декількох підходів, таких як поведінковий аналіз активності користувачів, кореляція подій автентифікації, моніторинг зовнішніх джерел витоків даних та контроль аномальних параметрів доступу. Комплексне застосування методів підвищує ймовірність своєчасного виявлення скомпрометованих облікових записів.
- Автоматична генерація сповіщень. Системи моніторингу подій безпеки повинні автоматично формувати сповіщення при виявленні підозрілих дій. Автоматизація дозволяє суттєво скоротити час між появою інциденту та початком реагування, зменшуючи ризик подальшої експлуатації скомпрометованих облікових даних
- Аналіз в сукупності. Окремі події безпеки самі по собі не завжди свідчать про компрометацію облікових даних. Тому важливим є аналіз подій у сукупності з урахуванням контексту, часових залежностей та взаємозв'язків між різними джерелами даних. Кореляція подій дозволяє виявляти складні сценарії атак, які не можуть бути ідентифіковані за допомогою одиничних правил.

Висновки

У процесі тестування були змодельовані різні сценарії автентифікації, що охоплювали як легітимну активність користувачів, так і нетипові дії, що могли свідчити про компрометацію. Було розглянуто підключення по SSH у неробочий час, автентифікації з альтернативних або раніше нехарактерних IP-адрес. Результати засвідчили, що використання кореляційних правил у поєднанні з часовими вікнами та елементарними поведінковими моделями дозволяє ефективно виявляти аномальні патерни доступу без застосування жорстко фіксованих сигнатур.

Оцінка результатів реагування показала, що автоматизація процесів виявлення та сповіщення суттєво скорочує час реагування на інциденти і сприяє зниженню показника MTTR. Разом із тим треба зазначити про необхідність розширення набору джерел телеметрії та застосування більш складних моделей аналізу для виявлення багатоступеневих сценаріїв атак.