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: “ПЕРСПЕКТИВИ І ВИКЛИКИ ВИКОРИСТАННЯ МЕТОДІВ ШТУЧНОГО ІНТЕЛЕКТУ В СИСТЕМАХ ПОВЕДІНКОВОЇ АНАЛІТИКИ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою

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

_____ Максим САЙНІДІ

(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ-61

Керівник: Тетяна МУЖАНОВА, к.держ.упр., доцент

Рецензент:

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут кібербезпеки та захисту інформації

Кафедра Управління кібербезпекою та захистом інформації
Ступінь вищої освіти магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УКБЗІ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студенту Сайніді Максиму Сергійовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "Перспективи і виклики використання методів штучного інтелекту в системах поведінкової аналітики"

керівник кваліфікаційної роботи Тетяна МУЖАНОВА, к.держ.упр., доцент
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "30" жовтня 2025 р. №467.

2. Строк подання кваліфікаційної роботи "___" грудня 2025 р.
3. Вихідні дані до кваліфікаційної роботи: *кіберзагрози, системи поведінкової аналітики (UEBA), штучний інтелект в UEBA*.
4. Перелік питань, які потрібно розробити:
   1. Дослідити основні характеристики інструментів поведінкової аналітики.
   2. Порівняти сучасні рішення UEBA і надати пропозиції щодо їх застосування.
   3. З'ясувати роль штучного інтелекту як засобу розширення можливостей систем UEBA, запропонувати рекомендації щодо його використання для команд кібербезпеки.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання "02" жовтня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назви етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2025	
2.	Збір та аналіз літератури.	23.10.2025	
3.	Дослідження основних характеристик інструментів поведінкової аналітики.	27.10.2025	
4.	Порівняння сучасних рішень UEBA і надання пропозицій щодо їх застосування.	10.11.2025	
5.	З’ясування ролі штучного інтелекту як засобу розширення можливостей систем UEBA і формування рекомендацій	15.11.2025	
6.	Формулювання висновків за результатами дослідження.	22.11.2025	
7.	Оформлення роботи.	04.12.2025	
8.	Оформлення презентації.	14.12.2025	
9.	Отримання рецензії на роботу.	18.12.2025	
10.	Захист в ЕК.	__.01.2026	

Здобувач вищої освіти _____ Максим САЙНІДІ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(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 магістра

Направляється здобувач Сайніді М.С. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека та захист інформації
(код, найменування спеціальності)
освітньо-професійної програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Перспективи і виклики використання методів штучного інтелекту в системах поведінкової аналітики"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **САЙНІДІ Максим** у кваліфікаційній роботі дослідив основні характеристики інструментів поведінкової аналітики, порівняв сучасні рішення UEBA і надав пропозиції щодо їх застосування, з'ясував роль штучного інтелекту як засобу розширення можливостей UEBA, зокрема визначив проблеми і перспективи впровадження ШІ, запропонував рекомендації щодо його використання для команд кібербезпеки.

САЙНІДІ Максим показав належну теоретичну і практичну підготовку, здатність визначати і вирішувати науково-дослідницькі завдання. Кваліфікаційна робота оформлена згідно з вимогами. Виклад матеріалу здійснено логічно і послідовно, зроблено відповідні висновки. Ключові положення роботи представлено у вигляді рисунків і таблиць. Результати дослідження апробовані на конференції "Актуальні проблеми кібербезпеки" 29 жовтня 2025 року.

Все це дозволяє оцінити кваліфікаційну роботу здобувача **САЙНІДІ Максима** на оцінку "відмінно" та присвоїти йому кваліфікацію "Магістр з кібербезпеки та захисту інформації за освітньо-професійною програмою Управління інформаційною та кібернетичною безпекою".

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

"____" _____ 2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Сайніді М.В. 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 магістерську роботу

здобувача вищої освіти Сайніді Максима Сергійовича
на тему "Перспективи і виклики використання методів штучного інтелекту в системах поведінкової аналітики"

Актуальність. З огляду на безпрецедентне зростання кількості даних і темпів їх аналізу, а також неможливість їх обробки за допомогою традиційних ручних або автоматизованих методів галузь кібербезпеки загалом і поведінкова аналітика зокрема все ширше використовує алгоритми ШІ та МН. Сьогодні майже 70% організацій вже застосовують рішення на основі ШІ для виявлення і запобігання загрозам.

Інструменти UEBA на основі ШІ надають потужні можливості в галузі кібербезпеки, підвищуючи якість і швидкість усіх процесів. Однак, використання ШІ пов'язане теж і з певними проблемами й обмеженнями, які необхідно подолати.

З огляду на зазначене дослідження перспектив і викликів використання методів штучного інтелекту в системах поведінкової аналітики є актуальним науковим завданням.

Позитивні сторони

1. У роботі досліджено основні характеристики інструментів поведінкової аналітики, здійснено порівняльний аналіз сучасних рішень UEBA і надано пропозиції щодо їх застосування, з'ясовано роль ШІ як засобу розширення можливостей UEBA, зокрема визначено проблеми і тенденції його розвитку і запропоновано рекомендації щодо використання ШІ для команд кібербезпеки.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено послідовно згідно з планом роботи, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків. Автор опрацював близько 70 публікацій та електронних джерел, в тому числі англомовні наукові статті.

3. За результатами дослідження запропоновано рекомендації щодо застосування методів ШІ для команд кібербезпеки.

Недоліки

1. Доцільно було б приділити більше уваги вивченню і класифікації методів ШІ та МН, особливостям їх використання UEBA на основі ШІ у вітчизняних умовах.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач Сайніді Максим Сергійович заслуговує присвоєння кваліфікації "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною та кібернетичною безпекою".

Рецензент:

підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 93 с.., 22 рис., 3 табл., 69 джерел.

Метою роботи є дослідження перспектив і викликів використання методів штучного інтелекту в системах поведінкової аналітики.

Об'єктом дослідження є системи поведінкової аналітики (UEBA) як засоби виявлення і запобігання кіберзагрозам.

Предмет дослідження – перспективи і виклики використання методів штучного інтелекту в системах поведінкової аналітики.

Методи дослідження. Для вирішення завдань дослідження використано історичний, статистичний і прогностичний методи, методи аналізу та синтезу, порівняння, класифікації, моделювання, теорії поведінкової аналітики.

Короткий зміст роботи. Як результат у роботі досліджено основні характеристики інструментів поведінкової аналітики, здійснено порівняльний аналіз сучасних рішень UEBA і надано пропозиції щодо їх застосування, з'ясовано роль ШІ як засобу розширення можливостей UEBA і запропоновано рекомендації щодо його використання для команд кібербезпеки.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації стратегій впровадження інструментів ШІ в системи поведінкової аналітики організації.

КЛЮЧОВІ СЛОВА : КІБЕРЗАГРОЗИ, СИСТЕМИ ПОВЕДІНКОВОЇ АНАЛІТИКИ (UEBA), ШТУЧНИЙ ІНТЕЛЕКТ, МАШИННЕ НАВЧАННЯ, ПЕРСПЕКТИВИ І ВИКЛИКИ ВИКОРИСТАННЯ ШІ В СИСТЕМАХ UEBA.

ABSTRACT

The text part of the qualification paper for obtaining a master's degree: 93 pages, 22 figures, 3 tables, 69 sources.

The purpose of the work is to study prospects and challenges of using artificial intelligence methods in behavioral analytics systems.

Object of research is behavioral analytics systems (UEBA) as a means of detecting and preventing cyber threats.

Subject ***of research*** is prospects and challenges of using artificial intelligence methods in behavioral analytics systems.

Research methods. For solving the research tasks, historical, statistical and prognostic methods, methods of analysis and synthesis, comparison, classification, modeling, and behavioral analytics were used.

Summary of the paper. The author investigated the main characteristics of behavioral analytics tools, conducted a comparative analysis of modern UEBA solutions and provided suggestions for their application, clarified the role of AI as an extension of UEBA capabilities and offered recommendations for its use for the cybersecurity teams.

Field of research. The developed approaches can be used in planning and implementing strategies for implementing AI tools in the organization's behavioral analytics systems.

KEYWORDS: The developed approaches can be used in planning and implementing strategies for implementing AI tools in the organization's behavioral analytics system.

KEYWORDS: CYBER THREATS, USER AND ENTITY BEHAVIOR ANALYTICS (UEBA), ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, PROSPECTS AND CHALLENGES FOR THE USE OF AI IN UEBA.

.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ 9
ВСТУП 10
РОЗДІЛ 1 ОСНОВНІ ХАРАКТЕРИСТИКИ ІНСТРУМЕНТІВ ПОВЕДІНКОВОЇ АНАЛІТИКИ 12
1.1 Компоненти й можливості UEBA 12
1.2 UEBA як засоби проактивного захисту із застосуванням ШІ 23
1.3 Ключові переваги та складнощі впровадження UEBA 29
Висновки до розділу 1 34
РОЗДІЛ 2 СУЧАСНІ РІШЕННЯ UEBA: ПОРІВНЯЛЬНИЙ АНАЛІЗ І РЕКОМЕНДАЦІЇ 36
2.1 Еволюція й актуальні підходи до поведінкової аналітики в кібербезпеці . 36
2.2 Огляд ринку продуктів поведінкової аналітики 43
2.3 Рекомендації щодо застосування кращих рішень UEBA 51
Висновки до розділу 2 58
РОЗДІЛ 3 ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЗАСІБ РОЗШИРЕННЯ МОЖЛИВОСТЕЙ СИСТЕМ UEBA 60
3.1 Напрями застосування ШІ в кібербезпеці й поведінковій аналітиці 60
3.2 Роль методів ШІ та МН у процесах сучасних UEBA-систем 69
3.3 Виклики і тенденції застосування ШІ в кібербезпеці й поведінковій аналітиці 74
Висновки до розділу 3 82
ВИСНОВКИ 84
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 87

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

AI (ШІ)	Artificial Intelligence
Ml (МН)	Machine Learning
APT	Advanced Persistent Threat
CNN	Convolutional Neural Network
DLP	Data Loss Prevention
DNN	Deep Neural Networks
EDR	Endpoint Detection and Response
GMM	Gaussian Mixture Model
GNN	Graph Neural Networks
IAM	Identity and Access Management
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
LDAP	Lightweight Directory Access Protocol
LLM	Large Language Model
NDR	Network Detection and Response
NLP	Natural Language Processing
PCAP	Packet Capture
RL	Reinforcement Learning
RNN	Recurrent Neural Networks
SIEM	Security Information and Event Management
SOAR	Security Orchestration Automation and Response
TTP	Tactics, Techniques, and Procedures
UBA	User Behavior Analytics
UEBA	User and Entity Behavior Analytics
XAI	Explainable Artificial Intelligence
XDR	Extended Detection and Response
YARA	Yet Another Recursive Acronym

ВСТУП

Актуальність теми. Як свідчить практика, рішення для аналізу поведінки користувачів та об'єктів (UEBA) сьогодні є критично важливими в корпоративній кібербезпеці. У сучасному складному і динамічному цифровому середовищі, де зловмисники часто проходять повз традиційні засоби захисту, інструменти UEBA дозволяють виявляти незвичайну поведінку, зупиняти внутрішні загрози і викривати атаки до їх ескалації. Використовуючи ШІ, ці платформи надають можливість командам безпеки покращувати якість і швидкість процесів захисту, переходити від реактивного до проактивного захисту від кіберзагроз.

Водночас ШІ широко використовується і з боку нападників, має недоліки, пов’язані із залежністю від якості даних, непрозорістю функціонування, етичними проблемами використання даних тощо. Вирішення зазначених проблем також є значущою частиною діяльності кіберкоманд.

З огляду на зазначене дослідження перспектив і викликів використання методів штучного інтелекту в системах поведінкової аналітики є актуальним науковим завданням.

Мета роботи полягає у дослідженні перспектив і викликів використання методів штучного інтелекту в системах поведінкової аналітики.

Об’єкт дослідження - системи поведінкової аналітики (UEBA) як засоби виявлення і запобігання кіберзагрозам.

Предмет дослідження – перспективи і виклики використання методів штучного інтелекту в системах поведінкової аналітики.

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

1. Дослідити основні характеристики інструментів поведінкової аналітики.
2. Порівняти сучасні рішення UEBA і надати пропозиції щодо їх застосування.
3. З’ясувати роль ШІ як засобу розширення можливостей UEBA і запропонувати рекомендації щодо його використання для команд кібербезпеки.

Методи дослідження. Для вирішення завдань дослідження використано історичний, статистичний і прогностичний методи, методи аналізу та синтезу, порівняння, класифікації, моделювання, теорії поведінкової аналітики.

Наукова новизна одержаних результатів. У роботі досліджено особливості сучасних систем поведінкової аналітики, в тому числі з огляду на застосування ШІ, проведено аналіз кращих продуктів за напрямом, проаналізовано переваги і труднощі впровадження інструментів ШІ в системи UEBA, а також окреслено перспективи галузі кібербезпеки у контексті розвитку ШІ.

Практичне значення одержаних результатів. Застосування напрацювань дослідження буде доцільним при обґрунтованому виборі й реалізації підходів до впровадження і вдосконалення систем поведінкової аналітики на основі ШІ.

Апробація результатів кваліфікаційної роботи була здійснена на конференції “Актуальні проблеми кібербезпеки” 29 жовтня 2025 року.

РОЗДІЛ 1
ОСНОВНІ ХАРАКТЕРИСТИКИ ІНСТРУМЕНТІВ ПОВЕДІНКОВОЇ АНАЛІТИКИ

1.1 Компоненти й можливості UEBA

Інструменти UEBA – це програмні системи, які використовують штучний інтелект (ШІ), машинне навчання (МН) і статистичні методи для виявлення аномальної поведінки або подій у мережі. Системи поведінкової аналітики працюють, аналізуючи та навчаючись на основі історичних даних, щоб встановити базовий рівень нормальної поведінки. Цей рівень потім використовується для виявлення відхилень або аномалій, які можуть свідчити про потенційну загрозу безпеці.

Засоби поведінкової аналітики не покладаються на попередньо визначені правила безпеки чи сигнатури. Натомість вони використовують алгоритми ШІ і МН для постійного навчання й адаптації до нових моделей поведінки, що робить їх дуже ефективними у виявленні невідомих загроз, зокрема скомпрометовані облікові дані, експлойти нульового дня і передові стійкі загрози (APT), які можуть пропустити традиційні рішення безпеки.

Крім того, UEBA аналізують не лише поведінку користувачів, але й поведінку інших об’єктів (entities), до яких відносять цифрові активи нелюдської природи в мережі організації, зокрема сервери, кінцеві точки (наприклад, ноутбуки), програми (як хмарні, так і локальні), мережеві пристрої (наприклад, маршрутизатори) та інші критично важливі IT-системи та інфраструктуру [1]. Це означає, що засоби UEBA можуть контролювати й аналізувати поведінку пристроїв, програм і мережевого трафіку, тобто будь-якого об’єкта, що є частиною цифрової екосистеми організації. Цей цілісний підхід дозволяє значно повніше і точніше виявляти загрози і реагувати на них.

Сучасні інструменти EUBA забезпечують надійні можливості виявлення в поєднанні з глибшим розумінням для розслідування та реагування. Вони

також надають автоматизовані часові рамки інцидентів, які виділяють події за ризиком, а також більш динамічні методи сповіщень, які дозволяють аналітикам з більшою точністю визначати пріоритети сортування сповіщень від сторонніх розробників.

На думку експертів Gartner [2], архітектура UEBA базується на підході «ззовні всередину» («outside-in»), а системам поведінкової аналітики притаманні три основні атрибути (pillars), показані на рис.1.1:

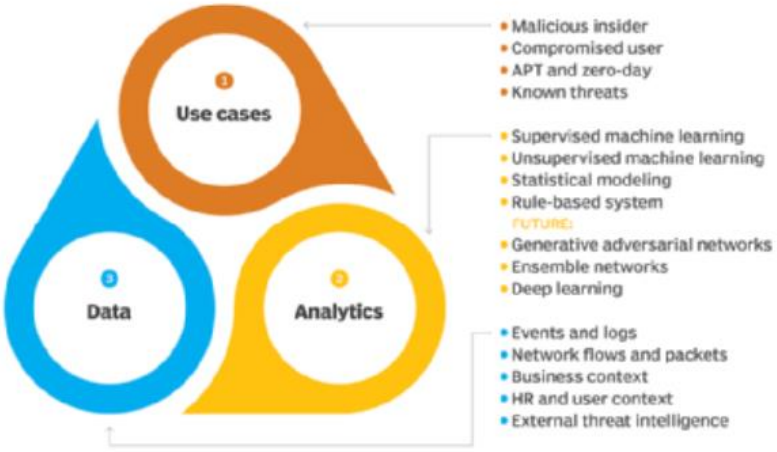


Рис. 1.1. Ключові атрибути рішень UEBA

• Варіанти використання (use cases): рішення UEBA надають інформацію про поведінку користувачів та інших об'єктів у корпоративній мережі, здійснюють моніторинг, виявлення та сповіщення про випадки відхилень від норми, застосовуються для кількох варіантів одночасно (виявлення внутрішнього зловмисника, скомпрометованого користувача, відомих і просунутих атак), на відміну від спеціалізованих засобів для виконання окремих функцій, наприклад моніторингу персоналу, хостів, шахрайських дій тощо.

• Джерела даних: рішення UEBA здатні отримувати дані (про події безпеки, мережеві потоки і пакети, функціонування бізнесу, управління персоналом, розвідки загроз тощо) із загального сховища даних, такого як озеро даних або сховище даних, або через системи управління інформацією та подіями безпеки SIEM. UEBA зазвичай не розгортають агентів для збору даних безпосередньо в IT-середовищі.

• Аналітика: засоби UEBA виявляють аномалії за допомогою різноманітних аналітичних підходів, зокрема статистичних моделей, ML, правил, сигнатур загроз тощо. Перспективними аналітичними напрямами є використання генеративних змагальних мереж, ансамблевих мереж, методів глибокого навчання.

Слід відзначити ключову роль в аналізі даних UEBA алгоритмів і моделей ML, які класифікують на дві основні категорії: контрольовані й неконтрольовані. Алгоритми контрольованого навчання потребують маркованих даних для навчання і тестування моделей, у той час, як алгоритми неконтрольованого навчання не потребують міток і можуть виявляти закономірності та кластери з самих даних. Прикладами алгоритмів контрольованого навчання для UEBA є логістична регресія, дерева рішень, методи опорних векторів та нейронні мережі. Зразками алгоритмів неконтрольованого навчання для UEBA є кластеризація k-середніх, аналіз головних компонентів, виявлення аномалій та автокодери [3].

Згідно з Quadrant Knowledge Solutions [4], ще одним атрибутом UEBA є ринкові аналітичні дані, які не варто недооцінювати, наприклад «Аналіз поведінки користувачів і об’єктів на 2023–2032 роки» від Polaris Market Research [5] та «Прогнозний аналіз ринку регіонів Європи, Середнього Сходу та Африки: аналіз поведінки користувачів та суб'єктів на 2022-2027» від Qksgroup [6].

Основні компоненти UEBA, які працюють разом для виявлення загроз та реагування на них, зазвичай охоплюють збір даних; побудову базових моделей; виявлення аномалій; сповіщення та реагування на інциденти (Рис.1.2.1).

Збір даних включає отримання інформації з різних джерел, таких як системи керування доступом до ідентифікаційних даних (IAM), інструменти управління інформацією та подіями безпеки (SIEM), журнали Active Directory, записи доступу до віртуальної приватної мережі (VPN), платформи виявлення та реагування на загрози кінцевим точкам (EDR), журнали хмарних сервісів і журнали доступу до програм або баз даних.

Після збору даних система створює базові моделі для розуміння нормальних моделей поведінки користувачів та об'єктів, включаючи звичайні

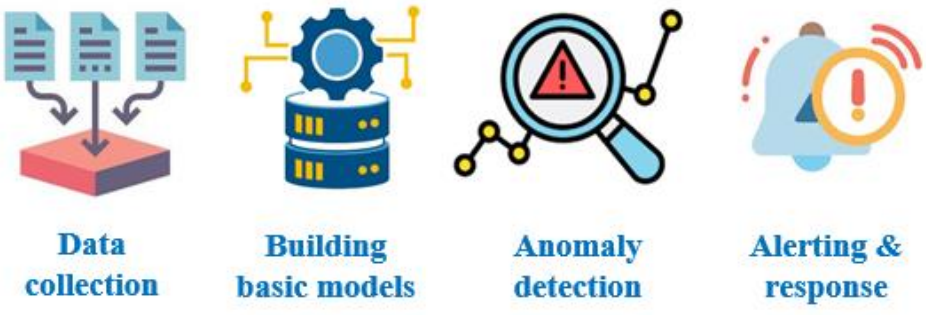
варіанти входу, використання програм, мережеву активність і взаємодію пристроїв.

Виявлення аномалій потім порівнює поточну активність з цими базовими показниками, використовуючи такі методи як статистичне визначення порогів, аналіз груп однорангових систем, часовий аналіз і МН, призначаючи оцінки ризику на основі серйозності й контексту відхилень.

Нарешті, механізми сповіщень та реагування співвідносять і пріоритезують аномалії для зменшення кількості хибнопозитивних результатів, часто інтегруючись з платформами оркестрації безпеки, автоматизації та реагування (SOAR) для запуску автоматизованих дій, таких як призупинення облікового запису, ізоляція мережі або посилена автентифікація [7].

Відповідно до іншого підходу [8] основними етапами роботи UEBA є: збір даних, який охоплює збирання журналів, пакетів та даних з усіх джерел; нормалізація, зберігання та аналіз даних у централізованому місці; аналіз даних з метою виявлення поведінки, яка не відповідає базовим шаблонам; звітність, тобто надсилання системою UEBA звітів і сповіщень працівникам команди безпеки. У більш загальному вигляді цей процес може бути представлений у вигляді схеми (Рис. 1.2.2).

1.2.1



1.2.2

Рис. 1.2. Основні компоненти UEBA

Встановлюючи базові рівні нормальної активності й застосовуючи МН для виявлення відхилень, UEBA покращує процеси виявлення, виводячи їх за межі традиційних систем, заснованих на правилах, забезпечуючи швидше й точніше реагування.

Системи поведінкової аналітики виявляють такі аномалії у діях користувачів та функціонуванні ІТ-об’єктів: відхилення у часі (наприклад, вхід у незвичний час), незвичну частоту дій (наприклад, доступ до бази даних 50 разів на годину), нерегулярну послідовність подій (наприклад, успішні входи після кількох невдач).

Сучасні рішення UEBA охоплюють власне моніторинг поведінки користувачів та об'єктів, відстежуючи дії користувачів і активність різних мережевих об'єктів для встановлення базового рівня нормальної поведінки; виявлення аномалій, які можуть свідчити про зловмисну діяльність або порушення безпеки, шляхом порівняння поточної активності зі встановленими базовими рівнями; ідентифікацію внутрішніх загроз через відстеження незвичних моделей доступу або передачі даних авторизованими користувачами.

Слід відзначити, що сучасні засоби UEBA відстежують кілька атрибутів, які допомагають швидко й точно виявляти і попереджати про підозрілу активність. Крім того, поєднання функцій дозволяє створити більш інклюзивну базову лінію, яка охоплює численні людські характеристики, що мінімізує шанси ввести систему в оману.

Так, об’єктами моніторингу є: комунікація (відстеження даних електронної пошти, чату та VoIP для контролю персоналу, з яким взаємодіють користувачі); системи, зокрема їхні цифрові сліди й поведінка під час підключення, які є цінним джерелом інформації і можуть бути отримані з кінцевих точок, браузерів, спільних файлів та фіксації звичок входу; людські ресурси, в тому числі мотиви кожної підозрілої активності та причини її зловмисної природи, які можна отримати з оглядів ефективності роботи працівників відділу кадрів і Active Directory; дані про фізичне

місцезнаходження і переміщення приміщенням, які дозволяють відстежувати дані бейджів, місця входу та історію подорожей [8].

Рішення UEBA працюють, постійно збираючи дані й аналізуючи поведінку, щоб виявити аномалії серед користувачів, пристроїв та інфраструктури. Системи працюють безшумно, збираючи інформацію для встановлення базових рівнів, не порушуючи нормальної діяльності.

Як відзначалося вище, трьома основними компонентами, які забезпечують розгортання UEBA є аналітика, інтеграція та презентація. Аналітика забезпечує збирання даних з різних джерел, створення профілів поведінки й застосовує статистичні моделі та алгоритми ML для виявлення незвичайних відхилень. За рахунок інтеграції даних і процесів система отримує та співвідносить інформацію з різних систем безпеки, забезпечуючи аналіз різних наборів даних. Представлення результатів аналізу дозволяє виявляти відхилення за допомогою сповіщень і візуалізації, а потім реагувати в автоматичному або ручному режимі [10].

Під час початкового розгортання рішення UEBA збирають журнали та інші системні дані для моделювання типових шаблонів доступу, потоків зв'язку, використання ресурсів та інших активностей. Системи застосовують розширену аналітику, таку як ML, для визначення нормальних базових рівнів як для користувачів, так і для об'єктів.

Після створення профілів поведінки користувачів або IT-об’єктів UEBA зіставляє поточну діяльність з ними, щоб розрахувати оцінки ризиків для аномалій та ідентифікувати загрози. Цей аналіз є безперервним, що дозволяє системам виявляти інсайдерські атаки, скомпрометовані облікові дані, витік даних та інші ризики в міру їх виникнення.

Поєднуючи дані з усієї інфраструктури з адаптивною аналітикою, рішення UEBA забезпечують надійні можливості виявлення та реагування на загрози, яких немає в традиційних інструментах. Для покращення операцій безпеки системи поведінкової аналітики зазвичай інтегруються з платформами SIEM.

Аналітика поведінки користувачів та IT-об’єктів є видом рішень кібербезпеки, які застосовують розширену аналітику та моделювання поведінки для визначення відхилень від норми. UEBA використовуються для виявлення розширених загроз безпеці, зокрема дії зловмисних інсайдерів та компрометація привілейованих облікових записів, які не можуть виявити традиційні інструменти безпеки на основі правил.

Рішення UEBA отримують операційні дані з багатьох джерел і визначають, якою є нормальна поведінка користувача або IT-об’єкта. Останні охоплюють IT-активи, такі як хости, програми, мережевий трафік, облікові записи служб та сховища даних. З часом рішення створює стандартні профілі поведінки у різних однотипних групах, щоб створити базовий рівень для організації. У разі виявлення аномальної активності, система її оцінює і присвоює рівень ризику. Оцінка серйозності ризику зростає зі збільшенням кількості аномальної поведінки, а в разі досягнення заздалегідь визначеного критичного порогу, спрацьовує сповіщення для аналітиків безпеки. Просунуті рішення UEBA здійснюють автоматизоване реагування [10].

Справжня сила засобів UEBA полягає в їх здатності долати організаційні кордони, відмінності й межі між IT-системами та різними джерелами даних і здійснювати цілісний аналіз багатьох джерел даних, серед яких: системи автентифікації, такі як Active Directory; системи контролю доступу, такі як VPN та проксі-сервери; бази даних управління конфігурацією; системи обліку людських ресурсів (наприклад, наймання і рух персоналу), що надають додатковий контекст про користувачів; брандмауери, системи IDS/IPS; антивіруси й системи виявлення зловмисних програм; засоби виявлення та реагування на загрози кінцевим точкам; аналізатори мережевого трафіку; інші канали інформації про загрози (Рис. 1.3).

Наприклад, рішення UEBA може виявляти незвичайний вхід через Active Directory, порівнювати його з критичністю пристрою, на який здійснюється вхід, чутливістю файлів, до яких здійснюється доступ, і попередньою незвичайною мережевою або шкідливою активністю, яка могла призвести до компрометації.

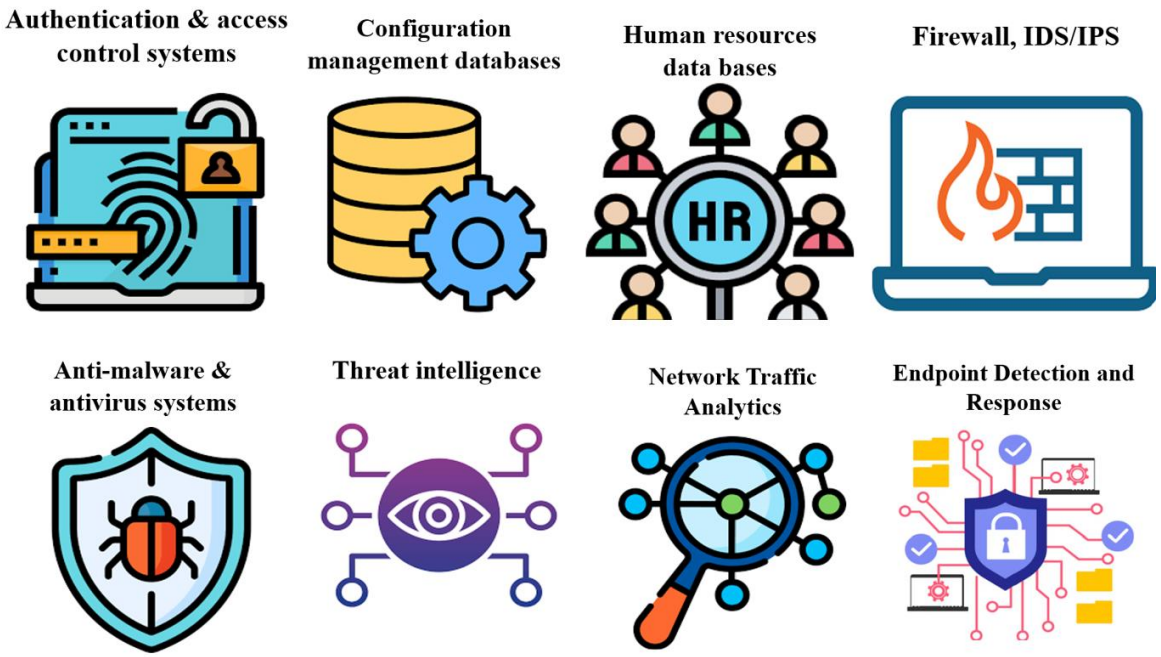


Рис. 1.3. Джерела даних для UEBA

Рішення UEBA вивчає нормальну поведінку для виявлення аномальної дій, досліджує широкий набір даних, щоб визначити базовий або поведінковий профіль користувача. Наприклад, система відстежує користувача й фіксує всі його дії: використання VPN, час приходу на робоче місце, входу в різні системи, використання принтера, частоту й розміри файлів, які особа надсилає електронною поштою або завантажує на USB-накопичувач, а також багато інших точок даних, що визначають нормальну поведінку користувача. Те саме стосується серверів, баз даних або будь-якої іншої IT-системи.

Як відзначалося вище, у випадку відхилення від базового рівня, система додає до оцінки ризику цього користувача або IT-об’єкт. Чим більш нетипова поведінка, тим вищий рівень ризику. Зі збільшенням кількості підозрілих дій оцінка критичності ризику зростає аж до досягнення певного порогу.

Такий аналітичний підхід має кілька переваг. По-перше, можливість агрегації даних про ризиковані події, завдяки якій аналітикам немає потреби вручну переглядати велику кількість окремих сповіщень і подумки об’єднувати їх для виявлення загрози.

По-друге, UEBA забезпечує зменшення кількості хибнопозитивних результатів, а отже, заощаджує час аналітиків. Це відбувається за рахунок того,

що системі для створення сповіщення потрібні кілька ознак аномальної поведінки, а одна незначна аномальна подія сама по собі не призведе до інформування фахівців команди безпеки.

Крім цього, UEBA здатні встановлювати контекстно-залежну базову лінію для кожної окремої групи користувачів, оскільки для різних категорій користувачів можуть бути застосовними відмінні правила кореляції. Наприклад, якщо фахівці відділу працюють позмінно або в різних часових поясах, вони будуть входити в систему в різний час, що постійно запускатиме сповіщення на основі традиційних правил. Натомість, у таких випадках система діятиме за складнішими правилами і не вважатиме такі випадки аномальними.

Під час аналізу інцидентів безпеки, які сьогодні нерідко є наслідком реалізації складних і розподілених у часі загроз, часова шкала є критичним поняттям, яке може пов'язати, на перший погляд, непов'язані дії. Передові рішення UEBA можуть «зшивати» дані з різних систем і потоків подій, щоб побудувати повну часову шкалу інциденту безпеки.

Наприклад, розглянемо користувача, який увійшов в систему, виконав підозрілу активність, а потім «зник» із журналів. Якщо буде встановлено, що та сама IP-адреса використовувалася для підключення до інших корпоративних систем невдовзі після першого аномального входу, то система зробить висновок, що це може бути частиною того самого інциденту, а той самий користувач продовжує спроби проникнення в систему. Додатковим прикладом може бути зловмисник, який кілька разів входить в систему на одному комп'ютері, використовуючи різні облікові дані. Це також вимагає «зшивання» даних про різні спроби входу та позначення їх як одного інциденту.

Після того, як система UEBA збере всі відповідні дані, вона може призначити оцінки ризику будь-якій активності на часовій шкалі події, а оцінка ризику додається для високоризикової та аномальної поведінки [9].

Відповідно до звіту Ponemon Institute [11], вартість і частота інцидентів безпеки, спричинених інсайдерами, продовжують зростати і у 2025 році обсяг середньорічних збитків від внутрішніх зловмисників досягне позначки у понад

17 млн доларів США (Табл. 1.1), а середній період часу для виявлення і стримування внутрішньої загрози становить 81 день.

На думку деяких експертів, застосування технологій UEBA дозволить, зменшити зазначений час удвічі [12], а згадане вище дослідження показало, що 55% організацій використовують саме системи поведінкової аналітики для виявлення й реагування на внутрішні атаки.

Таблиця 1.1

Середньорічна вартість кіберінцидентів, спричинених інсайдерами

Рік	Середньорічна вартість, млн доларів США
2018	8,3
2019	11,6
2022	15,4
2023	16,2
2024	17,4

Традиційно внутрішніх порушників поділяють на три види: недбалий, зловмисний і скомпрометований. Недбалим інсайдером є працівник або підрядник з привілейованим доступом до IT-систем, який ненавмисно наражає свою організацію на небезпеку, оскільки не дотримується належних IT-процедур. Наприклад, користувач, який залишив свій комп'ютер, не вийшовши з системи, або адміністратор, який не змінив пароль за замовчуванням або не встановив патч безпеки. Визначення нормальної та аномальної активності користувача є ключем до виявлення користувача, який був скомпрометований через недбалість.

Співробітник або підрядник з привілейованим доступом до IT-систем, який має намір здійснити кібератаку на організацію, є типовим прикладом зловмисного інсайдера. З огляду на те, що злочинний намір важко виміряти або виявити за допомогою файлів журналів або регулярних подій безпеки,

критично важливою є роль UEBA, яка встановлює базову лінію типової поведінки користувача та виявляє аномальну активність.

Зловмисники часто проникають в системи організації та зламують облікові записи привілейованих користувачів або довірені хости в мережі, а потім продовжують атаку від імені скомпрометованого інсайдера. Рішення UEBA можуть швидко виявити і проаналізувати шкідливу активність, яку зловмисник здійснює через скомпрометований обліковий запис.

Традиційним засобам безпеки важко виявити скомпрометованого інсайдера, якщо схема атаки або ланцюжок знищення є невідомими (наприклад, під час атаки нульового дня), або якщо атака реалізується латерально через організацію, змінюючи облікові дані, IP-адреси або машини. Однак технологія UEBA може виявляти ці типи атак, оскільки вони майже завжди змушують активи поводитися інакше, ніж згідно зі встановленими базовими показниками.

Значною проблемою команд кібербезпеки є так звана втома від сповіщень. Рішення UEBA можуть її пом’якшити, допомігши зрозуміти, які інциденти є особливо аномальними, підозрілими або потенційно небезпечними в контексті конкретної організації. UEBA може вийти за рамки базових рівнів і моделей загроз, додаючи дані про організаційну структуру, наприклад, критичність активів, ролі та рівні доступу до певних функцій організації. Невелике відхилення від норми для критично захищеної системи або адміністратора вищого рівня може бути вартим уваги для криміналіста, натомість для звичайного працівника лише значне відхилення отримає високий пріоритет.

Незважаючи на те, що традиційним інструментом запобігання втраті даних або незаконній передачі даних за межі організації є DLP, які теж нерідко створюють великий обсяг сповіщень, рішення UEBA можуть приймати сповіщення DLP, визначати їх пріоритети й консолідувати, виявляти аномальні події порівняно з відомими базовими рівнями. Це економить час криміналістам і допомагає швидше виявляти реальні інциденти безпеки.

UEBA є особливо важливим інструментом для боротьби з ризиками безпеки Інтернету речей (IoT). Організації розгортають великі парки підключених пристроїв, часто з мінімальними заходами безпеки або взагалі без них. Зловмисники можуть скомпрометувати пристрої IoT, використовувати їх для крадіжки даних або отримання доступу до інших IT-систем, або навіть використовувати їх для DDoS-атак чи інших атак на третіх сторін.

UEBA можуть відстежувати підключені пристрої, встановлювати базову поведінку для кожного пристрою або групи подібних пристроїв і негайно виявляти, чи пристрій поводиться у типовий спосіб, наприклад чи підключається до незвичайних адрес або пристроїв, проявляє активність у незвичний час, активує функції, які зазвичай не використовуються.

1.2 UEBA як засоби проактивного захисту із застосуванням ШІ

Системи поведінкової аналітики забезпечують проактивну безпеку, надаючи інформацію про потенційні загрози, перш ніж вони переростуть у серйозні інциденти, таким чином дозволяючи організаціям вийти за рамки реактивних заходів безпеки. Одним із основних чинників таких можливостей поведінкової аналітики є використання сучасних технологій ШІ і МН.

Завдяки цим алгоритмам UEBA здатні робити прогнози на основі даних за допомогою методів, що використовуються для складання складних алгоритмів. Рішення МН використовуються для зменшення кількості хибних спрацьовувань і підвищення точності в цих галузях, забезпечуючи можливості статистичного аналізу. Поведінка користувачів ніколи не буває статичною, а середовище постійно змінюється, що ускладнює впровадження монолітної системи виявлення в численних джерелах даних. МН є потужним інструментом у контекстній оцінці та цільовому виявленні UEBA.

Розглянемо детальніше ключові ознаки сучасних засобів UEBA (Рис. 1.4).

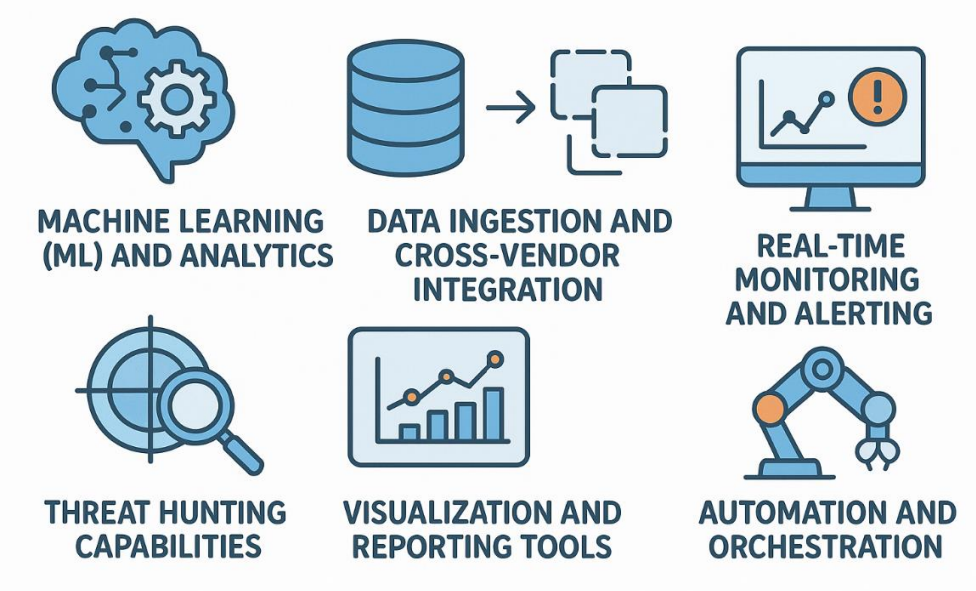


Рис. 1.4. Основні риси сучасних засобів UEBA

Машинне навчання (МН) й аналітика. Інструменти UEBA використовують МН для аналізу величезних обсягів даних у режимі реального часу, що дозволяє виявляти тонкі закономірності й кореляції, які можуть свідчити про загрозу безпеці. Це є одним із найперших застосувань МН в операціях безпеки.

Алгоритми МН можуть навчатися на історичних даних, щоб встановити базову лінію нормальної поведінки для користувачів та об'єктів у мережі. Будь-які відхилення від цієї базової лінії позначаються як потенційні загрози. Ця здатність навчатися й адаптуватися з часом робить інструменти UEBA дуже ефективними у виявленні нових та еволюціонуючих загроз.

Більше того, використання розширеної аналітики дозволяє інструментам поведінкової аналітики відсіювати шум і зосереджуватися на найважливіших загрозах, пріоритезувати сповіщення на основі серйозності загрози і вартості постраждалих активів.

Обробка великих даних та інтеграція з іншими системами. Інструменти UEBA можуть отримувати й аналізувати величезні обсяги даних з різних джерел. До них належать файли журналів, дані мережевого трафіку, ідентифікаційна інформація та канали розвідки про загрози.

Крім того, засоби поведінкової аналітики мають потужні можливості безперешкодної інтеграції з іншими інструментами і системами безпеки,

створюючи єдину інфраструктуру безпеки. Системи, які зазвичай інтегруються з UEBA, це системи управління інформацією та подіями безпеки SIEM, системи виявлення вторгнень IDS і брандмауери. Провідні продукти UEBA пропонують інтегровані рішення, що працюють разом у рамках SIEM.

Моніторинг та оповіщення в реальному часі. Інструменти UEBA пропонують можливості моніторингу та оповіщення в режимі реального часу. Вони постійно аналізують мережеву активність, що дозволяє їм виявляти загрози в міру їх виникнення. Це надзвичайно важливо в сучасному ландшафті загроз, де загрози можуть поширюватися та завдавати шкоди за лічені хвилини. Після виявлення загрози системи UEBA можуть надсилати сповіщення миттєво, що дозволяє командам безпеки швидко реагувати й усувати загрозу, перш ніж вона завдасть значної шкоди. У деяких випадках сповіщення з вищим рівнем серйозності ініціюють дії реагування за допомогою засобів автоматизації.

Можливості пошуку загроз. Окрім виявлення загроз у режимі реального часу, інструменти UEBA також підтримують пошук загроз. Цей проактивний підхід до кібербезпеки передбачає пошук загроз, які могли уникнути традиційних методів виявлення. За допомогою засобів поведінкової аналітики команди безпеки можуть проводити поглиблені розслідування підозрілої діяльності на ранніх етапах циклу атаки, щоб виявити приховані загрози.

Ці інструменти надають величезну кількість даних та аналітики, які можуть допомогти у пошуку загроз, зокрема виявляють моделі поведінки, які можуть свідчити про скоординовану атаку, визначають зв'язки між різними об’єктами, які можуть свідчити про скомпрометований пристрій, та надавати уявлення про тактику, методи та процедури (TTP), що використовуються зловмисниками. Деякі з провідних рішень надають розширені функції пошуку загроз, що дозволяє шукати серед відомих аномалій, неідентифікованих UEBA.

Інструменти візуалізації та звітності. Системи UEBA оснащені інструментами візуалізації і звітності, які забезпечують візуальне представлення даних про мережу та її активності для полегшення командам безпеки розуміння поточного ландшафту загроз. Також засоби візуалізації і

звітності можуть унаочнювати закономірності й тенденції, визначати гарячі точки активності та відстежувати зміни з часом.

Крім того, інструменти UEBA надають детальну та практичну звітність про виявлені загрози, генеруючи звіти за різними показниками, такими як кількість і типи виявлених загроз, уражені активи, час реагування тощо. Такі звіти можуть допомогти у процесі прийняття рішень і стратегічного планування, сприяючи організаціям у покращенні стану корпоративної кібербезпеки.

Автоматизація та оркестрація. Однією із ключових характеристик сучасних інструментів UEBA є їхня здатність автоматизувати й оркеструвати різні завдання безпеки. Автоматизація дозволяє цим інструментам автоматично виконувати заздалегідь визначені дії у разі досягнення певних критеріїв або порогових значень. Наприклад, якщо система виявила кілька невдалих спроб входу користувача протягом короткого періоду, вона автоматично заблокує обліковий запис, щоб запобігти несанкціонованому доступу.

Можливості оркестрації працюють разом з автоматизацією, забезпечуючи оптимізацію робочого процесу операцій безпеки. Завдяки оркестрації засоби UEBA можуть взаємодіяти з іншими рішеннями безпеки, такими як брандмауери, платформи захисту кінцевих точок та інструменти реагування на інциденти. Ця інтеграція дозволяє координувати швидке та своєчасне реагування на виявлені загрози. Наприклад, коли UEBA виявляє незвичне переміщення даних, яке може свідчити про витік даних, система без втручання людини запускає брандмауер для блокування підозрілої IP-адреси [9].

Деякі рішення UEBA спираються на традиційні методи виявлення підозрілої активності, зокрема правила, визначені вручну, кореляції між подіями безпеки та відомі шаблони атак. Обмеження таких методів полягає в тому, що вони ефективні лише настільки, наскільки ефективні правила, визначені адміністраторами безпеки, і не можуть адаптуватися до нових типів загроз або поведінки системи [13].

Натомість можливості розширеної аналітики є значно ширшими і охоплюють кілька сучасних технологій, які можуть допомогти виявити аномальну поведінку навіть за відсутності відомих закономірностей (Рис. 1.5).

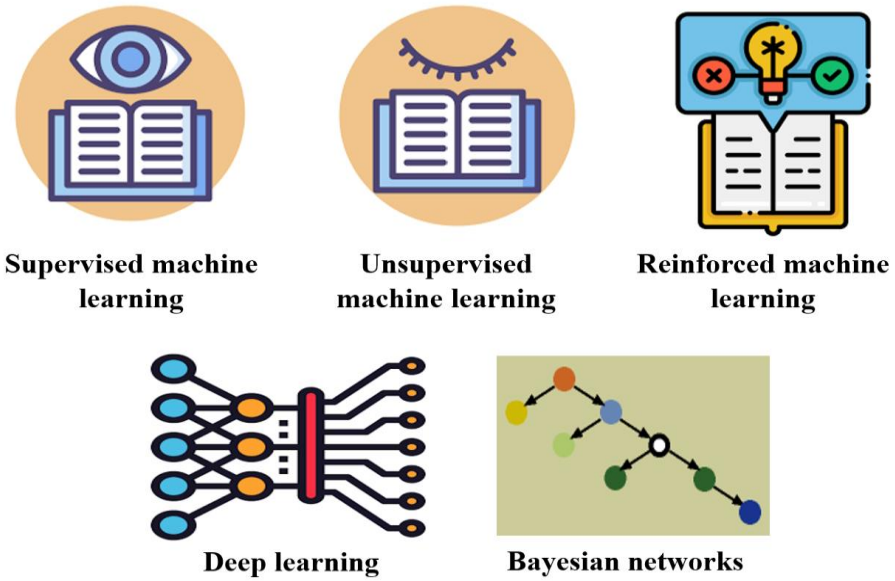


Рис. 1.5. Технології розширеної аналітики UEBA

Кероване навчання, навчання під наглядом (Supervised Learning) - набори відомих нормальної та хибної поведінки завантажуються в систему. Інструмент навчається аналізувати нову поведінку й визначати, чи вона «схожа» на набір відомої типової чи хибної поведінки.

• *Баєсівські мережі* можуть поєднувати кероване МН і правила для створення поведінкових профілів.

• *Некероване навчання*, навчання без нагляду (Unsupervised Learning) - система вивчає нормальну поведінку, здатна виявляти аномальну поведінку і попереджати про неї. Вона не може визначити, чи є аномальна поведінка порушенням, а лише те, що вона відхиляється від норми.

• *Підсилене машинне навчання* (Reinforced/Semi-supervised Learning) - це гібридна модель, де основою є навчання без нагляду людини, а фактичні рішення щодо сповіщень подаються назад у систему, щоб забезпечити точне налаштування моделі та зменшити співвідношення сигнал/шум.

• *Глибоке навчання* (Deep Learning) - дозволяє проводити віртуальне сортування та розслідування сповіщень. Система навчається на наборах даних,

що представляють тривоги безпеки та результати їх сортування, виконує самоідентифікацію ознак і здатна прогнозувати результати сортування для нових наборів сповіщень безпеки [9].

Традиційні методи аналітики є детермінованими, в тому сенсі, що якщо певні умови були виконані, генерувалося сповіщення, а якщо ні, система вважала, що «все гаразд». Перелічені вище розширені методи аналітики відрізняються тим, що вони є евристичними. Вони обчислюють оцінку ризику, яка є ймовірністю того, що подія являє собою аномалію або інцидент безпеки. Коли оцінка ризику перевищує певний поріг, система створює сповіщення безпеки .

Розширені можливості аналізу поведінки користувачів та IT-об'єктів у сучасних інструментах виявлення внутрішніх загроз можуть ефективно аналізувати події безпеки і значно зменшувати кількість хибнопозитивних результатів, дозволяючи командам безпеки зосередитися на справжніх загрозах.

Рис. 1.6. Просунуті можливості UEBA

Просунуті алгоритми МН дозволяють адаптувати й покращити виявлення загроз упродовж усього часу, а також застосовувати методи розпізнавання складних шаблонів для виявлення аномалій.

Всеохоплююча інтеграція даних охоплює безперебійне отримання даних з різних джерел, кореляцію дій користувачів на кількох платформах.

Аналітика і сповіщення в реальному часі передбачає миттєвий аналіз поведінки користувачів та взаємодії об’єктів, вчасні повідомлення про потенційні загрози безпеці.

Кастомізоване ранжування ризиків (з можливостями налаштування відповідно до конкретних потреб) забезпечує гнучке оцінювання ризиків з урахуванням притаманних організації характеристик і пріоритезацію високоризикових подій для негайного реагування.

Зручна для користувача візуалізація охоплює інтуїтивно зрозумілі панелі управління для легкої інтерпретації складних даних, а також візуальне представлення шаблонів поведінки користувачів і відхилень [14].

1.3 Ключові переваги та складнощі впровадження UEBA

Як і будь-які інші технології, системи поведінкової аналітики мають свої переваги і недоліки.

Аналіз літератури [9, 15-17] засвідчив такі ключові переваги UEBA (Рис. 1.7). Розглянемо їх детальніше.

Рис. 1.7. Ключові переваги UEBA

Покращене виявлення загроз полягає в тому, що UEBA здатні виявляти загрози, які можуть бути пропущені традиційними інструментами безпеки, в результаті використання засобів розширеної аналітики для виявлення аномальної поведінки або аномалій у діяльності користувачів. Це має вирішальне значення для виявлення складних таких кіберзагроз як внутрішні загрози, скомпрометовані облікові записи або передові постійні загрози (APT).

Крім цього, інструменти UEBA забезпечують раннє попередження, виявляючи потенційні ризики та загрози безпеці в міру їх формування, що дозволяє проактивно пом'якшувати загрози до того, як стануть доступні традиційні дані про події або відомі моделі.

UEBA є особливо ефективними у виявленні зловмисної або недбалої діяльності інсайдерів. Оскільки ці користувачі мають законний доступ до систем, звичайним інструментам безпеки може бути складніше виявити їхні шкідливі дії. Наприклад, система UEBA може виявити користувача, який раптово починає отримувати доступ до файлів, до яких він зазвичай не звертається, скачує великі обсяги даних з незвичайного місця або в незвичайний час доби, що може вказувати на те, що обліковий запис був скомпрометований тощо.

Зменшення кількості хибних спрацьовувань. З огляду на те, що надмірна кількість хибнопозитивних спрацьовувань знижує ефективність реагування, перевантажує аналітиків і може призводити до ігнорування реальних кібератак, у процесі аналізу моделей поведінки UEBA може допомогти зменшити кількість хибних спрацьовувань, що генеруються традиційними системами безпеки. Для цього використовуються такі підходи як аналіз контексту, адаптивні часові пороги й самонавчання, поєднання правил, статистики і МН/глибокого навчання тощо [18].

Поведінкове профілювання та оцінка ризиків. Інструменти UEBA часто містять функції поведінкового профілювання та оцінки ризиків, які допомагають пріоритезувати сповіщення безпеки, дозволяючи командам безпеки зосередитися на більш важливих проблемах.

Забезпечення відповідності нормативним вимогам. У законодавчо регульованих галузях, таких як фінансові послуги й охорона здоров’я, правила щодо захисту даних і конфіденційності передбачають стандарти, яких зобов’язана дотримуватися кожна компанія. UEBA відстежують дотримання цих нормативних вимог, здійснюючи необхідний моніторинг і ведення звітної документації.

Адаптація до розвитку ландшафту загроз. Системи UEBA ґрунтуються на алгоритмах МН, які постійно вивчають мінливі моделі поведінки користувачів та ІТ-об’єктів за допомогою аналізу даних. Пристосовуючись до потреб безпеки в режимі реального часу, рішення безпеки можуть залишатись ефективними в умовах мінливого ландшафту безпеки зі складними кіберзагрозами.

Запобігання втраті даних. UEBA сприяє запобіганню витокам і втратам даних, відстежуючи поведінку користувачів, виявляючи незвичайні моделі доступу або передачі даних, які можуть свідчити про витік даних або спробу крадіжки інформації.

Швидше й ефективне реагування на інциденти. UEBA надає цінні відомості для команд безпеки, зокрема детальний контекст і записи про дії користувачів, дозволяючи аналітикам оперативно дослідити аномалії, підтвердити порушення безпеки, оцінити їхні наслідки і надати своєчасну й дієву інформацію про потенційні інциденти кіберфахівцям для подальшого розслідування. Завдяки цьому інциденти усуваються швидше й ефективніше, що зводить до мінімуму загальний вплив кіберзагроз на всю організацію.

Слід також зазначити, що передові рішення UEBA можуть інтегруватися з іншими інструментами безпеки для автоматизації процесів реагування на виявлені загрози, що скорочує час і зусилля, необхідні для виправлення, та підвищує загальну ефективність управління кібербезпекою [19].

Довгостроковий аналіз тенденцій та криміналістика. Інструменти UEBA можуть зберігати й аналізувати дані у довгостроковій перспективі, що є цінним для аналізу тенденцій, наприклад розвитку загроз і технологій кібернападу. Дані, зібрані системами поведінкової аналітики, стають базовими доказами для кіберкриміналістів, які можуть розслідувати інцидент, виявити джерело атаки та зібрати докази для подальшого використання.

Адаптивне навчання. UEBA використовують алгоритми МН для постійної адаптації та вивчення нових моделей поведінки, що робить системи поведінкової аналітики дуже ефективними у виявленні невідомих загроз, таких

як скомпрометовані облікові дані, експлойти нульового дня і складні APT-атаки.

Можливості автономного використання UEBA і розширення базових рішень SIEM. Інструменти UEBA можуть бути дуже ефективними як автономні рішення, особливо в програмах боротьби з внутрішніми загрозами та нішевих випадках використання, пропонуючи надійний моніторинг безпеки, можливості виявлення підозрілих активностей і аномалій.

Водночас, рішення UEBA нерідко доповнюють традиційні рішення для управління інформацією та подіями безпеки (SIEM), заповнюючи прогалини в обмеженнях виявлення загроз і сприяючи появі SIEM наступного покоління, що є важливим для високоточного виявлення загроз.

Отже, системи UEBA є цінним доповненням до арсеналу засобів кібербезпеки будь-якої організації, який завдяки проактивному виявленню та усуненню потенційних загроз, допомагає організаціям підвищити якість і рівень захищеності корпоративних систем від динамічних кіберзагроз.

Незважаючи на значний перелік переваг, впровадження інструментів UEBA має охоплювати також і оцінку недоліків і потенційних проблем, пов’язаних з їх розгортанням і використанням.

Насамперед слід пам’ятати про *обмежені можливості інтеграції даних* UEBA, які збирають і обробляють комплексні, високоякісні дані із систем управління ідентифікацією, журналів програм, мережевого трафіку, телеметрії кінцевих точок тощо. Інтеграція цих джерел, часто в різних форматах і обсягах, може бути складною та трудомісткою.

Ще однією проблемою може стати *недостатня масштабованість* систем. Зі зростанням організацій та додаванням більшої кількості пристроїв, програм і користувачів обсяг даних зростає експоненційно. Рішення UEBA повинні обробляти ці дані майже в режимі реального часу, зберігаючи при цьому продуктивність. Без належного планування вузькі місця в продуктивності та збільшена затримка можуть погіршити можливості виявлення та пригальмувати робочі процеси аналітиків.

Проблеми з конфіденційністю даних. Посилення операцій безпеки не має здійснюватися через порушення прав окремих осіб на конфіденційність. Постійне відстеження поведінки користувачів та ІТ-об’єктів порушує питання, пов’язані з етикою та конфіденційністю, тому дуже важливо відповідально використовувати інструменти безпеки, зокрема на основі ШІ [20].

Незважаючи на розширену аналітику, *хибнопозитивні результати* залишаються значною проблемою при розгортанні UEBA. Якщо система генерує забагато сповіщень про нешкідливі аномалії, такі як робота легітимного користувача з нового місця розташування, аналітики безпеки можуть бути перевантажені або втратити пильність.

Ця проблема часто пов'язана з незрілим базовим підходом або недостатнім контекстом у моделях поведінки. З часом, коли система навчається та налаштовує оцінку ризиків, кількість хибнопозитивних результатів зазвичай зменшується. Однак на ранніх етапах розгортання або в динамічних середовищах підтримувати прийнятну якість сповіщень може бути складно.

Платформи UEBA потребують *кваліфікованого персоналу* для конфігурації, налаштування та обслуговування. Організаціям необхідні фахівці зі знаннями поведінкової аналітики, засад виявлення загроз і реагування на інциденти. Крім того, можуть знадобитися інженери обробки даних, щоб забезпечити належне отримання та нормалізацію інформації. Меншим організаціям може не вистачати досвіду або кількості персоналу для підтримки повномасштабного впровадження UEBA. Навіть для великих підприємств інтеграція UEBA в існуючі операції безпеки може вимагати значних витрат часу та постійних зусиль для підтримки точності та ефективності моделей.

Основні посади, необхідні для повноцінного впровадження і функціонування UEBA, охоплюють аналітиків безпеки (Security Analyst), які мають уміти інтерпретувати оповіщення системи та проводити розслідування; інженерів з безпеки (Security Engineer), відповідальні за налаштування і оптимізацію системи; аналітиків даних (Data Analyst), які спеціалізуються на обробці та аналізі великих обсягів даних, що надходять до UEBA-системи з різних

джерел; спеціалістів з IT-інфраструктури (IT Infrastructure Specialist), які забезпечують інтеграцію UEBA-системи з різними компонентами корпоративної IT-інфраструктури; архітекторів безпеки (Security Architect), відповідальних за розробку загальної стратегії кібербезпеки компанії, включаючи розгортання UEBA-рішень, з урахуванням бізнес-вимог і існуючих технологічних рішень [21].

Висновки до розділу 1

UEBA – це програмні системи, які використовують МН та статистичні методи для виявлення аномальної поведінки або подій у мережі. Системи поведінкової аналітики працюють, аналізуючи та навчаючись на основі історичних даних, щоб встановити базовий рівень нормальної поведінки користувачів та IT-об’єктів. Цей рівень потім використовується для виявлення відхилень або аномалій, які можуть свідчити про потенційну загрозу безпеці.

Сучасні інструменти EUBA забезпечують надійні можливості виявлення в поєднанні з глибшим розумінням для розслідування та реагування. Вони також надають автоматизовані часові рамки інцидентів, які виділяють події за ризиком, а також більш динамічні методи сповіщень, які дозволяють аналітикам з більшою точністю визначати пріоритети сортування сповіщень від сторонніх розробників.

Основні компоненти UEBA, які працюють разом для виявлення загроз і реагування на них, зазвичай охоплюють 1) збір даних із різних джерел, таких як IAM та SIEM, журнали Active Directory, записи доступу до VPN, платформи EDR, журнали хмарних сервісів і доступу до програм або баз даних тощо; 2) побудову базових моделей для розуміння нормальних моделей поведінки користувачів та об'єктів; 3) виявлення аномалій, яке охоплює порівняння поточної активності з базовими показниками; 4) сповіщення та реагування на інциденти з метою співвіднесення і пріоритезації аномалій.

Системи поведінкової аналітики забезпечують проактивну безпеку, надаючи інформацію про потенційні загрози, перш ніж вони переростуть у

серйозні інциденти, таким чином дозволяючи організаціям вийти за рамки реактивних заходів безпеки. Основними рисами сучасних UEBA є використання МН й аналітики для аналізу величезних обсягів даних у режимі реального часу; обробка великих даних та інтеграція з іншими системами, насамперед SIEM, IDS і брандмауерами; моніторинг та оповіщення в реальному часі; можливості пошуку загроз, зокрема тих, які могли уникнути стандартних методів виявлення; інструменти візуалізації та звітності; автоматизація завдань безпеки та оркестрація, тобто взаємодія з іншими системами безпеки.

Як і будь-які інші технології, системи поведінкової аналітики мають свої переваги і недоліки. Аналіз літератури засвідчив такі ключові переваги UEBA: покращене автоматизоване виявлення і раннє попередження загроз; зменшення кількості хибних спрацьовувань; забезпечення нормативної відповідності; адаптивність до ландшафту загроз; запобігання втраті даних; швидке й ефективне реагування на інциденти; довгостроковий аналіз тенденцій і криміналістика; можливості автономного використання UEBA і розширення базових рішень SIEM.

Незважаючи на значний перелік переваг, впровадження інструментів UEBA пов’язане з деякими недоліками і потенційними проблемами, зокрема обмежені можливості інтеграції даних; недостатня масштабованість систем; проблеми з етикою і конфіденційністю даних; наявність хибнопозитивних результатів; потреба у кваліфікованому персоналі.

РОЗДІЛ 2
СУЧАСНІ РІШЕННЯ UEBA: ПОРІВНЯЛЬНИЙ АНАЛІЗ І РЕКОМЕНДАЦІЇ

2.1 Еволюція й актуальні підходи до поведінкової аналітики в кібербезпеці

Еволюція UEBA ознаменована значним прогресом у технологіях і методах кібербезпеки. Системи поведінкової аналітики, які зародилися на поч. 2000-х років, засвідчили нагальну необхідність аналізу поведінки користувачів для виявлення внутрішніх загроз і несанкціонованої діяльності [22].

Протягом багатьох років UEBA еволюціонувала від базових методів поведінкового аналізу до складних рішень, що використовують МН, аналітику великих даних та автоматизацію. Перші впровадження були зосереджені на виявленні аномалій на основі правил, але оскільки кіберзагрози ставали складнішими, UEBA інтегрувала алгоритми МН для підвищення точності виявлення. Інтеграція можливостей аналітики великих даних дозволила організаціям аналізувати великі обсяги даних для комплексного виявлення загроз [23].

Впровадження хмарних технологій і масштабованість стали важливими рисами наприкінці 2010-х років, тоді як в останні роки спостерігається зсув у бік автоматизації, оркестрації та реалізації підходів на основі ШІ. Сьогодні UEBA є основним компонентом сучасних архітектур кібербезпеки, надаючи організаціям можливість проактивно виявляти і пом'якшувати широкий спектр загроз безпеці [24]. Розвиток систем UEBA з початку 2000-х років до теперішнього часу показано на рисунку 2.1.

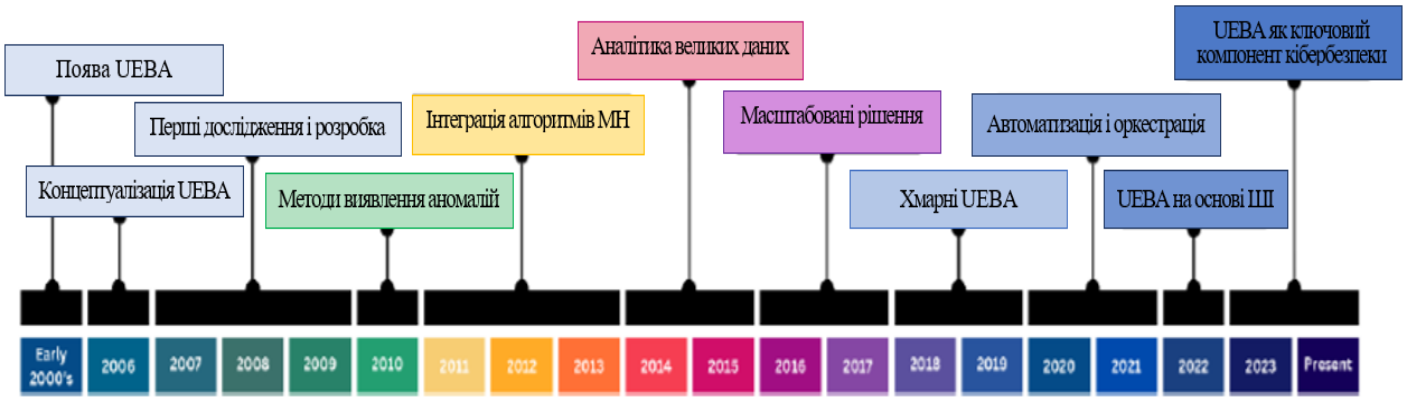


Рис. 2.1. Еволюція систем поведінкової аналітики

Отже, UEBA – це стратегія кібербезпеки, яка аналізує поведінку користувачів та IT-об'єктів у мережі або системі організації для виявлення внутрішніх загроз, скомпрометованих облікових записів і різних проблем безпеки. Як частково відзначалося вище, основними елементами сучасних систем поведінкової аналітики є: збір і обробка даних; алгоритми МН; поведінковий і контекстний аналіз; виявлення аномалій; оцінка ризиків і пріоритезація; візуалізація та звітність.

Системи UEBA забезпечують збір даних з різних джерел у мережі організації, включаючи журнали, потоки подій, записи про активність користувачів і дані кінцевих точок. Дані можуть охоплювати поведінку користувачів, мережевий трафік, активність системи та використання програм.

Наступним етапом є обробка даних, у рамках якого дані попередньо обробляються та нормалізуються, щоб гарантувати узгодженість і сумісність між кількома джерелами даних. Цей процес передбачає очищення, організацію та структурування необроблених даних для аналізу.

Алгоритми МН широко використовуються системами UEBA для обробки величезних наборів даних і розпізнавання закономірностей, аномалій та відхилень від типової поведінки. Ці алгоритми використовують вивчені моделі поведінки для виявлення підозрілої поведінки, нетипових моделей доступу та можливих проблем безпеки.

Методи поведінкової аналітики використовуються для створення базових профілів поведінки для окремих осіб, об'єктів (таких як пристрої, програми та сервери) та всієї системи. Відстежуючи відхилення від цих базових значень, системи UEBA виявляють незвичайну поведінку, яка може сигналізувати про порушення безпеки або внутрішню загрозу.

Засоби поведінкової аналітики використовують алгоритми виявлення аномалій для попередження про дивні дії або поведінку, які значно відрізняються від очікуваних. Прикладами таких подій є нетиповий час входу в систему, доступ до конфіденційних даних, зміни ролей або дозволів користувачів та інші підозрілі випадки поведінки.

Контекстний аналіз передбачає вивчення поведінки в контексті, враховуючи ролі користувачів, права доступу, час доби, місцезнаходження та критичність ресурсів, до яких здійснюється доступ. Контекстний аналіз допомагає у визначенні пріоритетів та контекстуалізації попереджень безпеки, зменшуючи кількість хибнопозитивних результатів і підвищуючи ефективність виявлення загроз.

Оцінювання ризиків та пріоритетність – також є елементом діяльності UEBA. Аномалії та події безпеки отримують рейтинги ризику на основі їхньої серйозності, можливого впливу та ймовірності реалізації небезпеки. Системи UEBA пріоритезують попередження та події на основі оцінок ризиків, що дозволяє командам безпеки зосередитися спочатку на найсерйозніших загрозах.

Завдяки функціям візуалізації та звітності, які є у складі більшості сучасних рішень UEBA, аналітики безпеки мають змогу вивчати шаблони даних, аналізувати події, унаочнювати результати аналізу і створювати звіти. Візуалізація допомагає також зрозуміти складні взаємозв'язки та шаблони в даних, що дозволяє приймати більш обґрунтовані рішення і належним чином реагувати на загрози [25].

Системи UEBA використовують різноманітні методи МН для аналізу моделей поведінки користувачів та ІТ-об’єктів, а також виявлення аномалій або

можливих вразливостей безпеки в мережі чи системі організації. Деякі типові методи МН, що використовуються в UEBA, показані на рисунку 2.2.

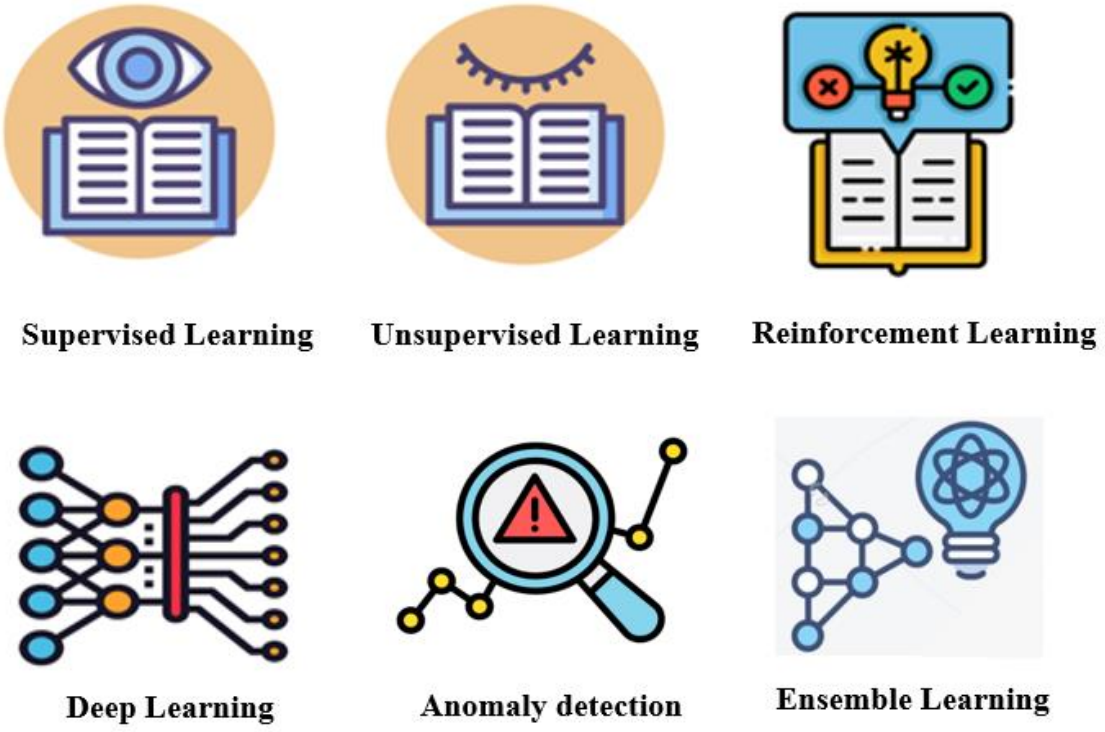


Рис. 2.2. Алгоритми машинного навчання UEBA.

Алгоритми некерованого навчання (без нагляду оператора) зазвичай використовуються в UEBA для виявлення моделей і аномалій у поведінці користувачів та IT-об'єктів без вимоги до маркованих навчальних даних. Методи кластеризації, такі як кластеризація k-середніх, ієрархічна кластеризація і кластеризація на основі щільності, використовуються для групування подібних моделей поведінки та виявлення відхилень і аномалій.

Алгоритми керованого навчання. UEBA використовує алгоритми навчання під наглядом для категоризації моделей поведінки та прогнозування того, чи є певна поведінка ознакою вразливостей безпеки. Методи класифікації, які охоплюють логістичну регресію, випадковий ліс, методи опорних векторів (SVM), дерева рішень та нейронні мережі, навчаються на маркованих наборах даних, щоб розрізняти нормальну та аномальну поведінку та надавати оцінки ризику інцидентам безпеки.

Моделі глибокого навчання, зокрема глибокі нейронні мережі (DNN), стають дедалі поширенішими в системах UEBA для аналізу складних і

багатогранних даних, таких як журнали мережевого трафіку, журнали активності користувачів та системні події. Такі архітектури, як згорткові нейронні мережі (CNN) та автокодери, можуть виявляти складні шаблони та представлення з необроблених даних. Це дозволяє точніше ідентифікувати аномальну поведінку та передові вектори атак.

Алгоритми виявлення аномалій, такі як моделі гаусової суміші (GMM), ізоляційний ліс, однокласова SVM і надійні статистичні підходи, використовуються UEBA, щоб знайти відхилення від типових моделей поведінки. Ці алгоритми описують розподіл типової поведінки й виявляють випадки, які значно відхиляються від прогнозованих шаблонів, як потенційні проблеми безпеки.

Підходи ансамблевого навчання, зокрема пакування, бустинг і стекування, є поширеними підходами, що використовуються в UEBA для інтеграції різних моделей МН та підвищення загальної точності та стійкості виявлення загроз. Ансамблеві підходи зменшують небезпеку перенавчання, одночасно збільшуючи здатність системи до узагальнення для опрацювання нових і невідомих загроз.

Навчання з підсиленням. Деякі складні системи UEBA можуть застосовувати методи підсиленого навчання для оптимізації правил безпеки і тактик реагування на основі зворотного зв'язку з навколишнім середовищем. Алгоритми підсиленого навчання навчаються робити послідовні судження й оновлювати політики безпеки у відповідь на загрози, що розвиваються, та слабкі місця [26].

Критично важливими для систем UEBA є підходи до моделювання поведінки, оскільки вони дозволяють їм створювати базові моделі поведінки, виявляти відхилення від типової активності й можливі вразливості безпеки в мережі або системі організації [27]. Деякі типові методології моделювання поведінки, що використовуються в UEBA, показані на рисунку 2.3.

Моделювання на основі профілів – це процес створення профілів поведінки для окремих осіб, об'єктів (таких як пристрої, програми та сервери) і

груп з використанням даних про попередню активність. Ці профілі документують типові моделі поведінки, такі як час входу в систему, моделі доступу, обсяги передачі даних та використання програм. Відхилення від цих моделей можуть свідчити про підозрілу або несанкціоновану діяльність.

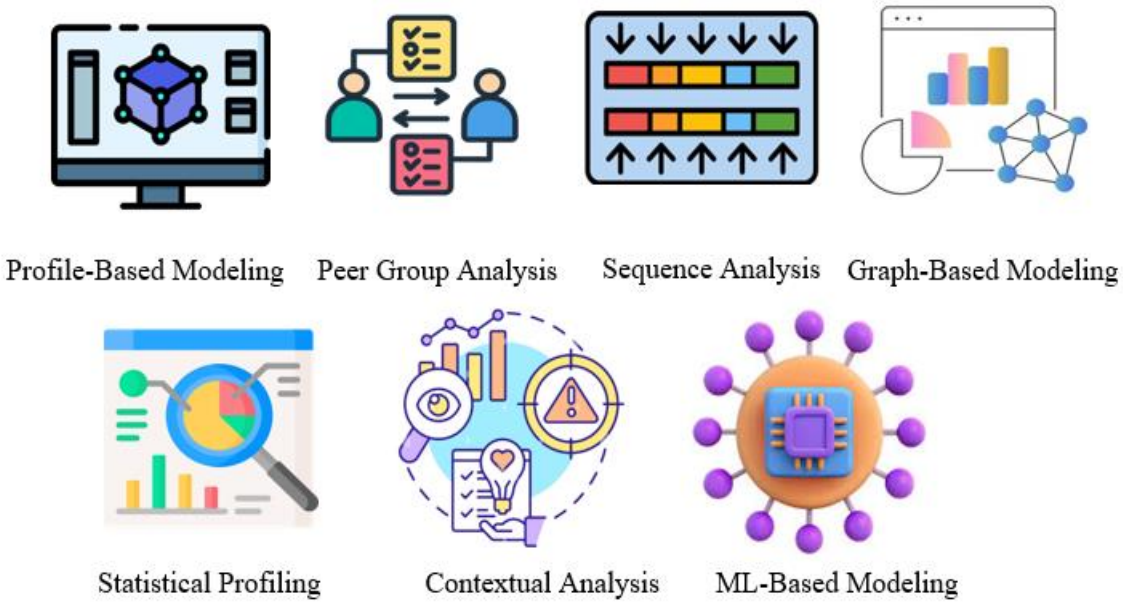


Рис. 2.3. Методології моделювання поведінки UEBA

Аналіз груп рівноцінних користувачів/IT-об’єктів, які належать до однієї категорії, наприклад, за рівнем чи повноваженнями за посадою, характеристики поведінки, функціями у корпоративних системах тощо. Аналіз таких груп передбачає порівняння поведінки окремих користувачів (або об’єктів IT) з поведінкою їхніх колег в організації або рівноцінних пристроїв і програм у корпоративних ІКС. Зіставляючи людей або об’єкти з порівнянними ролями, обов'язками та правами доступу, системи UEBA можуть виявляти аномалії та винятки, які значно відрізняються від норми в їхніх групах.

Аналіз послідовності. Ці підходи розглядають послідовні закономірності взаємодії користувачів та IT-об’єктів всередині системи. Це передбачає аналіз послідовності подій та дій, що виконуються окремими особами або IT-об’єктами з часом, таких як послідовність інструкцій, виданих під час сеансу, або серія мережевих підключень, створених пристроєм. Аналіз послідовності допомагає виявляти аномальні послідовності дій, які можуть свідчити про зловмисну поведінку або внутрішні загрози.

Моделювання на основі графів Графові структури використовуються для опису взаємозв'язків та дій між користувачами, IT-об’єктами й активами в корпоративній мережі. Моделюючи архітектуру мережі та аналізуючи потік даних і прав доступу між взаємопов'язаними організаціями, системи UEBA можуть виявляти аномальні закономірності зв'язку, ескалації привілеїв або витоку даних, які можуть свідчити про порушення безпеки або внутрішні атаки.

Статистичне профілювання передбачає вивчення кількісних вимірювань і статистичних аспектів поведінки користувачів та IT-об’єктів, таких як частота, тривалість, обсяг і зміни. Використовуючи статистичні підходи, такі як середнє значення, стандартне відхилення, гістограми й аналіз часових рядів для поведінкових даних, системи UEBA можуть виявляти винятки, закономірності та статистичні аномалії, що вказують на події безпеки або порушення політик.

Контекстуальний аналіз оцінює закономірності поведінки користувачів та IT-об’єктів, враховуючи характеристики середовища, такі як ролі користувачів, права доступу, час доби, місцезнаходження і критичність активів, до яких здійснюється доступ. Контекстуалізуючи поведінку у відповідному середовищі, системи UEBA можуть розрізняти законну та підозрілу активність, зменшуючи кількість хибнопозитивних результатів і підвищуючи точність виявлення загроз.

Моделювання на основі МН. Методи МН мають вирішальне значення для моделювання й аналізу складних поведінкових моделей у системах UEBA. Методи навчання під наглядом та без нагляду, напівкерованого навчання використовуються для навчання на основі минулих даних, адаптації до змінних загроз ті виявлення аномалій та проблем безпеки в режимі реального часу.

Статистичний аналіз. UEBA значною мірою спирається на статистичний аналіз, щоб отримати кількісне уявлення про закономірності, тенденції та аномалії в мережі або системі організації. Рішення UEBA використовують різноманітні статистичні методології для аналізу даних про поведінку користувачів та IT-об’єктів, виявлення відхилень від типової активності та виявлення можливих ризиків безпеці [28].

2.2 Огляд ринку продуктів поведінкової аналітики

Рішення для аналізу поведінки користувачів та об'єктів (UEBA) більше не є необов'язковими в корпоративній кібербезпеці - вони є критично важливими. У сучасному складному кіберсередовищі, де зловмисники часто проходять повз традиційні засоби захисту, засоби UEBA дозволяють організаціям виявляти незвичайну поведінку, зупиняти внутрішні загрози та викривати атаки до їх ескалації. Використовуючи ШІ, МН та поведінкові базові показники, ці платформи дозволяють командам безпеки переходити від реактивного до проактивного захисту.

Ринок рішень UEBA значно еволюціонував за останні роки. Рішення, які починалися як нішеві пропозиції для великих підприємств, перетворилися на інструменти широкого вжитку, які бездоганно інтегруються із SIEM, SOAR та хмарними системами безпеки. Аналіз публікацій від провідних експертних організацій і виробників засобів кібербезпеки за 2024-2025 роки [30-34] показав, що найбільш затребуваними є рішення від компаній-лідерів галузі, таких як Exabeam, Fortinet, IBM, Microsoft, Rapid7, Splunk (Рис. 2.4). Проаналізуємо кращі продукти з поведінкової аналітики детальніше.

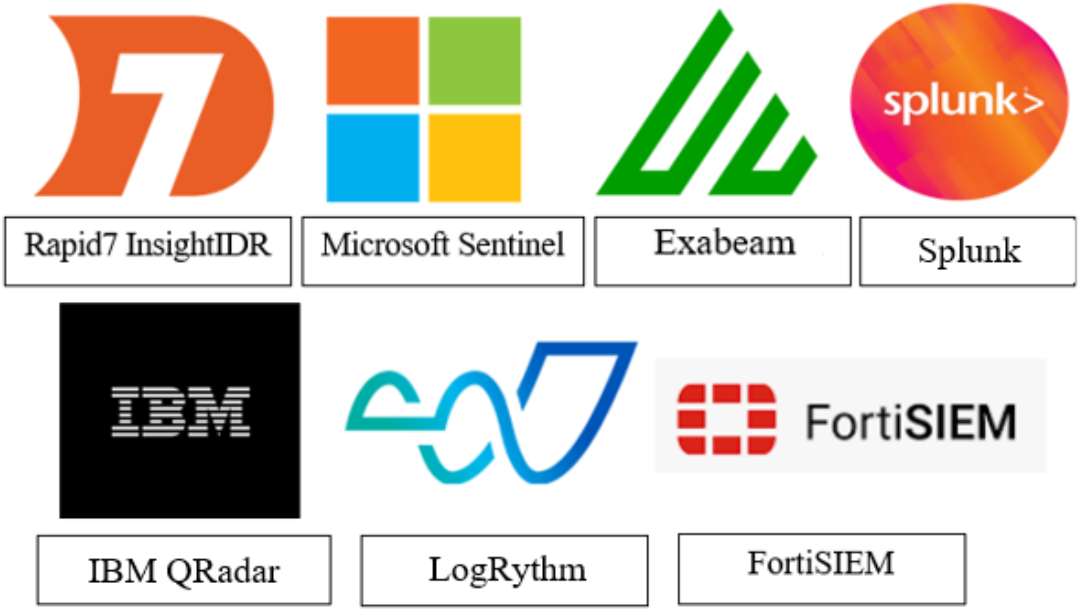


Рис. 2.4. Кращі рішення UEBA

Exabeam – це постачальник послуг безпеки, який пропонує UEBA як одну зі своїх основних можливостей у межах New-Scale SIEM. Ключові функції цього рішення охоплюють часові шкали подій, контроль доступу на основі ролей і можливість зберегти вже існуючу платформу SIEM компанії. Exabeam інтегрується із сотнями сторонніх інструментів безпеки, а також широким переліком систем-джерел даних, не пов'язаних із безпекою. Рішення від Exabeam рекомендують організаціям, яким потрібен широкий спектр джерел даних.

Відзначимо ключові риси Exabeam, серед яких можливість інтеграції з рішеннями від інших постачальників SIEM, що вже використовуються в компанії (крім цього Exabeam може інтегруватися з такими продуктами, як Microsoft 365, VMware ESXi, Salesforce та CrowdStrike); кореляція підозрілих сигналів від кількох продуктів для виявлення складних загроз у ході аналізу поведінки; формування груп однорангових користувачів і пристроїв на основі зв'язку між ними, наприклад, внутрішніх користувачів в одному бізнес-відділі; ідентифікація аномальної поведінки суб’єкта або IT-об’єкта порівняно з власним базовим рівнем, однотипними суб’єктами/об’єктами або всіма контрольованими ідентифікаторами [35].

Відповідно до опитувань Gartner рішення Exabeam отримало досить високу оцінку за функціонал продукту (4,6 бали) і можливості інтеграції та розгортання продукту (4,4) (Рис. 2.5).

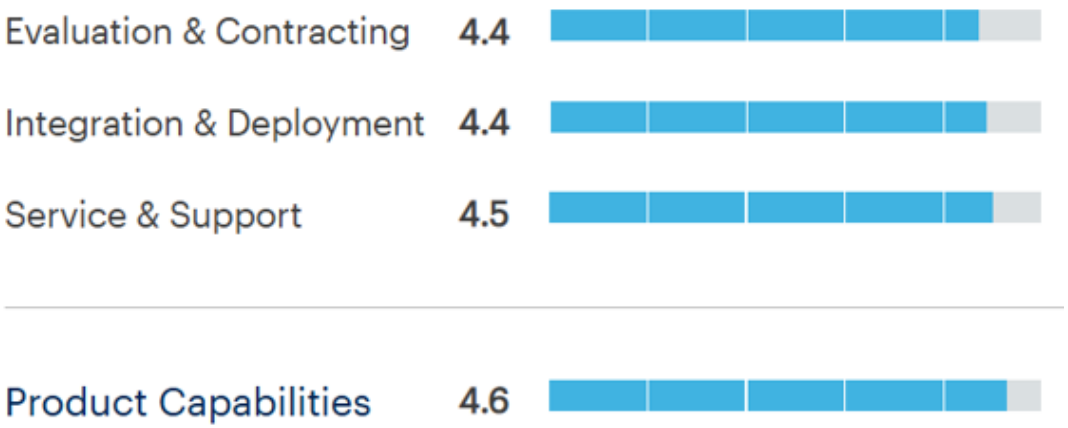


Рис. 2.5. Рейтинг рішення від Exabeam

Водночас, обслуговування і підтримка продукту Exabeam було оцінено на порівно високі 4,5 бали на відміну від більшості розглянутих нижче пропозицій від інших провідних постачальників рішень безпеки (4,2-4,3 бали).

У якості альтернативи потенційні покупці рішення від Exabeam розглядали продукти IBM (43%), Splunk (36%) і Microsoft (14%) [31].

Безсумнівними перевагами продукту Exabeam є можливість безлічі інтеграцій, включаючи із засобами, непов'язаними з безпекою; доступність «розумних» часових шкал подій і API для розробників. До недоліків належать нечіткі можливості автоматизованого виправлення; відсутність безкоштовної пробної версії і отримання рішення у вигляді керованої послуги.

FortiSIEM – це комплексний продукт SIEM від відомого постачальника мережевої безпеки Fortinet. FortiSIEM охоплює такі функції UEBA, як ідентифікація внутрішніх загроз, оцінка ризиків користувачів та виявлення скомпрометованих облікових записів. Це рішення є прийнятним для будь-якого бізнесу, однак буде особливо корисним для команд, які вже використовують мережеві пристрої Fortinet, що забезпечить ефективний обмін даними.

Варто відзначити такі основні риси продукту як виявлення аномальної поведінки кінцевих точок, зокрема скомпрометований системний обліковий запис або діяльність халатного чи зловмисного інсайдера; розвідка загроз із використанням джерел загроз, які надають файл CSV або підтримують стандарти STIC/TAXII 1.0, 1.1 та 2.0; реалізація множинних механізмів кореляції в режимі реального часу; виявлення аномальну поведінку IT-пристроїв і користувачів на основі МН без розробки власних правил [36].

FortiSIEM була оцінена на 4,5 бала як за функціональні можливості, так і можливості інтеграції та розгортання продукту (Рис. 2.6).

Компанії, які розглядали покупку продукту Fortinet, у якості аналогів визначили рішення від Microsoft (60%), Splunk (45%) та IBM (25%) [31].

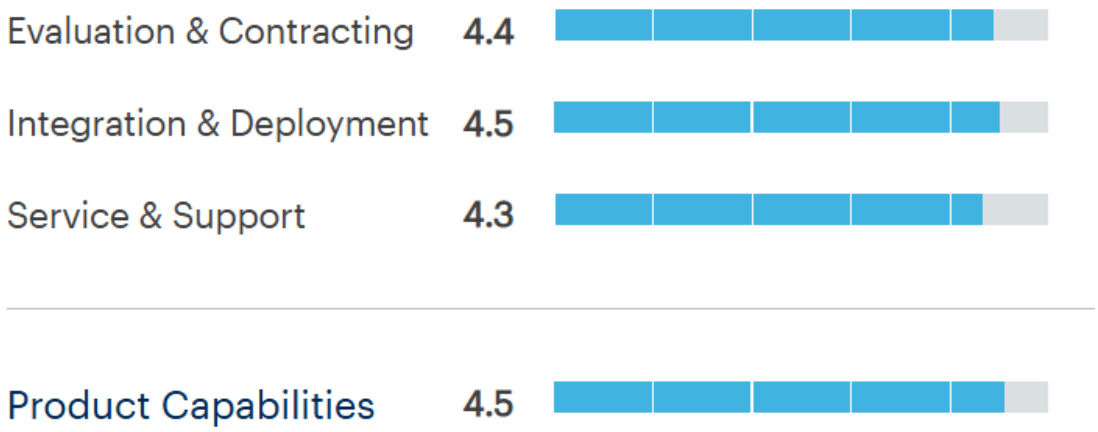


Рис. 2.6. Рейтинг рішення від Fortinet

Переваги FortiSIEM охоплюють наявність багатьох адміністративних функцій, таких як API; можливості розгортання як у хмарі, так і локально; підтримка пристроїв Інтернету речей. До слабких місць систем відносять відсутність деяких функцій UEB, а також безкоштовної пробної версії і вбудованих інструкцій з реагування.

IBM QRadar є SIEM-рішенням з хорошою репутацією, яке забезпечує функції аналізу поведінки користувачів та IT-об'єктів через QRadar User Behavior Analytics. Воно поєднує сильні правила кореляції з поведінковим моделюванням, допомагаючи великим організаціям виявляти внутрішні загрози і незвичайну активність облікових записів.

Характеризуючи, слід відзначити такі його функції: вивчення загроз і відхилень у поведінці користувачів, експертиза інцидентів, в результаті яких здійснюється глибокий аналіз пакетів для розслідування; профілювання ризиків та створення уніфікованих ідентифікаторів користувачів на основі існуючих даних про події та потоки у корпоративних системах; спрощення звітності для регульованих секторів через використання шаблонів відповідності.

IBM QRadar отримав досить високі оцінки за функціонал продукту (4,3 бали) і можливості інтеграції та розгортання продукту (4,4) відповідно до опитувань Gartner (Рис. 2.7).

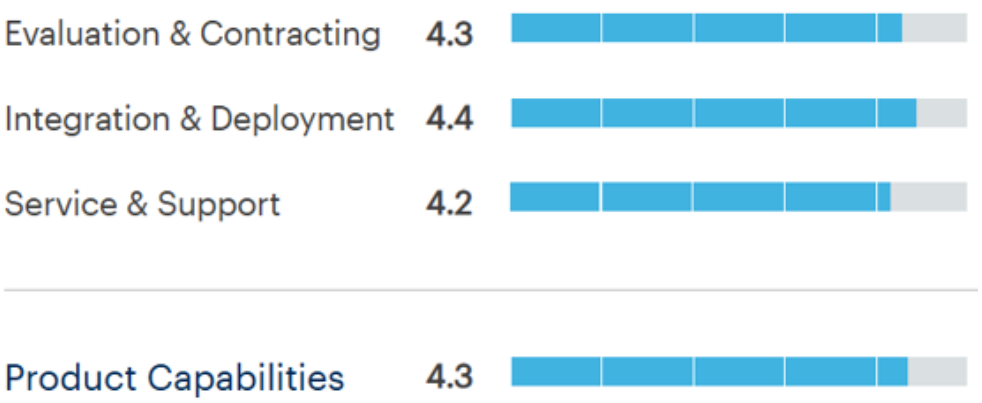


Рис. 2.7. Рейтинг продукту IBM QRadar

Альтернативними варіантами покупці IBM QRadar вважають рішення від Microsoft (36%), Splunk і Fortinet (27% кожен) [31].

Перевагами рішення від IBM вважаються поєднання сильної кореляції та поведінкового аналізу, широкі можливості інтеграції з іншими рішеннями безпеки, орієнтованість на забезпечення нормативної відповідності. Серед недоліків відзначають потребу у значних ресурсах для локального розгортання системи, громіздкість інтерфейсу і довший час упровадження у порівнянні з хмарними рішеннями [35, 37].

LogRhythm SIEM пропонує потужну платформу SIEM з функціональністю UEBA, використовуючи МН для виявлення аномалій, таких як внутрішні загрози, атаки методом повного перебору та зловживання адміністратором. Функція моніторингу цілісності файлів LogRhythm виявляє несанкціонований доступ до файлів. Рішення є оптимальним для компаній, які зберігають і обробляють велику кількість конфіденційних даних, а також досвідчених команд із розширеними вимогами до SIEM.

Насамперед слід звернути увагу на такі основні параметри продукту: інтеграція як з комерційними, так і з відкритими каналами інформації про загрози; індивідуальне оцінювання аномалій з метою визначення пріоритетів потенційних загроз для розслідування й усунення наслідків; SmartResponse - автоматизація процесів реагування на загрози, зокрема карантину файлів і блокування URL-адрес, що дозволяє зменшити ручну працю; здатність платформи визначати моделі аномальної поведінки користувача або IT-об’єкта

у порівнянні з власним базовим рівнем, аналогічними особами/засобами або всіма контрольованими ідентифікаторами [38].

Плюсами системи LogRhythm є здійснення моніторингу файлів, що допомагає командам захищати конфіденційні дані; можливості розгортання локально або в хмарі. Серед недоліків відзначають складність використання для невеликих команд; недостатність прозорої інформації про ціни; відсутність безкоштовної пробної версії.

Microsoft Sentinel – це хмарне рішення SIEM, яке також забезпечує функціональність UEBA. Його функції охоплюють пріоритезацію інцидентів, групування однорангових пристроїв і встановлення часових рамок інцидентів. Окрім цих інструментів, Sentinel пропонує багато інших функцій UEBA та SIEM, в тому числі розширених можливостей безпеки. Інструмент може інтегруватися з продуктами Defender і XDR від Microsoft, є оптимальним вибором для компаній, що працюють з хмарними сервісами Azure.

Основними характеристиками є можливості широкого збору даних від усіх користувачів, пристроїв, програм та інфраструктури, як локально, так і в кількох хмарах; виявлення горизонтального переміщення потенційного зловмисного актора між програмами або службами; проведення розслідувань з використанням алгоритмів ШІ, які значно пришвидшують процеси аналізу й виявлення загрози і аномалій; відсутність обмежень на запити через хмарну природу рішення [39].

Споживачі даного продукту Microsoft однаково високо (4,5 з 5-ти балів) оцінили можливості продукту загалом і можливості інтеграції та розгортання (Рис. 2.8).

Інші постачальники, яких розглядали покупці цього рішення від Microsoft, охоплюють IBM (19% від загальної кількості покупців), Fortinet (17%) [31].

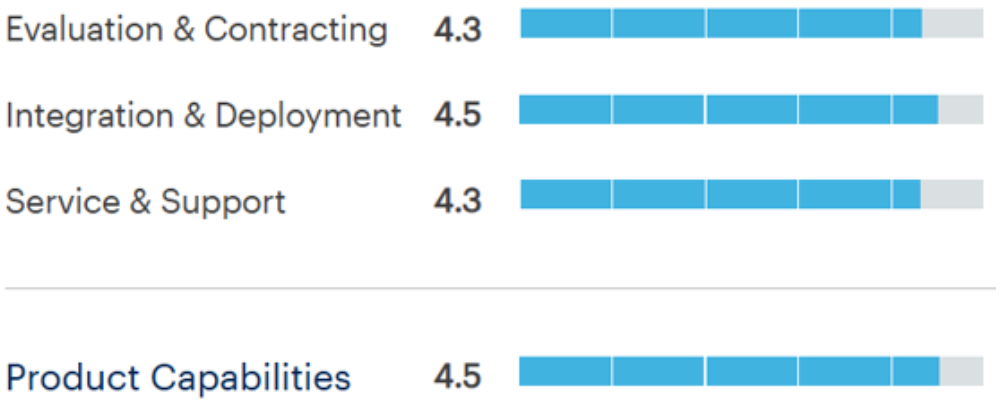


Рис. 2.8. Рейтинг продукту Microsoft Sentinel

Плюсами Microsoft Sentinel є наявність багатьох основних і розширених функцій UEBA, можливість отримувати рішення у вигляді керованої послуги. Зауваження фахівців викликають обмежені можливості розгортання і відсутність демонстрації продукту, досить висока цінова структура.

Rapid7 InsightIDR - це комбінована хмарна платформа SIEM та XDR, яка постійно аналізує звичайну активність користувачів поза межами визначених індикаторів компрометації. InsightIDR розроблений для виявлення загроз, які часто пропускаються традиційними засобами безпеки, зокрема атаки від імені працівників компанії, або спроби викрадання даних від зловмисних інсайдерів. Рішення охоплює потужний набір функцій і адміністративні можливості.

Основні характеристики InsightIDR охоплюють: автоматичну кореляцію активності, тобто співвіднесення подій у мережі клієнта з конкретними користувачами та IT-об'єктами, які стоять за цими подіями; здатність системи адаптуватися до користувачів та об'єктів у мережі на основі базових показників їх активності, щоб продовжувати визначати нормальну поведінку; відстеження користувачів, які можуть потенційно становити підвищений ризик; виявлення неправильної конфігурації через візуальний пошук у журналі та попередньо створені картки відповідності для виявлення аномалій [40].

Відповідно до даних Gartner компанії-споживачі даного рішення високо оцінили можливості інтеграції та розгортання продукту (4,7 з 5-ти максимальних балів), а також можливості продукту загалом (4,5 балів) (Рис. 2.9).

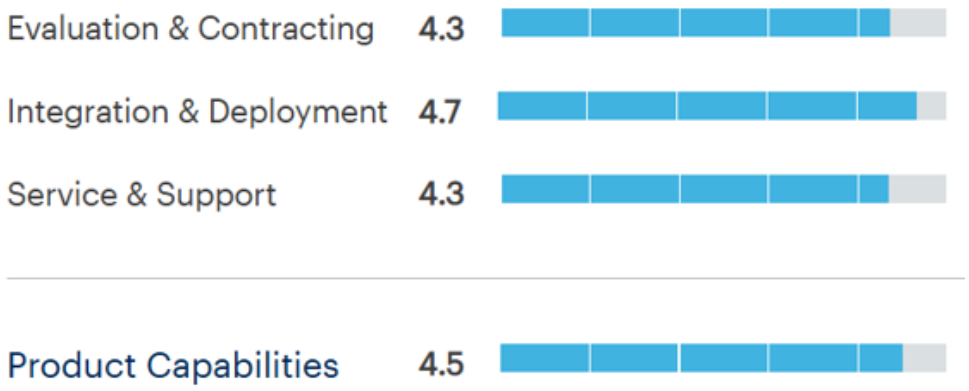


Рис. 2.9. Рейтинг продукту Rapid7 InsightIDR

У якості альтернативи потенційні покупці Rapid7 розглядали продукти Splunk від Cisco Systems (42%), Microsoft (31%), Exabeam (14%) [31].

До переваг InsightIDR відносять наявність багатьох розширених функцій, а також наявність досить прозорої інформації про ціни і безкоштовної пробної версії на один місяць. Водночас, до недоліків рішення відносять необхідність часу для вивчення платформи, нечіткість функції пріоритезації інцидентів, відсутність підтримки пристроїв Інтернету речей.

Splunk UEBA – це досить рідкісний на ринку окремий продукт для поведінкової аналітики, який надає можливості, необхідні командам для моніторингу, аналізу та виявлення загроз з боку користувачів. Організації можуть покращити свою безпеку за допомогою робочого процесу Splunk щодо загроз незалежно від розміру бізнесу чи набору навичок. Ця технологія звужує кількість первинних подій у масштабі бізнесу до кількох можливих загроз. Splunk UEBA є найбільш підходящим рішенням для команд, які потрібують окремого засобу, призначеного виключно для аналітики користувачів.

Основні характеристики рішення від Splunk: пріоритезація інцидентів із визначенням власного балу ризику, що дозволяє реагувати на найважливіші проблеми в першу чергу; використання кількох моделей аномалій і загроз із фокусом на виявленні загроз зовні організації; розширене виявлення загроз, серед яких захоплення облікового запису, діяльності командування й управління, а також експлойтів браузера; виявлення витоку даних (вилучення

або передачу конфіденційної інформації компанії з місць їхнього зберігання) [41].

Рішення Splunk отримало високі оцінки за функціонал продукту (4,5 бали), можливості інтеграції та розгортання продукту (4,6) і наряду Exabeam 4,5 бали за обслуговування і підтримку продукту (Рис. 2.10).

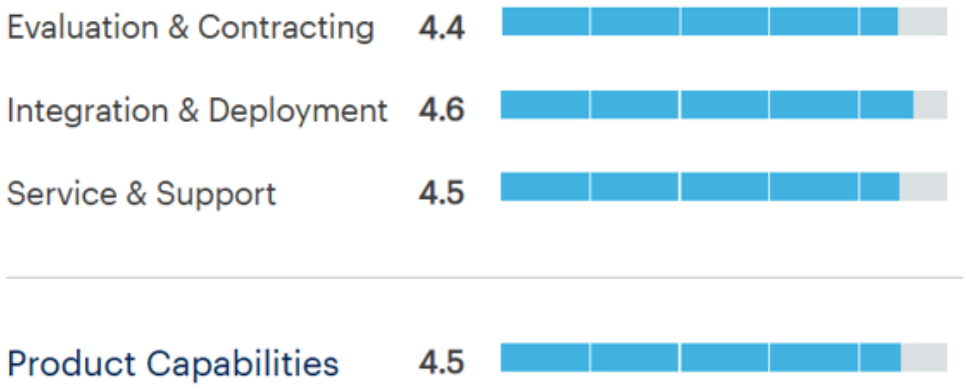


Рис. 2.10. Рейтинг рішення від Splunk

Потенційні покупці як альтернативу Splunk розглядали продукти IBM (30% від загальної кількості покупців), Microsoft (24%) і Fortinet (19%) [31].

До переваг Splunk UEBA слід віднести можливості обробки й фільтрації величезної кількості необроблених подій; ціноутворення на основі врахування даних дозволяє платити по мірі використання; наявність технічного менеджера облікових записів. Мінуси охоплюють відсутність деяких функцій, які є у конкурентів; здійснення виявлення й аналізу тільки поведінки користувачів без урахування дій IT-об’єктів; відсутність інтеграції з Active Directory.

2.3 Рекомендації щодо застосування кращих рішень UEBA

Дослідження джерел [29-33] дозволило зробити висновки щодо особливостей рішень та їх прийнятності для використання у різних організаціях і галузях. Встановлено, що:

- Exabeam вважається найкращим варіантом для хмарної та розширеної поведінкової аналітики, а також відкритим для інтеграції рішень безпеки від сторонніх розробників;

- FortiSIEM – є найбільш пристосованим продуктом для використання в мережевих середовищах;
- IBM QRadar характеризують як найбільш прийнятний варіант для середовищ безпеки, орієнтованих на дотримання нормативних вимог і проведення аудитів, тобто доцільно використовувати продукт у жорстко регульованих галузях, наприклад фінансовій і охорони здоров'я;
- LogRhythm є оптимальним вибором для інтегрованого використання систем SIEM та UEBA в разі їх локального розгортання, також засіб забезпечує розширені потреби SIEM;
- Microsoft Sentinel найкраще виконує основні функції UEBA, також продукт доцільно використовувати організаціям, які вже працюють в екосистемі Azure;
- Rapid7 InsightIDR є найкращим загальним рішенням поведінкової аналітики, забезпечує швидке розгортання і є достойним прикладом продукту UEBA, готового до негайного використання;
- Splunk UEBA найбільше підходить для організацій, які мають на меті забезпечити масштабоване й налаштоване під потреби організації/вимоги нормативних документів виявлення, Splunk UEBA є одним із небагатьох популярних автономним рішень для аналітики користувачів.

Узагальнені дані про переваги та рекомендації щодо використання рішень UEBA від провідних постачальників [31] показані в таблиці 2.1.

Таблиця 2.1.

Характеристика рішень UEBA

Виробник	Характеристики	Рекомендації: для кого
Exabeam	хмарне виявлення на основі поведінки з автоматизованими часовими шкалами інцидентів	для команд, яким прагнуть швидкого процесу розслідування на основі контекстних сповіщень
FortiSIEM	використання в мережевих середовищах	для команд, які працюють із мережевими пристроями виробника Fortinet
IBM QRadar	забезпечення нормативної відповідності і проведення аудитів	для команд безпеки/SOC підприємств жорстко регульованих галузей
LogRhythm UEBA	рішення, тісно інтегроване у стек SIEM	для команд безпеки, які віддають перевагу уніфікованій реєстрації подій у поєднанні з аналітикою поведінки
Microsoft Sentinel	хмарна аналітика поведінки іт-об’єктів з основним покриттям Azure/365	для команд, які працюють з хмарними сервісами Microsoft
Rapid7 InsightIDR	просте розвертання із вбудованими робочими процесами SOC	для команд середнього розміру, які прагнуть швидкого результату і універсального підходу до виявлення загроз
Splunk UEBA	автономне рішення / інтеграція з екосистемою Splunk SIEM	для команд із розвиненими процесами SOC і високою пропускною здатністю даних

Також здійснено аналіз перелічених вище автономних або інтегрованих у комплексні продукти безпеки рішень поведінкової аналітики (Табл. 2.2) за такими критеріями як:

- основні функції, зокрема інтегрована аналітика загроз, управління сповіщеннями, пріоритезація інцидентів, журналювання тощо;
- додаткові функції, такі як вилучення даних і автоматизоване виправлення, контроль доступу на основі ролей та виявлення прихованих активностей;

Таблиця 2.2.

Кращі рішення поведінкової аналітики

Критерій	Опис критерію	Кращі рішення
Основні функції	інтегрована аналітика загроз, управління сповіщеннями, пріоритезація інцидентів, журналювання тощо	Microsoft
Додаткові функції	вилучення даних і автоматизоване виправлення, контроль доступу на основі ролей і виявлення прихованих активностей	Rapid7
Простота використання і адміністрування	інтуїтивно зрозумілі робочі процеси розслідування, документування і простота адміністрування	Exabeam
Ціноутворення	прозорість ціноутворення постачальників, а також тривалість підписки і безкоштовні пробні версії	LogRhythm
Підтримка клієнтів	наявність каналів підтримки (телефон, електронна пошта і живий чат, а також демонстрація і можливість мати технічного менеджера облікових записів)	Exabeam, Splunk

- зручність і простота використання й адміністрування;
- цінова політика, в тому числі наявність безкоштовної пробної версії;
- підтримка клієнтів, включаючи різні канали та наявність демонстрацій.

Розглянемо детальніше основні завдання досліджуваних продуктів поведінкової аналітики й методи їх досягнення [42-49].

Exabeam UEBA як доповнення корпоративної SIEM дозволяє протидіяти внутрішнім загрозам, крадіжкам облікових даних та іншим складним атакам в рамках корпоративної SIEM завдяки механізму виявлення, який не має аналогів на ринку і фіксує поведінку користувачів і пристроїв для виявлення аномалій на основі ризиків та визначення пріоритетів сповіщень. Рішення забезпечує виявлення та визначення пріоритетів аномалій шляхом встановлення базових показників користувачів і пристроїв для визначення аномалій та застосування бізнес-факторів для оптимізації оцінки ризику, ідентифікує людей та IT-об’єкти у вхідних проаналізованих журналах через кореляцію атрибутів і контекстних даних, а також інтегрує дані з різних джерел, щоб забезпечити видимість у локальних і хмарних середовищах. Система максимізує продуктивність за допомогою ШІ й автоматизації: автоматизовані часові шкали впорядковують пов'язані виявлення негайно та хронологічно, візуалізуючи повний масштаб загрози; моделі аналізу даних підсумовують аномальну активність, розроблені схеми дій пришвидшують реагування та зменшують кількість ручних процедур.

UEBA FortiSIEM вирішує такі основні завдання: розширене виявлення складних кіберзагроз із застосуванням МН для виявлення аномальної поведінки і надалі - потенційних інцидентів безпеки по мірі їх появи; забезпечення комплексної видимості шляхом відстеження активності користувачів і пристроїв, забезпечуючи цілісне уявлення про мережеве середовище; «безшовна» інтеграція з існуючими системами безпеки, що покращує загальний рівень безпеки без порушення поточних операцій; масштабоване розгортання, яке доступне як хмарний сервіс або локальний віртуальний пристрій; зручний інтерфейс, який має інтуїтивно зрозумілу графічну платформу для виявлення аномалій та пошуку загроз, що спрощує процес виявлення та зменшення

ризиків безпеки. Інтеграція МН зменшує обсяги ручного моніторингу, дозволяючи ІТ-командам зосередитися на стратегічних ініціативах, зберігаючи при цьому надійний рівень безпеки.

Програма *IBM QRadar UEBA* покликана надати споживачам кращу видимість інсайдерських потоків, виявляти аномальну поведінку, швидко визначати ризикованих користувачів та ІТ-об'єкти для отримання змістовної аналітики. Відмінними рисами продукту є наявність майстера імпорту користувачів, який переносить їхні дані безпосередньо з програми UEBA, LDAP-сервера, сервера Active Directory, довідкових таблиць і CSV-файлів, а також може створювати власні атрибути. У межах оцінювання ризиків система створює профілі ризиків, призначаючи ризик різним сценаріям безпеки, залежно від серйозності та надійності інциденту, а також використовуючи існуючі дані про події та потоки у корпоративній системі QRadar. Уніфікація ідентифікаційних даних користувачів шляхом об'єднання різних облікових записів дозволяє об'єднувати дані про ризик і трафік для різних імен користувачів у додатку, щоб краще контролювати їхні дії і запобігати атакам. UEBA автоматично виявляє ІТ-об’єкти, такі як IP-адреси, імена хостів критичних пристроїв, сервери, і відстежує їх на відповідність увімкненим сценаріям використання. Налаштування порогу оцінки ризику дозволяє генерувати сповіщення у разі досягнення порогового рівня. Використання МН уможливлює профілювання і кластеризацію часових рядів, створення прогнозних моделей і базових рівнів нормальної поведінки.

UEBA від InsightIDR надає своїм клієнтам можливості максимально досяжної видимості корпоративного ІТ-середовища завдяки постійному моніторингу користувачів та облікових даних, надійного захисту найбільш чутливих даних та інформації, а також виявлення внутрішніх і раніше невідомих загроз. Досягнення зазначених цілей забезпечують такі методи як автоматизоване виявлення загроз із використанням алгоритмів МН для виявлення складних атак, таких як фішинг або внутрішні загрози; глибокий аналіз подій і даних користувачів; інтеграція й ефективне функціонування

спільно з іншими інструментами безпеки для створення єдиної екосистеми кіберзахисту; реагування на інциденти й автоматизоване управління інцидентами.

LogRhythm UEBA, хмарне доповнення до платформи LogRhythm SIEM, використовує МН для виявлення аномалій, пов'язаних з потенційними атаками користувачів, такими як внутрішні загрози, скомпрометовані облікові записи, зловживання адміністратором і неправильне використання. Разом LogRhythm UEBA та перевірені на практиці моделі загроз LogRhythm SIEM AI Engine забезпечують цілісний аналіз і глибоке розуміння активності користувачів і пристроїв, які в іншому випадку залишилися б непоміченими. LogRhythm UEBA виявляє зміни в поведінці користувачів, які сигналізують про потенційні загрози. Аналітики можуть використовувати окремі оцінки аномалій і зведену оцінку користувачів/IT-об’єктів для визначення пріоритетів аномалій, що сприятиме швидким і більш ефективним розслідуванню та реагуванню.

Microsoft UEBA є рішенням, інтегрованим у Microsoft Sentinel, і забезпечує для своїх клієнтів унікальні можливості щодо виявлення загроз у режимі реального часу за допомогою базових ліній, навчених ШІ; кореляції між ідентифікаторами, пристроями і місцями розташування для додавання контексту; виділення відхилень однорангових користувачів між посадами та шаблонами доступу; виявлення внутрішніх загроз без написання власних правил кореляції. UEBA розроблено, щоб допомогти аналітикам безпеки виявляти загрози, аналізуючи моделі поведінки користувачів, пристроїв, програм та інших IT-об'єктів. UEBA використовує МН для визначення базової регулярної активності та виявлення аномалій, які не викликають традиційних сповіщень, таких як скомпрометовані облікові записи. Перевагою продукту є здатність створювати глибокі профілі поведінки, які долучають дані з плином часу та між групами однотипних користувачів або пристроїв, допомагаючи виявляти випадки, навіть коли аномальна поведінка здається малопомітною. Рішення UEBA від Microsoft також надає часову шкалу поведінки для кожного об’єкта, що допомагає аналітикам відстежувати тенденції активності й розуміти контекст підозрілих

закономірностей. Ці дані генеруються за допомогою вбудованих запитів мови запитів Kusto (KQL) та розширених аналітичних правил, які збагачують існуючу систему виявлення. Також плюсом Sentinel UEBA, зокрема для організацій з обмеженими ресурсами інженерії безпеки, є його швидке впровадження.

Рішення *Splunk UEBA* забезпечує проактивне виявлення та зменшення внутрішніх загроз; покращення видимості безпеки за допомогою аналізу ризиків для користувачів та об'єктів; оптимізацію ефективності SOC за допомогою автоматичного виявлення та визначення пріоритетів загроз. Методи, які дозволяють задовольнити очікування споживачів, охоплюють поведінкову аналітику та МН, оцінювання й агрегацію ризиків для об'єктів, застосування ШІ та моніторинг LLM, аналіз ризиків у режимі реального часу за допомогою контекстного аналізу, автоматизоване виявлення та визначення пріоритетів загроз, а також безперешкодну інтеграцію зі Splunk Enterprise Security.

Висновки до розділу 2

Встановлено, що розвиток UEBA систем з початку 2000-х років охопив еволюцію базових методів поведінкового аналізу до складних рішень, що використовують МН, аналітику великих даних і автоматизацію. Впровадження хмарних технологій і масштабованість стали важливими рисами наприкінці 2010-х років, тоді як в останні роки спостерігається зсув у бік автоматизації, оркестрації та реалізації підходів на основі ШІ. Сьогодні UEBA є основним компонентом сучасних архітектур кібербезпеки і охоплюють такі складові збір і обробка даних; алгоритми МН; поведінковий і контекстний аналіз; виявлення аномалій; оцінка ризиків і пріоритезація; візуалізація і звітність.

UEBA використовують різноманітні методи МН для аналізу моделей поведінки користувачів та ІТ-об’єктів, а також виявлення аномалій або можливих вразливостей безпеки ІКС організації, зокрема алгоритми

некерованого і керованого навчання, навчання з підсиленням, моделі глибокого навчання, зокрема глибокі нейронні мережі (DNN), алгоритми виявлення аномалій, такі як моделі гаусової суміші (GMM), ізоляційний ліс, однокласова SVM і надійні статистичні підходи, підходи ансамблевого навчання, зокрема пакування, бустинг і стекування.

Деякі типові методології моделювання поведінки, що використовуються в UEBA, охоплюють моделювання на основі профілів, аналіз послідовності, моделювання на основі графів, статистичне профілювання, контекстуальний аналіз, моделювання на основі МН, статистичний аналіз.

Як показало дослідження, ринок рішень UEBA значно еволюціонував за останні роки. Рішення, які починалися як нішеві пропозиції для великих підприємств, перетворилися на інструменти широкого вжитку, які бездоганно інтегруються із SIEM, SOAR і хмарними системами безпеки. Аналіз публікацій від провідних експертних організацій і виробників засобів кібербезпеки за 2024-2025 роки показав, що найбільш затребуваними є рішення від компаній-лідерів галузі, таких як Exabeam, Fortinet, IBM, Microsoft, Rapid7, Splunk.

Встановлено особливості рішень та їх прийнятності для використання у різних організаціях і галузях. Так, зокрема рішення Exabeam вважається найкращим варіантом для хмарної та розширеної поведінкової аналітики; FortiSIEM – є найбільш пристосованим продуктом для використання в мережевих середовищах; IBM QRadar характеризують як найбільш прийнятний варіант для підприємств регульованих галузей; LogRhythm є оптимальним вибором для інтегрованого використання систем SIEM та UEBA в разі їх локального розгортання; хмарне рішення Microsoft Sentinel доцільно використовувати організаціям, які вже працюють в екосистемі Azure; Rapid7 InsightIDR є найкращим загальним рішенням поведінкової аналітики, яке забезпечує швидке розгортання і готовність до використання; Splunk UEBA найбільше підходить для організацій, які мають на меті забезпечити масштабоване й кастомізоване виявлення загроз.

РОЗДІЛ 3
ШТУЧНИЙ ІНТЕЛЕКТ ЯК ЗАСІБ РОЗШИРЕННЯ МОЖЛИВОСТЕЙ СИСТЕМ UEBA

3.1 Напрями застосування ШІ в кібербезпеці й поведінковій аналітиці

Практика показує, що впровадження алгоритмів ШІ та МН для виконання завдань кібербезпеки загалом і поведінкової аналітики зокрема відбувається надзвичайно швидко. Як свідчать результати дослідження Guruculum, поведінкова аналітика і на основі ШІ та МН покращує виявлення загроз і зменшує кількість хибнопозитивних спрацювань до 90%, роблячи більш ефективним захист організації від внутрішніх загроз [12]. З огляду на це 69% організацій вже використовують рішення безпеки на основі ШІ для виявлення та запобігання загрозам [48].

Очевидним є те, що ландшафт сучасної кібербезпеки різко і швидко змінився лише за останні кілька років. Зловмисники, чи то окремі хакери, чи державні організації, стають все більш витонченими, використовуючи нові тактики й інструменти, що базуються на електронній пошті, соціальних мережах або діпфейках, для проникнення та обходу традиційних систем виявлення загроз. Такі атаки спрямовані на доступ до критично важливих корпоративних активів або персональних даних з кінцевою метою викрадення цінної інформації та, часом, спричинення порушень нормальної роботи бізнесу.

Паралельно постачальники засобів безпеки і дослідницькі організації вдосконалюють технологічні інновації, щоб надавати передові інструменти та інтегровані рішення для прогнозування, запобігання, виявлення та пом'якшення загроз з дедалі більшою ефективністю та результативністю. Так, аналітики Gartner нещодавно запропонували концепцію безперервної адаптивної оцінки ризиків та довіри (Continuous Adaptive Risk and Trust Assessment, CARTA), щоб виділити інтегровані технології кібербезпеки і те, як їх можна використовувати на різних етапах захисту від кібератак [49].

Крім того, мережі 5G та хмарні обчислення змінюють спосіб і темп комунікації. Світ переходить на цифровий формат з безпрецедентно високою швидкістю, обсяг інформації та даних зростає вибуховими темпами, а величезні обсяги даних зараз доступні і контролюються, збираються, зберігаються, аналізуються та представляються за допомогою багатьох різних типів програм. Ці дані надходять з різноманітних джерел: кінцевих точок, мережевих пристроїв, мобільних пристроїв, хмари, окремих користувачів та інших об'єктів тощо. Виходячи з цього продуктивні й ефективні аналіз і використання цих даних є критично важливим завданням для великих і малих організацій.

Як результат, збирання, зберігання й аналіз цих даних більше не можуть виконуватися за допомогою традиційних ручних або автоматизованих методів виявлення і запобігання загрозам. Сьогодні автоматизація безпеки, особливо автоматизація, що базується на ШІ та МН, у пошуку, виявленні, аналізі та реагуванні на загрози, є однією з найактивніших сфер розвитку кібербезпеки.

ШІ використовується для застосування передових методів аналізу та логіки, включаючи МН, для інтерпретації подій, підтримки й автоматизації прийняття рішень, а також для допомоги адміністраторам у реалізації обґрунтованих і ефективних заходів реагування на загрози й атаки. Технології ШІ, такі як глибоке навчання МН, теорія графів і нейронні мережі, існують ще з початку 80-х років, однак з появою високошвидкісного Інтернету і доступністю передових програм і великих даних, технології ШІ досягли критичної маси й перетворилися на потужний набір інструментів, що допомагають запобігати і протидіяти відомим і невідомим видам кібератак.

Сучасні аналітики безпеки й адміністратори часто перевантажені обсягом даних, що їм надаються, а також поширеними сповіщеннями про загрози, що ускладнює проведення аналізу та вжиття належних і своєчасних заходів. Через всю цю динаміку постачальники безпеки й аналітики зараз активно звертаються до технологій ШІ та МН для вирішення проблем захисту від загроз, що було б неможливим лише за допомогою людських чи ручних процесів [50].

Моніторинг поведінки користувачів і виявлення аномалій на основі ШІ. Зловмисники часто коригують і видозмінюють свою поведінку для уникнення ідентифікації, що робить статичні механізми виявлення на основі політик і сигнатур менш ефективними через необхідність постійного оновлення та виправлення баз даних сигнатур.

Виявлення загроз на основі ШІ використовує МН та глибоке навчання для аналізу великих наборів даних, розпізнавання шаблонів і виявлення аномалій у режимі реального часу. Виявлення аномалій використовує ШІ для розрізнення нормальної та аномальної поведінки системи, виявлення потенційних кібератак, таких як експлойти нульового дня та передові стійкі загрози (APT).

UEBA на основі ШІ використовує МН для *встановлення базової поведінки користувачів і виявлення відхилень*, які можуть свідчити про внутрішні загрози або компрометацію облікових записів. Завдяки постійному моніторингу шаблонів входу, запитів на доступ і мережевої активності, ШІ здатен виявляти спроби несанкціонованого доступу, атаки на ескалацію привілеїв і крадіжку облікових даних. Цей підхід особливо ефективний для виявлення атак соціальної інженерії, таких як компрометація ділової електронної пошти (BEC) та фішингові шахрайства.

ШІ покращує *розвідку кіберзагроз* шляхом агрегування й аналізу даних про загрози з різних джерел, включаючи даркнет, бази даних атак, мережеві журнали, зовнішні канали розвідки загроз тощо. Ці системи здатні адаптуватися та навчатися на минулих інцидентах, покращуючи точність виявлення загроз з часом. Завдяки постійному навчанню на нових даних ці інструменти на базі ШІ можуть виявляти нові методи атак, гарантуючи, що команди безпеки залишаються готовими до раніше невідомих загроз. Прогнозна аналітика на базі ШІ прогнозує потенційні вектори атак, дозволяючи компаніям впроваджувати проактивні заходи безпеки до реалізації кібератаки.

Завдяки ШІ та МН більш ефективним підходом є *моніторинг поведінки* зловмисників на шляху атаки, а потім використання аналітики для створення моделей стандартних профілів або базових ліній поведінки для користувачів та

ІТ-об’єктів, таких як хости, програми, мережевий трафік тощо, у просторовому і часовому спектрах. Активність, яка є аномальною для цих стандартних базових ліній, позначається як підозріла, і адміністратори безпеки отримують сповіщення для подальшого аналізу. Два найпоширеніші випадки використання аналізу поведінки - виявлення зловмисних інсайдерів і зовнішніх зловмисників, які проникають у їхні організації (скомпрометовані інсайдери) [50].

Наприклад, інструменти моніторингу загроз на базі ШІ, такі як QRadar від IBM або брандмауери на базі ШІ від Cisco, аналізують мережеві дані в режимі реального часу, щоб виявляти і реагувати на несанкціонований доступ, шкідливе ПЗ та спроби фішингу [51]. Такі системи скорочують час реагування, автоматизуючи заходи безпеки, такі як блокування підозрілих IP-адрес або ізоляція заражених кінцевих точок.

Використовуючи ШІ для *аналізу загроз* у режимі реального часу, організації можуть підвищити стійкість до кібератак, мінімізувати ручне втручання і зменшити ризик порушень безпеки. Однак постійне вдосконалення і людський нагляд залишаються важливими для запобігання хибним спрацьовуванням і забезпечення ефективності й етичності рішень безпеки на основі ШІ. На відміну від систем безпеки на основі правил, рішення на базі ШІ постійно навчаються на нових шаблонах атак, що робить їх більш адаптивними та ефективними проти нових кіберзагроз.

Прогнозні заходи безпеки використовують можливості ШІ для аналізу історичних даних, виявлення закономірностей і прогнозування потенційних вразливостей або загроз. Використовуючи такі методи, як прогнозна аналітика та МН, ШІ може передбачати кібератаки, включаючи спалахи шкідливого ПЗ, фішингові схеми та мережеві вторгнення. Здатність ШІ постійно контролювати великі набори даних у режимі реального часу робить його дуже ефективним у виявленні ранніх ознак атаки, що дозволяє організаціям вживати превентивних заходів до того, як станеться інцидент [52].

Аналітичний інструмент на основі ШІ контролює і вивчає нормальну поведінку користувачів та пристроїв/програм під час так званої «фази

навчання». Він перетворює всю інформацію на математичні моделі та результати, щоб встановити нормальні базові лінії поведінки, враховуючи винятки, такі як вихідні й заплановані IT-операції. Під час «фази виявлення» відповідний трафік користувачів та IT-об'єктів збирається, декодується і перевіряється на відповідність нормальним базовим рівням, а аномалії позначаються, якщо правила виявлення порушені.

На рис. 3.1 показано профіль користувача (кінцевої точки) з показниками його активності.

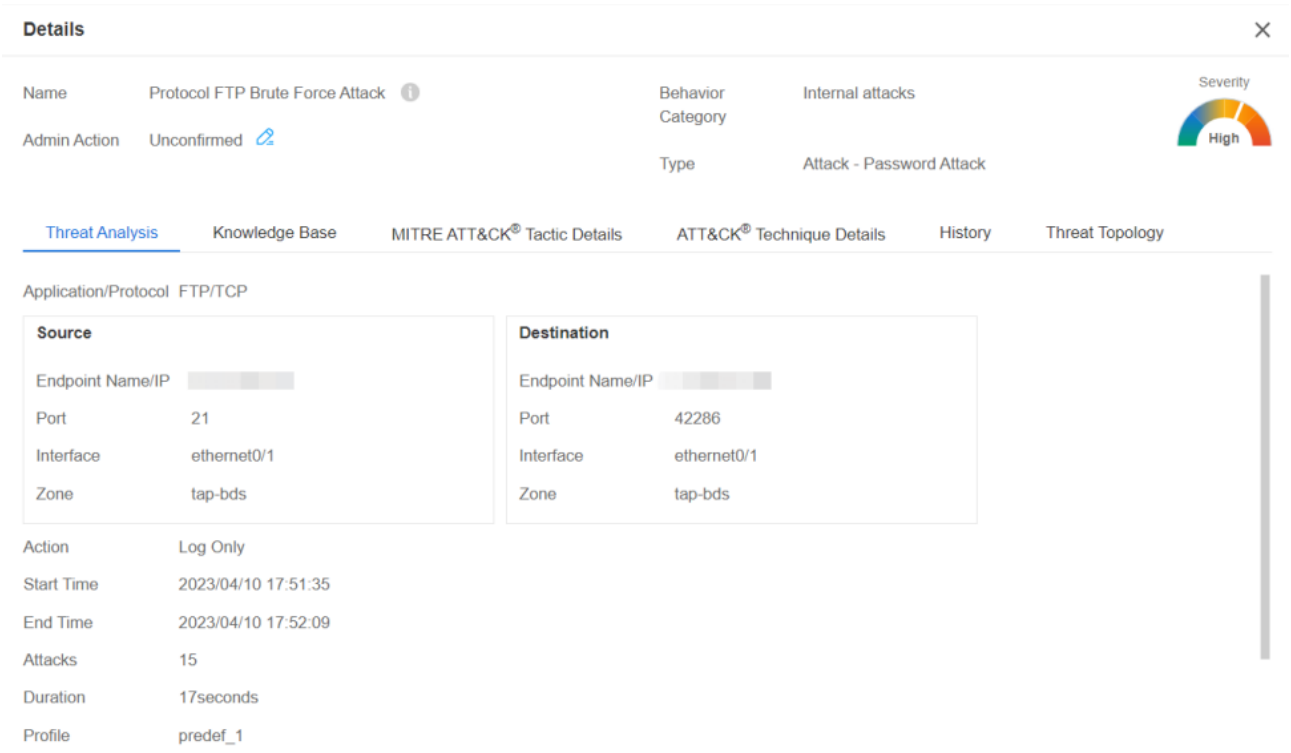


Рис. 3.1. Профіль користувача з показниками його активності

Аналіз мережевого трафіку на основі ШІ. Особливим напрямом функціонування UEBA є виявлення та реагування на мережу (NDR). Мережевий трафік, в тому числі необроблений трафік, метадані чи записи потоків (наприклад, NetFlow, сесії, журнали), містить багато інформації як на рівні додатків, так і на мережевому рівні, включаючи звичайні та шкідливі шаблони.

Враховуючи, що обсяг мережевого трафіку величезний і вимагає моніторингу в режимі реального часу, неможливо провести аналіз трафіку в

ручному режимі. Методи на основі ШІ або МН є найкращими засобами на допомогу аналітикам безпеки і мережевим адміністраторам у проведенні моніторингу й аналітики сучасних потоків мережевого трафіку в режимі реального часу. Ці методи допомагають встановити нормальні базові лінії трафіку, наприклад, звичайну ділову активність, доступ до файлів і передачу даних тощо. Це також сприяє забезпеченню повної видимості, особливо для горизонтального трафіку в корпоративних інтрамережах або між віртуалізованими мережами в центрах обробки даних. Таким чином можна виявити, проаналізувати і запобігати аномальній поведінці.

На рис. 3.2 показано механізм NDR на основі ШІ в робочій дії. Мережевий трафік, особливо вхідний і вихідний трафік від так званих критичних активів (зазвичай, важливих корпоративних серверів), моніториться, збирається та декодується в режимі реального часу. Набір важливих метаданих трафіку або PCAP періодично вибірково перевіряється та зберігається [50].

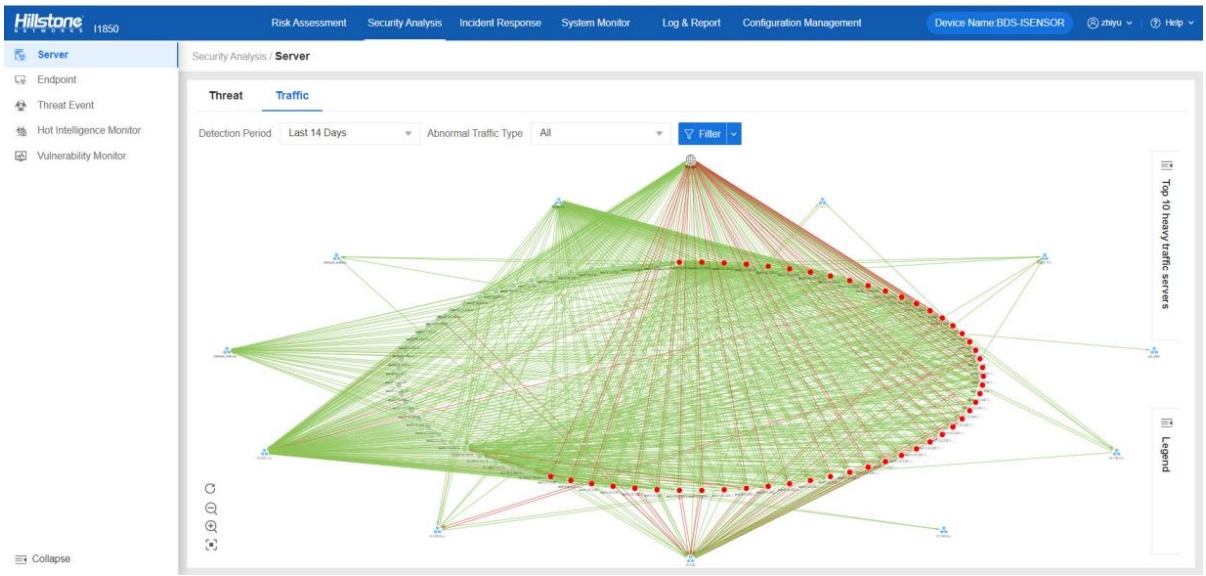


Рис. 3.2. Механізм NDR на основі ШІ

Механізм NDR виконує класифікацію трафіку та відображає його за допомогою математичних моделей для виявлення аномальних активностей. Після цього механізм кореляції на основі ШІ ініціює поведінковий аналіз кореляції, а також приймає та об'єднує додаткові історичні дані, інформацію про репутацію, канали розвідки про загрози та поведінку мережі. Мета полягає

в тому, щоб зменшити кількість хибних спрацьовувань і генерувати точні сповіщення про загрози з багатими доказами експертизи.

Аналіз поведінки користувачів і трафіку на основі ШІ відстежує поведінку мережевого трафіку зловмисника в ході атаки і допомагає виявляти підозрілу або аномальну поведінку користувачів, програм або трафіку. ШІ також може співвідносити додаткову інформацію розвідки загроз або експертизу в часі та просторі для генерування точних подій і сповіщень про загрози [53].

Виявлення загроз на основі ШІ за допомогою науки про дані. Щодня постачальники рішень безпеки та дослідницькі організації збирають до мільярдів зразків і даних шкідливого ПЗ. Аналіз цього «океану» даних вже давно є справою фахівців з обробки даних і до недавно був дуже складним і відповідальним, а часто і не повністю реальним завданням. Однак, використовуючи методи ШІ та МН, дослідники й аналітики автоматизують цей процес для досягнення бажаних результатів. Це також називається аналізом великих даних (Big Data analysis). Згідно з галузевими опитуваннями, більшість директорів з інформаційної безпеки й аналітиків безпеки вважають, що рішення на основі ШІ розвиваються та можуть бути використані в галузях виявлення шкідливого ПЗ і розширеного виявлення загроз [54].

Методи ШІ або МН у виявленні шкідливих програм на основі моделювання даних зазвичай включають інтелектуальний аналіз даних, навчання моделей і прогнозування. Під час інтелектуального аналізу даних великі обсяги необроблених даних очищаються, нормалізуються та класифікуються в набори даних, а характеристики сімейств шкідливих програм абстрагуються в набори ознак. Набори даних навчаються моделям під наглядом або без нагляду. У випадку МН цей процес контролюється, але його можна виконувати автоматично за допомогою методів глибокого навчання.

Живий трафік контролюється й аналізується відповідно до визначених правил і політик, а підозрілі пакети передаються попередньо встановленим моделям виявлення для прогнозування. Вихідні дані потім можуть бути передані до інших механізмів кореляції на основі ШІ, які включають більше

криміналістичних доказів і відповідних даних про загрози для генерації точних істинних позитивних результатів.

Діаграма на рис. 3.3 показує сповіщення про веб-загрозу від механізму виявлення МН. За лаштунками механізм виявлення загроз на базі МН постійно витягує характеристики мільйонів відомих сімейств шкідливих програм, використовуючи неконтрольовані алгоритми МН і математичне моделювання для виявлення їхніх спільних рис і навчання цих наборів даних.

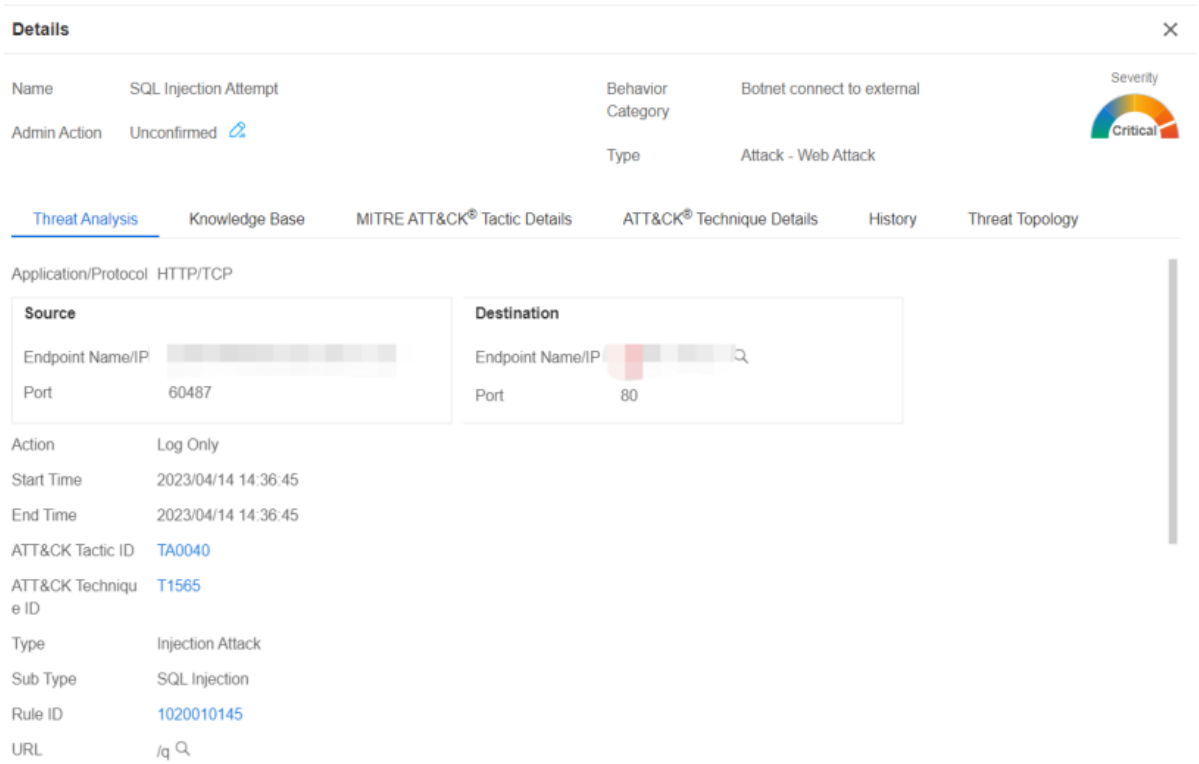


Рис. 3.3. Сповіщення про веб-загрозу на основі МН

Модель встановлюється на фізичних та віртуальних пристроях безпеки і виявляє як відомі сімейства шкідливих програм, так і ті, що з мутаціями. Після захоплення підозрілих пакетів, вони вивчаються й аналізуються відповідно до правил моделі МН і згодом подаються до моделі для прогнозування. Результати зазвичай надаються адміністраторам разом із збагаченою судово-медичною інформацією [50].

Автоматизація на основі ШІ. Ще одним важливим аспектом застосування ШІ в кібербезпеці є розширення можливостей оркестрації і автоматизації безпеки. На думку експертів компанії Gartner, ці технології

можуть швидко застаріти без переходу на передові рішення ШІ в операціях безпеки [55]. Сьогодні, через постійно зростаючі обсяги даних і ускладнення аналітики, співробітники служби безпеки постійно надто перевантажені обсягом даних і робочим навантаженням, не встигаючи за трудомісткими і ресурсномісткими операціями та робочими процесами безпеки.

Через цю динаміку технології ШІ та МН стали новою парадигмою в покращенні автоматизації безпеки. Зокрема, багато рутинних і повторюваних завдань інтелектуально розроблені та вбудовані в ігрові книги (Playbook). Ігрові книги – це набір правил для робочих процесів, які можна ініціювати, коли відбувається подія або активується доступ до даних. Подібно до програмного забезпечення, ігрові книги дозволяють користувачам створювати складні структури та логіку процесів залежно від вимог і бажаних результатів.

Мікроінструменти на основі ШІ або МН також можуть динамічно завантажуватися під час різних фаз робочого процесу, щоб допомогти у пошуку загроз, збагачувати криміналістичні докази, підвищувати точність виявлення, зменшувати хибнопозитивні результати, автоматизувати квитки на реагування та оптимізувати робочі процеси реагування на інциденти. Це звільнить фахівців з обробки даних та адміністраторів від виснажливих і рутинних завдань і дозволить їм зосередитися на вирішенні проблем та інших критично важливих для бізнесу видах діяльності.

Сучасні рішення оркестрації та автоматизації безпеки на основі генеративного ШІ дозволяють отримати низку суттєвих переваг, серед яких автоматизація комплексних завдань, адаптованих до нових загроз; легка інтеграція з використанням просунутих можливостей API й алгоритмів МН; більш ефективне функціонування в довготерміновій перспективі зі зменшенням ручного втручання; доповнення людської аналітики з фокусом на стратегічні завдання; зручність використання без елементів програмування; спрощений доступ до просунутих опцій автоматизації. Водночас, слід пам’ятати, що ШІ є тільки доповненням діяльності людини, а не його замінником [56].

3.2 Роль методів ШІ та МН у процесах сучасних UEBA-систем

Виявлення загроз, зокрема шкідливого ПЗ на основі ШІ аналізує динамічну поведінку та особливості ПЗ, щоб знайти шкідливу активність. Методи ШІ/МН використовуються для пошуку будь-яких характеристик шкідливого ПЗ та ідентифікації будь-яких загроз. Моделі керованого МН широко використовуються для виявлення будь-яких шкідливих програм шляхом навчання їх на великих мічених наборах даних зразків шкідливих загроз. Підходи глибокого навчання є винятковими, коли йдеться про завдання класифікації шкідливого ПЗ. Вони можуть автоматично вивчати складні шаблони, які використовуються для розрізнення звичайних і зловмисних програм, і вони не вимагають від експертів з безпеки вручну визначати сигнатури та правила.

Згорткові нейронні мережі (CNN), наприклад, використовуються для виявлення будь-якого шкідливого ПЗ шляхом перехоплення двійкового коду у вигляді зображень або послідовностей байтів. Рекурентні нейронні мережі RNN і трансформатори можуть моделювати послідовності викликів API, інструкцій для виявлення будь-яких загроз або поведінки шкідливого ПЗ. За даними Sophos, його механізм глибокого навчання зловмисних програм має вищі показники виявлення, ніж як застарілі, так і старі моделі МН, зберігаючи при цьому низький рівень хибнопозитивних результатів порівняно з традиційним антивірусом [57].

Поряд зі статичним аналізом файлів, глибокі нейронні мережі використовуються в динамічному аналізі поведінки. Шкідливе ПЗ виконується в пісочниці, і його поведінка спостерігається (мережевий трафік, системні виклики, використання пам'яті тощо). Будь-які спостережувані послідовності або графіки поведінки можуть бути передані в моделі глибокого навчання для виявлення та класифікації шкідливого ПЗ відповідно до моделей поведінки. Це також допомагає виявляти безфайлові шкідливі програми та багатоетапні атаки, які проявляються лише через будь-які підозрілі взаємодії під час виконання.

Сучасні платформи захисту кінцевих точок поєднують статичні моделі глибокого навчання з поведінковими моделями ШІ, які постійно вивчають, як виглядатиме нормальна активність, і позначають будь-які відхилення. Наприклад, Defender від Microsoft перейшов від повного підходу на основі сигнатур до поведінкового МН з використанням хмари, збирає загальну телеметрію, таку як дії процесів, з'єднання, і використовує хмару для кореляції та виявлення аномалій, що вказують на шкідливе ПЗ, не покладаючись на відомі сигнатури. Підхід на основі МН дозволяє виявляти загрози високополіморфного шкідливого ПЗ в режимі реального часу [58].

Виявлення аномалій і некероване навчання. Поведінка загроз невідома, доки вони не атакують. Їх неможливо позначити заздалегідь, тому системам необхідно виконувати навчання без нагляду, а методи виявлення аномалій надзвичайно важливі для прогнозування нових атак. Моделі ШІ вивчають базову норму поведінки системи і користувачів, а потім виявляють будь-які відхилення, які можуть сигналізувати про шкідливу поведінку.

Саме аналітика поведінки користувачів та ІТ-об’єктів профілює типового користувача, поведінку мережі або пристрою, а потім використовує МН для виявлення будь-яких нерегулярних закономірностей, які можуть вказувати на внутрішню загрозу або скомпрометований обліковий запис. Наприклад, якщо користувач отримує доступ до систем або даних, які він ніколи раніше не використовував, у незвичайний час або у великих обсягах, то система виявлення на основі аномалій може підняти тривогу.

Системи на основі ШІ використовують такі алгоритми, як кластеризація, нейронні автокодери та однокласові SVM, щоб розрізняти нормальну активність від загроз без будь-якої попередньо визначеної сигнатури шкідливого ПЗ. IBM стверджує, що рішення UEBA використовують поведінкову аналітику і МН для виявлення загроз [44].

Виявлення аномалій також застосовується до мережевого трафіку, наприклад, позначаючи будь-які незвичайні потоки, які нагадують витік даних або комунікації командування та управління, а також спостерігаються системні

процеси. Такі поведінкові відхилення часто забезпечують раннє попередження про шкідливі програми, зокрема експлойти нульового дня, які не виявляються інструментами на основі сигнатур. Проблема із системами виявлення на основі аномалій полягає в налаштуванні систем для мінімізації хибних спрацьовувань, оскільки не кожне відхилення від визначеного шаблону буде шкідливим. Саме тому ці системи ШІ поєднуються з контекстом платформ розвідки загроз або будь-якими іншими індикаторами для підвищення точності.

Обробка природної мови в аналізі загроз. Нещодавні дослідження також застосовували методи обробки природної мови (NLP) для виявлення шкідливого ПЗ і виконання аналізу загроз. Деякі артефакти шкідливого ПЗ, такі як код, послідовності викликів API, бінарні коди операцій або навіть текстовий контент у скриптах і журналах, можуть розглядатися як мова, що дозволяє моделям NLP виводити з них значення. Наприклад, код шкідливого ПЗ або дизасембльовані бінарні файли можуть бути представлені як послідовності токенів (інструкцій, рядків, операндів).

Методи NLP, такі як n-грамний аналіз, вбудовування слів або мовні моделі на основі трансформер, можуть вивчати закономірності, які відрізняють шкідливий код від доброякісного ПЗ. Аналіз друкованих рядків, витягнутих з двійкових файлів за допомогою підходів, подібних до NLP, ефективний для виявлення зловмисного ПЗ, проміжних представлень програмного коду (наприклад, абстрактних синтаксичних дерев або користувацьких мов байт-коду), а прикладні методи, такі як word2vec, також використовуються для виявлення шкідливих програм за семантичним контентом.

NLP також використовується для обробки величезних обсягів неструктурованого тексту в розвідці загроз. Моделі мови ШІ можуть зчитувати звіти про загрози, обговорення на хакерських форумах та описи шкідливого ПЗ. Використовуючи NLP для кластеризації та узагальнення показників з блогів безпеки або баз даних ШІ, останній може допомогти захисникам у ранньому виявленні нових атак шкідливого ПЗ. Моделі великих мов (LLM) також використовуються для аналізу поведінки шкідливого коду простою

англійською мовою, що допомагає кіберфахівцям і дослідникам зрозуміти складні загрози. Виявлення на основі NLP також має свої обмеження, такі як робота з обфускованим або зашифрованим кодом і потреба в спеціалізованих навчальних даних для створення ефективної мовної моделі [59].

Навчання з підкріпленням і змагальне моделювання. Навчання з підкріпленням (RL) – це новий підхід до ШІ, в якому автономний агент навчається оптимальним діям за допомогою системи взаємодії з середовищем методом спроб і помилок. Одним із варіантів є використання агентів RL у симульованих IT-середовищах і приманках, щоб зрозуміти, як поширюється шкідливий вплив, які дії призводять до виявлення та як найшвидше його стримувати [58]. Наприклад, агент RL може бути навчений розподіляти ресурси безпеки або запускати заходи стримування у відповідь на певні події, таким чином мінімізуючи збитки.

RL також може бути використане для моделювання поведінки зловмисника шляхом навчання агентів ШІ діяти як він. Це допомагає кіберспеціалістам передбачати тактику порушника. З іншого боку, RL використовується дослідниками для автоматизації генерації змагального шкідливого ПЗ, яке поступово модифікується, щоб уникнути виявлення ШІ.

У дослідженні агент RL навчився змінювати нешкідливі байти на зловмисні, щоб уникнути виявлення, не порушуючи функціональності шкідливого ПЗ. Подвійна природа RL відображає ширшу тему, де ШІ може як посилювати кіберзахист, так і бути використаним зловмисниками. У реальних сценаріях навчання з підкріпленням для виявлення загроз все ще є експериментальним, але в майбутньому системи ШІ зможуть активно навчатися в реальному середовищі й адаптуватися до атак у режимі реального часу. Ймовірно, інструменти захисту на основі RL будуть автономно вишукувати загрози й одночасно інтелектуально організовувати дії реагування як частину систем безпеки на базі ШІ.

Прогнозування загроз і проактивна розвідка загроз. Аналізуючи тенденції в наборах даних розвідки загроз, таких як телеметрія шкідливого ПЗ, TTP

зловмисників, канали вразливостей, моделі МН можуть ідентифікувати закономірності, що передують будь-яким новим атакам. Наприклад, алгоритми кластеризації можуть виявляти нові сімейства шкідливих програм, пов'язуючи разом рідкісні варіанти, які спостерігаються в реальних умовах, що спонукатиме аналітиків до подальшого дослідження аномалії.

Деякі платформи на основі ШІ використовують кілька джерел даних, таких як репозиторії зразків шкідливих програм, розмови в даркнеті й соціальні мережі, і поєднують їх для прогнозування вразливостей, на які слід здійснити атаку. Графові нейронні мережі та розширене виявлення аномалій виявляють слабкі сигнали, які людина-аналітик може пропустити. Кінцевим результатом є перехід від реактивної безпеки до більш проактивної позиції.

Наприклад, платформи розвідки загроз Recorded Future використовують ШІ для аналізу понад мільйона джерел і попередження організацій про будь-які нові загрози шкідливих програм, перш ніж вони вплинуть на них [60]. Здатність передбачати атаки є ключовим фактором безпеки ШІ. Розпізнаючи слабкі закономірності будь-якої активності зловмисника, система ШІ може спонукати до вжиття превентивних заходів і зірвати атаку на етапі планування. Мовні моделі на основі трансформерів можуть вивчати закономірності, які відрізняють шкідливий код від доброякісного програмного забезпечення.

Моніторинг і аналіз поведінки з нейронними мережами. Для виявлення поведінкових аномалій застосовуються автоенкодери (різновид архітектури реккурентних нейронних мереж) з навчанням без нагляду, які навчаються реконструювати нормальну поведінку, а помилки реконструкції позначають як аномалії. Автоенкодери демонструють відмінні результати в аналізі послідовності дій користувача /подій безпеки і можуть бути корисні для раннього виявлення аномалій за допомогою порівняння відновлених даних з оригінальними.

Моделі-трансформери розроблені для розуміння порядку та контексту подій безпеки, зосереджуючись на тому, як кожна подія пов'язана з іншими Трансформери є методом, який діє подібно до того, як сучасні мовні моделі,

такі як ChatGPT, інтерпретують текст. Механізм їх дії передбачає запис довгострокових залежностей за допомогою механізмів самоконтролю і подальше моделювання маскованих подій без нагляду.

Графові нейронні мережі (GNN) розглядають поведінку користувачів та IT-об’єктів у вигляді гетерогенних графів, де вузли відповідають пристроям або IP-адресам, а ребра показують зв'язки між ними. Ці інструменти вивчають вбудовування графів та виконують класифікацію аномалій вузлів [61].

3.3 Виклики і тенденції застосування ШІ в кібербезпеці й поведінковій аналітиці

Незважаючи на те, що інструменти поведінкової аналітики на основі ШІ надають потужні можливості, їх використання пов’язане з певними проблемами й обмеженнями [52, 58, 62] (Рис. 3.4).

Розглянемо основні з них.

Уникнення ШІ з боку зловмисників. Сучасні хакери адаптуються до уникнення моделей ШІ, використовуючи тактики зловмисного МН, щоб знайти сліпі зони та отруїти моделі. Одним із таких прикладів був обхід антивірусу МН Cylance внаслідок додавання нешкідливих рядків до файлів шкідливого ПЗ [63]. Крім того, розробники шкідливих програм тестують свої зловмисні продукти на механізмах на базі ШІ та використовують його для створення нових варіантів, щоб уникнути виявлення.

Рис. 3.4. Проблеми й обмеження застосування ШІ

Хибнопозитивні результати та втома від сповіщень. Навіть з усіма покращеннями, системи ШІ можуть генерувати хибнопозитивні результати, що ускладнює роботу команд безпеки. Модель МН може позначати нешкідливу поведінку системи як шкідливу лише тому, що вона рідко зустрічається в навчальних даних. Щоб мінімізувати невиправдане блокування законної активності, необхідно належним чином налаштовувати ШІ-системи у поєднанні з контекстом. Зазвичай це досягається за допомогою підходу «людина в циклі», коли ШІ позначає або автоматично блокує загрози, а людина-аналітик може перевірити та налаштувати пороги.

Відсутність пояснень. Моделі ШІ, особливо мережі глибокого навчання, працюють як чорні ящики, що робить рішення важкими для інтерпретації. Відсутність пояснень ШІ (XAI) викликає серйозне занепокоєння з боку аналітиків, які прагнуть розуміти, чому модель позначила подію як фактичну шкідливу атаку або збій. Пояснення необхідне також для підзвітності, охоплюючи аналіз рішення ШІ. Без розуміння, налагодження помилкових виявлень і покращення моделі є складним.

Якість даних та упередженість. Ефективність ШІ в аналізі шкідливих подій і виявленні загроз залежить від якості навчальних даних, що створює постійні труднощі в отриманні комплексних, актуальних, точних та маркованих наборів даних. Навчання ШІ обмеженому діапазону зловмисних подій/дій призведе до низької продуктивності, що демонструє упередженість набору даних.

Існують також ризики, пов'язані з «отруєними» даними, коли зловмисники вводять неправильно марковані шкідливі зразки в канали загроз, щоб маніпулювати навчанням ШІ. Також виникають етичні проблеми щодо обробки даних, особливо при використанні даних про загрози, що містять конфіденційну інформацію.

Життєвий цикл та обслуговування моделі. Підтримка моделі виявлення загроз ШІ є критично важливою, і це не одноразове завдання. Моделі з часом деградують через розвиток атак і потребують регулярного перенавчання з

використанням найновіших даних, оновлень та моніторингу продуктивності. Організації повинні мати власну або зовнішню експертизу для управління моделями ШІ, що вимагає кваліфікованого персоналу для аналізу, налаштування та включення нової інформації про загрози. Крім того, стійкість та надійні методи МН, такі як змагальне навчання, валідація та резервні механізми, є важливими для будь-якого розгортання безпеки ШІ.

Етичне використання ШІ та конфіденційність. Виявлення зловмисної поведінки за допомогою ШІ є потужним, але викликає етичні проблеми через його залежність від потенційно чутливих системних даних і мережевих даних. Прозорість стає критично важливою, організації повинні інформувати зацікавлені сторони про автоматизований моніторинг і вирішувати проблеми щодо неправомірного використання даних або недобросовісного профілювання. Подвійний характер використання ШІ в кібербезпеці створює етичну проблему, захисні моделі ШІ можуть бути використані зловмисниками для створення складних фішингових атак або прискорення виявлення вразливостей.

Спільнота кібербезпеки, включаючи такі організації, як MITRE, активно вирішує ці проблеми, розробляючи етичні та безпекові рамки для ШІ, такі як MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) та Матриця загроз змагального машинного навчання [64].

Особливо варто наголосити, що ШІ потрібно розглядати як доповнення до кваліфікованих аналітиків-людей, а не як заміну, тому організаціям необхідно інвестувати в надійність, пояснювальність і етичне управління своїми системами ШІ.

Аналіз наукових напрацювань і прогнозів експертів-практиків дозволив виокремити низку нових тенденцій і перспективних напрямів розвитку ШІ в кібербезпеці та поведінковій аналітиці Рис. 3.5).

Рис. 3.5. Тенденції і перспективи розвитку ШІ в кібербезпеці та UEBA

Використання генеративного ШІ як для захисту, так і для нападу. В останні роки ШІ став палицею з двома кінцями, адже злочинці використовують його для створення складних шкідливих програм і приманок для соціальної інженерії. Дослідники Palo Alto Networks продемонстрували моделі ШІ, які можуть генерувати функціональне шкідливе ПЗ на основі фреймворків MITRE ATT&CK [65]. Початкові зразки шкідливих програм, згенеровані ШІ, були базовими, але з часом вони вдосконалилися і створили тривожні, складні варіанти, які могли обійти захист. Однією з тривожних можливостей є використання ШІ для імітації відомих сімейств шкідливих програм.

Навчаючись на загальнодоступних звітах про загрози, ШІ може генерувати шкідливе ПЗ, яке точно імітує стиль. Це викликає занепокоєння щодо операцій під хибним прапором, за допомогою яких зловмисники навмисно вводять в оману атрибуцію. Зловмисники також можуть використовувати генеративний ШІ для створення нескінченних поліморфних варіантів шкідливого коду, який виконує аналогічні шкідливі дії, але постійно видозмінюється, перевантажуючи захист.

З боку захисту генеративний ШІ використовується для допомоги аналітикам та інструментам безпеки. Наприклад, моделі великих мов використовують в Security Copilot від Microsoft для аналізу даних про інциденти та пропонування подальших кроків природною мовою [66]. Існують

також прототипи ШІ, які автоматично записують сигнатури виявлення на основі опису нової загрози. ШІ може створювати безпечні зразки трафіку та шкідливого коду для навчання і тестування, що підвищує стійкість моделі. У майбутньому команди безпеки будуть регулярно використовувати агентів ШІ як віртуальних колег для аналітиків з метою автоматизованого пошуку загроз, генерування гіпотез про потенційні інциденти та дії.

Інтегровані платформи безпеки на базі ШІ. Постачальники засобів безпеки все частіше інтегрують ШІ у свої продукти, що призводить до більш уніфікованих платформ безпеки. Це видно в таких концепціях як Extended Detection and Response (XDR), яка використовує ШІ для кореляції даних з кінцевих точок, мереж, хмар та ідентифікаційних даних. У майбутньому більше механізмів кореляції на базі ШІ будуть використовуватися для зв'язку різних сповіщень, таких як зв'язування фішингових електронних листів із завантаженнями шкідливого ПЗ і незвичайним доступом до сервера, щоб забезпечити повний опис атаки.

Хмарний ШІ слугуватиме центральним центром розвідки, навчаючись на глобальних загрозах і поширюючи оновлення. Альянс кібербезпеки OpenAI та інші ініціативи з відкритим кодом розробляють інструменти ШІ для класифікації шкідливих програм і виявлення вразливостей. Спеціалізовані моделі ШІ стануть поширеними, орієнтуючись на такі галузі, як шкідливе ПЗ прошивки, аномалії Інтернету речей, аномалії та проблеми ідентифікації та доступу [67]. ШІ покращить інструменти оркестрації для автоматизації завдань, таких як сортування оповіщень, збагачення та ініціювання реагування. Майбутні SOC будуть мати розмовні ШІ-інтерфейси, які дозволять аналітикам ставити запитання природною мовою для миттєвого отримання інформації.

Зрозумілий і прозорий ШІ. Зрозумілість аналізу шкідливих програм на основі ШІ наразі є проблемою, але може стати ключовою зоною в майбутніх розробках. Будуть розроблені нові інструменти, які пропонують візуалізацію та обґрунтування рішень ШІ. Наприклад, панелі безпеки можуть відображати

конкретні точки даних, що впливають на оцінку загрози файлу, або перераховувати основні причини ізоляції хоста.

Дослідження в галузі XAI можуть створити такі методи, як локальні сурогатні моделі та візуалізації механізмів уваги, тим самим підвищуючи прозорість. Прозорість допомагає у формуванні довіри з аналітиком і налаштуванні ШІ, підтримує дотримання вимог і звітність, надаючи докази дій ШІ. Зростаючий інтерес до інтерпретованого МН для безпеки в академічних спільнотах може призвести до його інтеграції в комерційні продукти. Системи постійної валідації ШІ, такі як тестування симульованих атак, стануть стандартною практикою для забезпечення постійної ефективності та уникнення будь-якого зниження продуктивності.

ШІ та розвідка загроз/реагування на інциденти. Роль ШІ в кібербезпеці виходить за рамки виявлення, а охоплює реагування на інциденти і розвідку загроз. Майбутні розробки охоплять цифрову криміналістику на базі ШІ для швидкого аналізу першопричин і прогнозування рухів зловмисника. Навчаючись на численних інцидентах, ШІ зможе консультувати служби реагування щодо пріоритетів розслідування, ефективного стримування та потенційного впливу.

Навчання з підкріпленням у кіберзахисті – це нова тенденція, де агенти ШІ можуть навчитися оптимально ізолювати заражені хости з мінімальними збоями або динамічно коригувати конфігурації програм після виявлення загрози. Платформи SOAR інтегрують ШІ для покращення прийняття рішень поза межами статичних правил. Незабаром ШІ зможе автономно керувати незначними інцидентами (наприклад, скиданням паролів, карантином шкідливих вкладень), передаючи аналітикам лише складні випадки.

Концепція автономного кіберзахисту з використанням агентів ШІ є перспективною, але складною галуззю, яка вимагає ретельного впровадження, щоб запобігти перетворенню самого ШІ на вразливість.

Співпраця та обмін інформацією через ШІ. Спільнота кібербезпеки використовує ШІ для сприяння кращій співпраці. ШІ може допомогти

аналізувати дані про загрози від різних організацій та обмінюватися аналітичними даними, не розкриваючи жодної конфіденційної інформації. Наприклад, федеративне навчання може дозволити кільком організаціям навчати спільну модель виявлення шкідливого коду з їхніми об'єднаними даними та не обмінюватися необробленими даними, захищаючи конфіденційність. Це збільшить різноманітність даних, доступних для навчання, та покращить моделі ШІ.

Моделі ШІ, специфічні для певних галузей (фінанси, охорона здоров'я) також, імовірно, будуть створені за допомогою консорціумів компаній, які об'єднують свої аналітичні дані через ШІ. ШІ також може автоматизувати генерацію правил YARA, правил Sigma або зіставлень ATT&CK для нових загроз і поширювати їх через такі платформи, як репозиторії CTI MITRE [68].

З появою обміну інформацією про загрози на основі ШІ, агенти ШІ можуть переглядати канали та координувати свої дії, щоб майже миттєво попереджати членів довірчої групи про новий шкідливий засіб та його характеристики. У майбутньому ШІ може забезпечити кращу колективну оборонну позицію, а дані про одне порушення миттєво аналізуються та поширюються для захисту інших.

Інтеграція UEBA з архітектурою Zero Trust. Оскільки організації все частіше впроваджують архітектуру Zero Trust, інтеграція UEBA матиме вирішальне значення для забезпечення аналізу безпеки в режимі реального часу на основі поведінки. Вже у цьому році буде забезпечено кращу безшовну інтеграцію між рішеннями UEBA та фреймворками Zero Trust, що дозволить безперервно моніторити діяльність користувачів, доступ до пристроїв та мережеві підключення. Ця інтеграція дозволить проводити адаптивну оцінку ризиків і забезпечить динамічний контроль доступу на основі поведінки в реальному часі, посилюючи заходи безпеки та зменшуючи вразливості в середовищах з високим рівнем ризику.

Посилена увага до хмарних та гібридних середовищ. Оскільки все більше підприємств переходять до хмарних і гібридних середовищ, UEBA буде

розширювати свою спрямованість. Сучасні організації надаватимуть пріоритет рішенням UEBA, які забезпечують видимість на хмарних платформах, локальних мережах і гібридних інфраструктурах. Оскільки більше конфіденційних даних зберігаються поза межами офісу, UEBA дозволить організаціям відстежувати діяльність користувачів у різних середовищах, виявляючи такі ризики, як несанкціонований доступ або незвичайні передачі даних, гарантуючи, що безпека виходить за межі традиційних ІКС [69].

Майбутнє кібербезпеки буде значною мірою пов'язане зі ШІ як інструментом захисту, так і методом атаки. Команди безпеки мають бути в курсі цих розробок і впроваджувати нові ШІ-інструменти для покращення своїх можливостей і усунення вразливостей, зокрема використання генеративного ШІ для доповнення роботи аналітиків і розгортання спеціалізованих моделей МН для кращого кіберзахисту. Також важливо стежити за тим, як зловмисники використовують ШІ для розробки контрзаходів. Динамічний кіберландшафт все більше перетворюватиметься на алгоритмічну конкуренцію. Завдяки співпраці та інноваціям фахівці з безпеки зможуть підтримувати стратегічну перевагу.

Отже, як засвідчило дослідження, ШІ змінює ландшафт захисту від зловмисних атак і прогнозування загроз. За допомогою таких методів як глибоке навчання, виявлення аномалій, NLP та інших, системи ШІ можуть аналізувати поведінку шкідливих програм і величезні обсяги даних про загрози з глибиною та масштабом, що значно перевищують людські можливості.

Ключові рекомендації для команд кіберзахисту охоплюють інвестування високоякісних даних і постійне навчання моделей ШІ, використання ШІ для розширення людської експертизи, а не її заміни, інформування про критичні рішення, впровадження надійної валідації та моніторингу систем ШІ для захисту від помилок або відхилень, розробку політики етичного використання ШІ, забезпечення прозорості та справедливості в автоматизованих рішеннях. Також важливо поєднувати виявлення за допомогою ШІ з багаторівневим підходом до безпеки, зокрема використання ШІ для позначення аномалій, а

потім застосування традиційного або людського аналізу для підтвердження і розслідування.

Висновки до розділу 3

Встановлено, що з огляду на безпрецедентне зростання кількості даних і вимог до темпів їх аналізу, а також неможливість їх обробки за допомогою традиційних ручних або автоматизованих методів поведінкова аналітика все ширше використовує алгоритми ШІ та МН для вирішення завдань кібербезпеки. Сьогодні майже 70% організацій вже використовують рішення безпеки на основі ШІ для виявлення та запобігання загрозам.

Основними напрямами застосування ШІ і МН в рішеннях UEBA є моніторинг поведінки користувачів та ІТ-об’єктів, виявлення аномалій поведінки, розвідка загроз, аналіз подій безпеки, предиктивна аналітика, розподіл ресурсів безпеки і запуск заходів стримування, автоматизація прийняття рішень. Інструменти ШІ, які використовуються у системах UEBA, охоплюють глибоке навчання, кероване і некероване навчання, різні види нейронних мереж, алгоритми кластеризації, нейронні автокодери та однокласові SVM, NLP тощо.

Незважаючи на те, що інструменти UEBA на основі ШІ надають потужні можливості, їх використання пов’язане з певними проблемами й обмеженнями, які охоплюють можливості уникнення ШІ з боку зловмисників; хибнопозитивні результати та втома від сповіщень; складнощі в інтерпретації рішень моделей ШІ людиною; залежність ШІ від якості даних та упередженість наборів даних; етичні проблеми щодо обробки даних, зокрема конфіденційних; потреба в управлінні життєвим циклом моделі (моніторинг, експертиза, перенавчання, оновлення, обслуговування тощо).

Аналіз дозволив виокремити низку нових тенденцій і перспективних напрямів розвитку ШІ в кібербезпеці та поведінковій аналітиці, серед яких використання генеративного ШІ як для захисту, так і для нападу; розбудова інтегрованих платформ безпеки на базі ШІ; створення зрозумілого і прозорого

ШІ шляхом візуалізації та обґрунтування, валідації рішень ШІ; зростання ролі ШІ у процесах розвідки загроз і реагування на інциденти, розвиток механізмів цифрової криміналістики, ефективного стримування та потенційного впливу на базі ШІ; співпраця та обмін інформацією, наприклад щодо виявлення й реагування на загрози, з використанням ШІ; інтеграція поведінкової аналітики з архітектурою Zero Trust; посилена увага до технологій безпеки, зокрема UEBA у хмарних та гібридних середовищах.

За результатами дослідження окреслено ключові рекомендації для команд кіберзахисту, що охоплюють інвестування високоякісних даних і постійне навчання моделей ШІ, використання ШІ для розширення людської експертизи, а не її заміни, інформування про критичні рішення, впровадження надійної валідації та моніторингу систем ШІ для захисту від помилок або відхилень, розробку політики етичного використання ШІ, забезпечення прозорості та справедливості в автоматизованих рішеннях. Також важливо поєднувати виявлення за допомогою ШІ з багаторівневим підходом до безпеки, зокрема використання ШІ для позначення аномалій, а потім застосування традиційного або людського аналізу для підтвердження і розслідування.

ВИСНОВКИ

Дослідження показало, що сучасні інструменти EUBA забезпечують надійні можливості виявлення в поєднанні з глибшим розумінням для розслідування та реагування. Вони надають автоматизовані часові рамки інцидентів, які виділяють події за ризиком, а також більш динамічні методи сповіщень, які дозволяють аналітикам з більшою точністю визначати пріоритети сортування сповіщень від сторонніх розробників.

Основні компоненти UEBA, які працюють разом для виявлення загроз і реагування на них, зазвичай охоплюють 1) збір даних із різних джерел; 2) побудову базових моделей для розуміння нормальних моделей поведінки користувачів та об'єктів; 3) виявлення аномалій, яке охоплює порівняння поточної активності з базовими показниками; 4) сповіщення та реагування на інциденти з метою співвіднесення і пріоритезації аномалій.

Сучасні системи поведінкової аналітики забезпечують проактивну безпеку, надаючи інформацію про потенційні загрози, перш ніж вони переростуть у серйозні інциденти, таким чином дозволяючи організаціям вийти за рамки реактивних заходів безпеки. Основними рисами UEBA є використання ШІ, МН й аналітики для аналізу величезних обсягів даних у режимі реального часу; інтеграція з іншими системами безпеки; моніторинг та оповіщення в реальному часі; пошук загроз, зокрема тих, які могли уникнути стандартних методів виявлення; візуалізація та звітність; автоматизація завдань безпеки та оркестрація, тобто взаємодія з іншими системами безпеки.

Аналіз літератури засвідчив такі ключові переваги UEBA: покращене автоматизоване виявлення і раннє попередження загроз; зменшення кількості хибних спрацьовувань; забезпечення нормативної відповідності; адаптивність до ландшафту загроз; запобігання втраті даних; швидке й ефективне реагування на інциденти; довгостроковий аналіз тенденцій і криміналістика; можливості автономного використання UEBA і розширення базових рішень SIEM.

Незважаючи на значний перелік переваг, впровадження інструментів UEBA пов’язане з деякими недоліками і потенційними проблемами, зокрема обмежені можливості інтеграції даних; недостатня масштабованість систем; проблеми з етикою і конфіденційністю даних; наявність хибнопозитивних результатів; потреба у кваліфікованому персоналі.

Як показало дослідження, ринок рішень UEBA значно еволюціонував за останні роки. Рішення, які починалися як нішеві пропозиції для великих підприємств, перетворилися на інструменти широкого вжитку, які бездоганно інтегруються із SIEM, SOAR і хмарними системами безпеки. Аналіз публікацій від провідних експертних організацій і виробників засобів кібербезпеки за 2024-2025 роки показав, що найбільш затребуваними є рішення від компаній-лідерів галузі, таких як Exabeam, Fortinet, IBM, Microsoft, Rapid7, Splunk.

Встановлено, що основними напрямами застосування ШІ і МН в рішеннях UEBA є моніторинг поведінки користувачів та ІТ-об’єктів, виявлення аномалій поведінки, розвідка загроз, аналіз подій безпеки, предиктивна аналітика, розподіл ресурсів безпеки і запуск заходів стримування, автоматизація.

UEBA використовують різноманітні методи МН, зокрема алгоритми некерованого і керованого навчання, навчання з підсиленням, моделі глибокого навчання, зокрема глибокі нейронні мережі (DNN), алгоритми виявлення аномалій, такі як моделі гаусової суміші (GMM), ізоляційний ліс, однокласова SVM і статистичні підходи, методи ансамблевого навчання. Поведінковий аналіз охоплює моделювання на основі профілів і графів, аналіз послідовності, контекстуальний і статистичний аналіз, статистичне профілювання тощо.

Незважаючи на те, що інструменти UEBA на основі ШІ надають потужні можливості, їх використання пов’язане з певними проблемами й обмеженнями, які охоплюють можливості уникнення ШІ з боку зловмисників; хибнопозитивні результати та втома від сповіщень; складнощі в інтерпретації рішень моделей ШІ людиною; залежність ШІ від якості даних та упередженість наборів даних; етичні проблеми щодо обробки даних, зокрема конфіденційних; потреба в управлінні життєвим циклом моделі.

Аналіз дозволив виокремити низку нових тенденцій розвитку ШІ в кібербезпеці та поведінковій аналітиці, серед яких використання генеративного ШІ як для захисту, так і для нападу; розбудова інтегрованих платформ безпеки на базі ШІ; створення зрозумілого і прозорого ШІ шляхом візуалізації та обґрунтування, валідації рішень ШІ; зростання ролі ШІ у процесах розвідки загроз і реагування на інциденти, розвиток механізмів цифрової криміналістики, ефективного стримування та потенційного впливу на базі ШІ; співпраця та обмін інформацією, наприклад щодо виявлення й реагування на загрози, з використанням ШІ; інтеграція поведінкової аналітики з архітектурою Zero Trust; посилена увага до технологій безпеки у хмарних і гібридних середовищах.

За результатами дослідження окреслено ключові рекомендації для команд кіберзахисту, що охоплюють інвестування високоякісних даних і постійне навчання моделей ШІ, використання ШІ для розширення людської експертизи, а не її заміни, інформування про критичні рішення, впровадження надійної валідації та моніторингу систем ШІ для захисту від помилок або відхилень, розробку політики етичного використання ШІ, забезпечення прозорості та справедливості в автоматизованих рішеннях. Також важливо поєднувати виявлення за допомогою ШІ з багаторівневим підходом до безпеки, зокрема використання ШІ для позначення аномалій, а потім застосування традиційного або людського аналізу для підтвердження і розслідування.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. What is user and entity behavior analytics (UEBA)? *Microsoft*. URL: https://www.microsoft.com/en-ca/security/business/security-101/what-is-user-entity-behavior-analytics-ueba

2. Market Guide for User and Entity Behavior Analytics. 21 May 2019. *Gartner*. URL: https://www.gartner.com/en/documents/3917096

3. What is User and Entity Behavior Analytics (UEBA)? *Radware*. URL: https://www.radware.com/cyberpedia/cloud-security/ueba/

4. Demystifying User and Entity Behavior Analytics (UEBA): Enhancing Cybersecurity. *Quadrant9*. URL: https://quadrant9.wordpress.com/2024/04/10/demystifying-user-and-entity-behavior-analytics-ueba-enhancing-cybersecurity/

5. User and Entity Behavior Analytics Market Share, Size, Trends, Industry Analysis Report By Component (Solution, Services); By Deployment (On-premise, Cloud); By Enterprise Size, By Vertical, By Region, And Segment Forecasts, 2023 – 2032. /august 2023. 119 p. URL: https://www.polarismarketresearch.com/industry-analysis/user-and-entity-behavior-analytics-market

6. Shekhar Menkudale, Divya Baranawal. Market Forecast Analysis: User & Entity Behavior Analytics, 2022-2027, EMEA Qksgroup URL: https://qksgroup.com/market-research/market-forecast-analysis-user-entity-behavior-analytics-2022-2027-emea-288

7. Nirupam Samanta. Understanding UEBA: The Behavioral Defense Against AI-Powered Attacks. URL: https://www.forbes.com/councils/forbestechcouncil/2025/06/11/understanding-ueba-the-behavioral-defense-against-ai-powered-attacks/

8. Liku Zelleke What is UEBA (User and Entity Behavior Analytics)? *Comparitech*. URL: https://www.comparitech.com/net-admin/user-entity-behavior-analytics/

9. UEBA Tools: Key Capabilities and 7 Tools You Should Know. *Exabeam*. URL: https://www.exabeam.com/explainers/ueba/ueba-tools-key-capabilities-and-7-tools-you-should-know/

10. User and Entity Behavioral Analytics (UEBA). *Delinea*. URL: https://delinea.com/what-is/user-and-entity-behavioral-analytics-ueba

11. Yana Storchak. Insider Threat Statistics for 2025: Key Facts, Types of Incidents, and Costs. *Syteca*. URL: https://www.syteca.com/en/blog/insider-threat-statistics-facts-and-figures

12. Insider Threat Detection Software: Strengthening Cybersecurity from Within. *Gurucul*. URL: https://gurucul.com/blog/insider-threat-detection-software-strengthening-cybersecurity-from-within/

13. T. Muzhanova, S. Lehominova, Y. Yakymenko, I. Mordas. Технології моніторингу й аналізу діяльності користувачів у запобіганні внутрішнім загрозам інформаційній безпеці організації. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2021. 1(13). С. 50–62. https://doi.org/10.28925/2663-4023.2021.13.5062

14. UEBA Tools: Your Guide to Behavioral Based Security Analytics. *Gurucul*. URL: https://gurucul.com/blog/ueba-tools-your-guide-to-behavioral-based-security-analytics/

15. Shashanka, Madhu & Shen, Min-Yi & Wang, Jisheng. User and entity behavior analytics for enterprise security. *2016 IEEE International Conference on Big Data (Big Data)*, Washington, DC, USA, 2016, pp. 1867-1874. URL: https://ieeexplore.ieee.org/document/7840805

16. Пасєка І., Сєвєрінов О. Проблеми впровадження системи аналітики поведінки користувачів та сутностей. «Global Cyber Security Forum 2019». 14–16 листопада 2019, Харків. С. 82-83. URL: https://openarchive.nure.ua/server/api/core/bitstreams/66a64a70-17c8-4eb1-9652-780ed85c39a9/content

17. Polyakov, Oleg. UEBA (User and Entity Behavior Analytics) for When Traditional Cyber Security Can't Protect Your Network. 2021. URL: https://www.academia.edu/37806646/UEBA_User_and_Entity_Behavior_Analytics_for_when_traditional_Cyber_Security_cant_protect_your_network#key-takeaways

18. Фесьоха В., Унтілова О., Чернявський Р. Аналіз підходів до мінімізації хибних результатів у процесі виявлення аномалій системами

кіберзахисту. Науковий журнал "*Комп'ютерно-інтегровані технології: освіта, наука, виробництво*". Луцьк, 2025. Випуск № 60. С. 318-327.

19. Benefits of Implementing UEBA. *Paloalto Networks*. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-user-entity-behavior-analytics-ueba

20. Що таке аналітика поведінки користувачів і сутностей? *Microsoft*. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-user-entity-behavior-analytics-ueba

21. Vlad Yakushkin. 7 Cybersecurity Challenges to Solve with a UEBA Deployment. *Syteca*. October 27, 2021. URL: https://www.syteca.com/en/blog/ueba-use-cases

22. What Is UEBA and Why It Should Be an Essential Part of Your Incident Response. *Exabeam*: URL: https://www.exabeam.com/explainers/ueba/what-is-ueba-and-why-it-should-be-an-essential-part-of-your-incident-response/

23. Khaliq S, Tariq ZU, Masood A. Role of user and entity behavior analytics in detecting insider attacks. *2020 IEEE International Conference on Cyber Warfare and Security (ICCWS*). 2020 Oct 20; 1–6. URL: https://www.researchgate.net/publication/347979474_Role_of_User_and_Entity_Behavior_Analytics_in_Detecting_Insider_Attacks

24. UEBA Trends - What's New and What's Next. *Logsign*. 22.06.2023. URL: https://www.logsign.com/blog/ueba-trends-whats-new-whats-next/

25. Garima Sharma, Ambika Thakur, Chetna Tiwari. Developing a Comprehensive Framework for User and Entity Behavior Analytics (UEBA): Integrating Advanced Machine Learning and Contextual Insights. *Journal of Communication Engineering & Systems.* 2024. Volume 14. Issue 2. pp. 20-31. URL: https://journals.stmjournals.com/joces

26. ABCs of UEBA: M is for Machine Learning. *Gurucul*. 2019. URL: https://gurucul.com/blog/abcs-of-ueba-m-is-for-machine-learning/

27. Salitin MA, Zolait AH. The role of User Entity Behavior Analytics to detect network attacks in real time. *2018 IEEE international conference on*

innovation and intelligence for informatics, computing, and technologies (3ICT). 2018. Nov 18. pp. 1-5. URL: https://www.researchgate.net/publication/336259455_The_role_of_User_Entity_Behavior_Analytics_to_detect_network_attacks_in_real_time

28. Khan MZ, Khan MM, Arshad J. Anomaly detection and enterprise security using user and entity behavior analytics (UEBA). *2022 IEEE 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS)*. 2022 Dec 14; pp. 1-9.

29. What Is UEBA (User and Entity Behavior Analytics)? *Exabeam*. URL: https://www.exabeam.com/explainers/ueba/what-ueba-stands-for-and-a-5-minute-ueba-primer/

30. 7 Best User & Entity Behavior Analytics (UEBA) Tools. *Esecurity Planet*. https://www.esecurityplanet.com/products/best-user-and-entity-behavior-analytics-ueba-tools/

31. Insider Risk Management Solutions Reviews and Ratings. *Gartner*. URL: https://www.gartner.com/reviews/market/insider-risk-management-solutions

32. 5 Leading UEBA Solutions Transforming Cybersecurity in 2025. *Massdata*. URL: https://massdata.com/5-leading-ueba-solutions/

33. Top 7 UEBA Tools That Security Teams Should Rely on in 2025. *Cybernx*. URL: https://www.cybernx.com/ueba-tools/

34. Adil Hafa. Top 9 User and Entity Behavior Analytics (UEBA) Tools. URL: https://aimultiple.com/ueba-tools

35. Exabeam New-Scale SIEM. *Exabeam*. URL: https://www.exabeam.com/platform/new-scale-siem/

36. Security Information and Event Management (SIEM). *Fortinet*. URL: https://www.fortinet.com/products/siem/fortisiem

37. IBM QRadar. Reviews of IBM Security QRadar. *Capterra*. URL: https://www.capterra.com/p/179511/IBM-QRadar-SIEM/reviews/

38. LogRhythm SIEM. *LogRhythm*. URL: https://docs.logrhythm.com/lrsiem/docs/

39. Microsoft Sentinel. *Microsoft*. URL: https://www.microsoft.com/uk-ua/security/business/siem-and-xdr/microsoft-sentinel

40. Rapid7 InsightIDR. *Rapid7*. URL: https://docs.rapid7.com/insightidr/

41. Splunk UEBA. *Splunk*. URL: https://www.splunk.com/en_us/products/user-and-entity-behavior-analytics.html

42. Exabeam User and Entity Behavior Analytics (UEBA). *Exabeam*. URL: https://www.exabeam.com/capabilities/ueba/

43. Brandon Summers-Miller. Best User and Entity Behavior Analytics (UEBA) Software. *G2*. URL: https://www.g2.com/products/fortinet-user-and-entity-behavior-analytics-ueba/reviews

44. QRadar User Entity Behavior Analytics. *IBM*. URL: https://www.ibm.com/docs/en/qradar-common?topic=app-qradar-user-entity-behavior-analytics

45. LogRhythm UEBA. URL: https://docs.logrhythm.com/ueba/docs/logrhythm-ueba

46. Microsoft Sentinel User and Entity Behavior Analytics (UEBA). *Microsoft*. URL: https://secureazcloud.com/microsoft-security/f/microsoftsentinelueba2025guidetobehavioranalytics

47. User and Entity Behavior Analytics (UEBA). *Splunk*. URL: https://www.splunk.com/en_us/products/user-and-entity-behavior-analytics.html

48. Bao Tran. AI and Cybersecurity: Latest Stats on AI-Driven Threat Detection and Attacks. Dec 11, 2025. URL: https://patentpc.com/blog/ai-and-cybersecurity-latest-stats-on-ai-driven-threat-detection-and-attacks

49. Continuous Adaptive Risk and Trust Assessment (CARTA). *SSH Academy*. URL: https://www.ssh.com/academy/iam/carta

50. AI Driven Threat Defense The Next Frontier in Cybersecurity. White Paper. 2023. *Hillstone networks.* URL: https://www.hillstonenet.com/wp-content/uploads/AI-Driven-Threat-Defense-The-Next-Frontier-in-Cybersecurity-2023.pdf

51. Sharma, R., & Singh, A. AI-Driven Cybersecurity: Enhancing Threat Detection and Prevention. *Cybersecurity Journal*. 2022. №15(4), P. 112-128.

52. Ikechukwu Innocent Umeh. Enhancing Cybersecurity in the Age of AI: Challenges and Solutions. *World Journal of Advanced Research and Reviews*. 2025,

26(01), P.1095-1105. URL: https://journalwjarr.com/sites/default/files/fulltext_pdf/WJARR-2025-1157.pdf

53. Network Detection and Response (NDR) Buyer's Guide. *Secureworks*. 2024. URL: https://www.secureworks.com/-/media/files/us/buyers-guides/secureworks_ndr-buyers-guide.pdf

54. Prottoy Khan, Md Zahirul Islam, Sazib Hossain. AI-Powered Cybersecurity: Revolutionizing Business Threat Detection and Response. American Journal of Smart Technology and Solutions (AJSTS). 2025. Volume 4. Issue 1. P. 37-48.

55. Hype Cycle for Security Operations. 2024. *Gartner Research*. URL: https://www.gartner.com/en/documents/5622491

56. Aileen Balzano. Saying Goodbye to SOAR: What's Next for Security Operations? 2024. *Blinkops*. URL: https://www.blinkops.com/blog/gartner-says-goodbye-to-soar-whats-next-for-security-operations

57. Deep Learning Malware Detection in Intercept X. 2024. *Sophos*. URL: https://www.infoguard.ch/hubfs/partner/sophos/infoguard-sophos-intercept-x-deep-learning-dsna-en.pdf

58. John Komarthi. AI-Driven Malware Behavior Analysis and Threat Prediction. *IJIRMPS*. 2025. Volume 13. Issue 4. URL: https://www.ijirmps.org/papers/2025/4/232671.pdf

59. Victor Moka, Andrew James. Natural Language Processing for Cyber Threat Intelligence Analysis. 2025. URL: https://www.researchgate.net/publication/390113970_Natural_Language_Processing_for_Cyber_Threat_Intelligence_Analysis

60. 2025 State of Threat Intelligence: From tactical tool to strategic imperative. *Recorded Future*. URL: https://www.recordedfuture.com/

61. Mustafa Aljumaily, Hayder Abd, Elaf Majeed. Enhancing User and Entity Behavior Analytics in SIEM Systems Using AI-Powered Anomaly Detection: A Data-Driven Simulation Approach. *International Journal of Mechatronics, Robotics, and Artificial Intelligence*. 2025. Vol. 1 № 2. URL: https://ijmrai.edu.iq/ijmrai/article/view/11

62. Subhash Parimalla, Chelumala Sreshta, M. Haarika, Ch. Likhitha Sowmya, Adiba Sania and Yagati Vaishnavi. Hunting the Invisible: Harnessing UEBA to Unmask Insider Threats. In Mastering Intrusion Detection for Cybersecurity. 2024. URL: https://www.intechopen.com/chapters/1208835

63. Attacking Machine Learning. The Cylance Case Study BSides. Sydney 2019. *Skylight*. URL: https://skylightcyber.com/2019/07/18/cylance-i-kill-you/Cylance%20-%20Adversarial%20Machine%20Learning%20Case%20Study.pdf

64. Navigate threats to AI systems through real-world insights. *MITRE*. URL: https://atlas.mitre.org/

65. Top GenAI Security Challenges: Risks, Issues, & Solutions. Paloalto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/generative-ai-security-risks

66. Microsoft Security Copilot agents and new protections for AI. *Microsoft*. URL: https://www.microsoft.com/en-us/security/blog/2025/03/24/microsoft-unveils-microsoft-security-copilot-agents-and-new-protections-for-ai/

67. Strengthening cyber resilience as AI capabilities advance. 2025. *OpenAI*. URL: https://openai.com/index/strengthening-cyber-resilience/

68. The Role of AI and Machine Learning in Cybersecurity in 2025. *Lazarus Alliance.* URL: https://lazarusalliance.com/uk/the-role-of-ai-and-machine-learning-in-cybersecurity-in-2025/

69. Trends in User & Entity Behavior Analytics: What to Watch For in 2025? *LinkShadow*. URL: https://www.linkedin.com/pulse/trends-user-entity-behavior-analytics-what-watch-2025-linkshadow-ihzcf