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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія виявлення внутрішньої загрози в інформаційних системах організації на базі QRadar User Behavior Analytics»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

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

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

_____ Дмитрій КОРЧУК
(підпис)

Виконав: здобувач(ка) вищої освіти групи БСДМ-61
КОРЧУК Дмитрій
(прізвище, ім'я)

Керівник к.військ.н., доцент ГАХОВ Сергій
(науковий ступінь, вчене звання, прізвище, ім'я)

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

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІС – інформаційна система

ABAC - Attribute-Based Access Control (контроль доступу на основі атрибутів).

APT - Advanced Persistent Threat (просунута постійна загроза).

CRE - Cloud Runtime Environment (хмарне середовище виконання).

DDoS - Distributed Denial of Service (розподілене блокування сервісу).

DLP - Data Loss Prevention (запобігання втраті даних).

GDPR - General Data Protection Regulation (Загальний регламент захисту даних).

HIPAA - Health Insurance Portability and Accountability Act (Закон про портативність і відповідальність медичного страхування).

HR - Human Resources (кадровий відділ).

IBM - International Business Machines (міжнародна корпорація IBM).

IDS - Intrusion Detection System (система виявлення вторгнень).

IP - Internet Protocol (інтернет-протокол).

IPS - Intrusion Prevention System (система запобігання вторгнень).

ISO - International Organization for Standardization (Міжнародна організація зі стандартизації).

IT - Information Technology (інформаційні технології).

ML - Machine Learning (машинне навчання).

NDR - Network Detection and Response (виявлення та реагування на мережеві загрози).

PAM - Privileged Access Management (управління привілейованим доступом).

RAM – Random Access Memory (оперативна пам’ять)

RBAC - Role-Based Access Control (контроль доступу на основі ролей).

SIEM - Security Information and Event Management (управління інформацією та подіями безпеки).

SOAR - Security Orchestration, Automation, and Response (оркестрація, автоматизація та реагування в сфері безпеки).

UBA - User Behavior Analytics (аналіз поведінки користувачів).

UEBA - User and Entity Behavior Analytics (аналіз поведінки користувачів та сутностей).

VPN - Virtual Private Network (віртуальна приватна мережа).

ВСТУП

Актуальність дослідження. У сучасних інформаційних системах організацій, які функціонують у динамічному технологічному середовищі, основну увагу приділяють захисту від внутрішніх загроз, оскільки вони можуть становити значну небезпеку для конфіденційності, цілісності та доступності даних. Внутрішні загрози, як навмисні, так і ненавмисні, є особливо небезпечними через складність їх виявлення традиційними методами. У такому контексті технології поведінкового аналізу, такі як QRadar User Behavior Analytics, дозволяють забезпечити глибокий моніторинг активності користувачів і виявляти аномалії, що свідчать про потенційні ризики.

Впровадження систем на базі QRadar User Behavior Analytics у процеси забезпечення безпеки дозволяє ефективно реагувати на інциденти безпеки, аналізувати підозрілі дії та мінімізувати вплив загроз. Це надає організаціям можливість своєчасно виявляти порушення, які можуть залишитися непоміченими іншими засобами захисту. Вищезазначене визначає актуальність теми даної кваліфікаційної роботи, яка зосереджена на дослідженні технології виявлення внутрішніх загроз в інформаційних системах організацій із використанням QRadar User Behavior Analytics.

Об'єкт дослідження – виявлення внутрішньої загрози в інформаційних системах організації.

Предмет дослідження – технологія виявлення внутрішньої загрози в інформаційних системах організації на базі QRadar User Behavior Analytics.

Мета роботи – розробити порядок застосування технології виявлення внутрішньої загрози в інформаційних системах організації та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми виявлення внутрішньої загрози в інформаційних системах організацій;

проаналізувати підходи до виявлення внутрішньої загрози в інформаційних системах організацій;

проаналізувати існуючі рішення для виявлення внутрішньої загрози в інформаційних системах організацій;

проаналізувати методи та засоби виявлення внутрішньої загрози в інформаційних системах організації на базі QRadar User Behavior Analytics;

розкрити порядок реалізації технології виявлення внутрішньої загрози в інформаційних системах організації на базі QRadar User Behavior Analytics.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології виявлення внутрішньої загрози в інформаційних системах організації на базі QRadar User Behavior Analytics, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 25 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ВИЯВЛЕННЯ ВНУТРІШНЬОЇ ЗАГРОЗИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОРГАНІЗАЦІЙ

1.1. Дослідження проблеми виявлення внутрішньої загрози в інформаційних системах організацій

Кібербезпека є одним із ключових викликів сучасних організацій, оскільки дані та системи стають головною цінністю для бізнесу і урядових установ. Внутрішні загрози, як специфічний тип ризику, становлять значну небезпеку для забезпечення конфіденційності, цілісності та доступності даних. Відповідно до звіту IBM Security, близько 40% інцидентів кібербезпеки пов'язані з внутрішніми загрозами і ці цифри тільки ростуть, що свідчить про їх актуальність для сучасних організацій. Збитки від внутрішніх загроз можна побачити на рисунку 1.1.

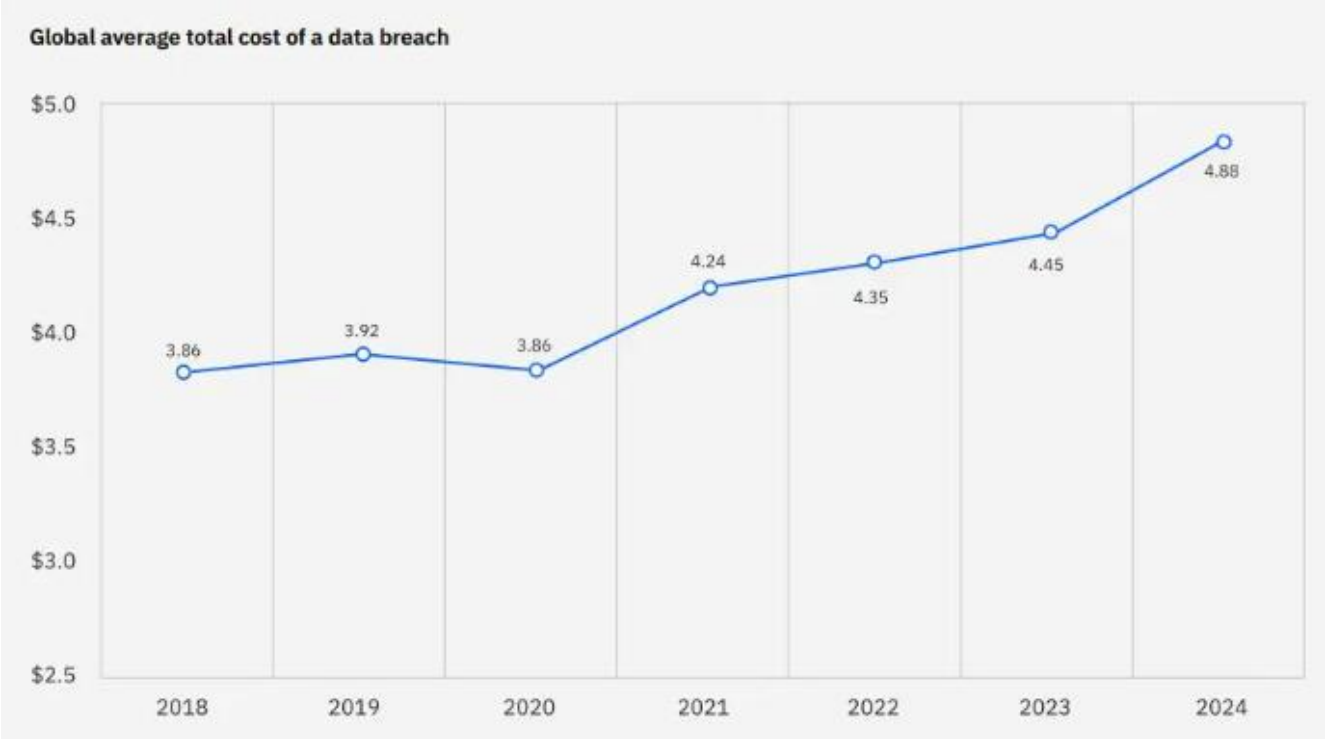

Рис. 1.1. Збитки від втрати даних згідно IBM Security [1]

У звіті Insider Threat Report 2023, підготовленому Cybersecurity Insiders, зазначається, що 74% організацій вважають себе принаймні помірно вразливими до внутрішніх загроз. Це цілком зрозуміло, адже значна частина атак, пов’язаних із зловмисними інсайдерами, а також витоків даних у 2022 році, була спричинена недбалістю користувачів, що підкреслює важливість проблеми [2].

Додатково, згідно з глобальним звітом Ponemon Institute про вартість інсайдерських ризиків за 2023 рік, дані якого ілюструються на рисунку 1.2, загальна середня вартість інцидентів, пов’язаних із внутрішніми загрозами, зросла майже на 95% за період з 2018 по 2023 рік. Це свідчить про зростання складності та масштабів інцидентів, а також про суттєві економічні втрати, які вони завдають організаціям.

Такі статистичні дані підкреслюють необхідність впровадження ефективних механізмів виявлення та запобігання внутрішнім загрозам, а також посилення культури кібергігієни серед співробітників, що є важливим аспектом забезпечення інформаційної безпеки у сучасних умовах.

Рис. 1.2. Загальна середня вартість інцидентів, пов'язаних з внутрішніми загрозами [3]

Компанії з Північної Америки найбільше страждають від внутрішніх атак та їх наслідків; середня вартість у цьому регіоні зросла з 11,1 мільйона доларів до 19,09 мільйона доларів за п’ять років. Середні загальні витрати на один інцидент внутрішньої загрози також зросли на 80% між 2016 і 2023 роками, це видно на рисунку 1.3 [2]. Пом’якшення внутрішніх загроз передбачає витрати на моніторинг

і стеження, розслідування, ескалацію, реагування на інциденти, локалізацію, фактичний аналіз і усунення.

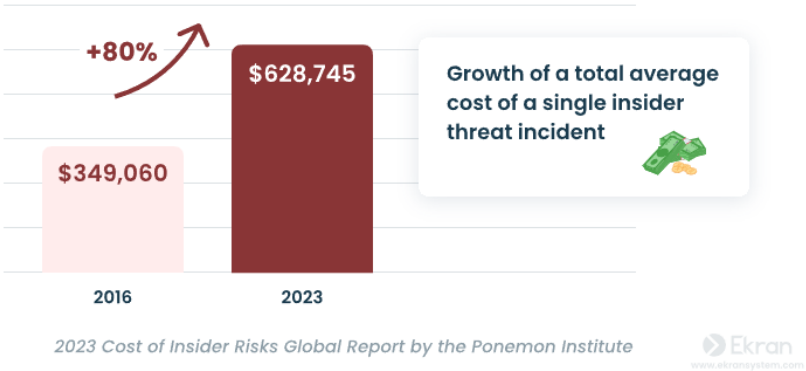

Рис. 1.3. Зростання збитків за внутрішні загрози [4]

Внутрішня загроза визначається як потенційна чи реальна небезпека, створена співробітниками, підрядниками чи іншими особами, які мають законний доступ до інформаційних систем організації. Ці загрози можуть бути класифіковані як навмисні (шкідливі дії, наприклад, викрадення даних) або ненавмисні (помилки чи недбалість, наприклад, відкриття фішингових повідомлень). Навмисні дії можуть бути мотивовані особистою вигодою, корпоративним шантажем або політичними мотивами, тоді як ненавмисні дії часто виникають через недостатній рівень обізнаності працівників щодо кібербезпеки. Зазвичай таких осіб називають інсайдерами.

Інсайдер це будь-яка особа, яка має або мала санкціонований доступ або знання про ресурси організації, включаючи персонал, приміщення, інформацію, обладнання, мережі та системи.

Приклади інсайдерів:

особа, якій організація довіряє, включно з співробітниками, членами організації та тими, кому організація надала конфіденційну інформацію та доступ до неї;

особа, яка отримала бейдж або пристрій доступу, що ідентифікує її як особу з регулярним або постійним доступом (наприклад, співробітник або член організації, підрядник, постачальник, зберігач або ремонтник);

особа, якій організація надала комп'ютер та/або доступ до мережі;

особа, яка розробляє продукти та послуги організації; ця група включає тих, хто знає секрети продуктів, що створюють цінність для організації;

особа, яка обізнана з основами діяльності організації, включаючи ціноутворення, витрати, а також сильні та слабкі сторони організації;

особа, яка обізнана з бізнес-стратегією та цілями організації, якій довірені плани на майбутнє або засоби для підтримки організації та забезпечення добробуту її людей;

у контексті державних установ інсайдером може бути особа, яка має доступ до захищеної інформації, що, у разі компрометації, може завдати шкоди національній та громадській безпеці.

Як вже писалося вище, внутрішні загрози поділяються на навмисні та ненавмисні.

Навмисні загрози навмисного інсайдера часто називають «зловмисним інсайдером». Навмисні загрози це дії, спрямовані на те, щоб завдати шкоди організації заради особистої вигоди або через особисту образу. Наприклад, багато інсайдерів мотивовані «поквитатися» через брак визнання (наприклад, підвищення, премії, бажані подорожі) або звільнення. Їхні дії можуть включати витік конфіденційної інформації, переслідування колег, саботаж обладнання, вчинення насильства або крадіжку службових даних чи інтелектуальної власності в хибній надії на просування по службі.

Ненавмисні загрози - інсайдери цього типу наражають організацію на загрозу через необережність, необачність, недбалість. Такі інсайдери, як правило, знайомі з політикою безпеки та/або IT-політикою, але вирішують їх ігнорувати, створюючи ризик для організації. Приклади включають в себе дозвіл комусь пройти через захищену точку входу, втрату портативного пристрою зберігання даних, що містить конфіденційну інформацію, ігнорування повідомлень про встановлення нових оновлень і патчів безпеки [5].

Випадкові - інсайдери цього типу помилково спричиняють ненавмисний ризик для організації. Приклади включають помилковий набір адреси електронної

пошти і випадкове відправлення конфіденційного бізнес-документа конкуренту, несвідоме або ненавмисне натискання на гіперпосилання, відкриття вкладення у фішинговому електронному листі, що містить вірус, або неналежна утилізація конфіденційних документів.

Зустрічаються й інші види внутрішніх загроз, такі як:

Змовницькі загрози це підгрупа зловмисних інсайдерських загроз називається змовницькими загрозами, коли один або кілька інсайдерів співпрацюють із зовнішнім суб'єктом загрози, щоб скомпрометувати організацію. Ці інциденти часто пов'язані з кіберзлочинцями, які вербують інсайдера або кількох інсайдерів для здійснення шахрайства, крадіжки інтелектуальної власності, шпигунства або поєднання цих трьох видів діяльності.

Загрози з боку третіх осіб - це, як правило, підрядники або постачальники, які не є офіційними членами організації, але яким надано певний рівень доступу до об'єктів, систем, мереж або людей для виконання їхньої роботи. Ці загрози можуть бути прямими або непрямими.

Причини виникнення внутрішніх загроз є різні, це може бути: насильство, шпигунство, саботаж, крадіжки та кібератаки.

Насильство - ця дія включає погрозу насильства(включаючи психологічне), а також іншу загрозливу поведінку, яка створює залякуюче, вороже або токсичне середовище.

Насильство на робочому місці/в організації - це будь-яка дія або загроза фізичного насильства, переслідування, сексуальні домагання, залякування, знущання, образливі жарти або інша загрозлива поведінка з боку колег або партнерів, що відбувається на робочому місці або під час роботи людини. Такі дії можуть підштовхнути працівника якось помститися колезі чи компанії.

Шпигунство - це таємна або незаконна практика шпигунства за іноземним урядом, організацією, юридичною або фізичною особою з метою отримання конфіденційної інформації для отримання військової, політичної, стратегічної або фінансової вигоди.

Економічне шпигунство - це таємна практика отримання комерційної

таємниці від іноземної держави (наприклад, усіх форм і видів фінансової, ділової, наукової, технічної, економічної або інженерної інформації, а також методів, прийомів, процесів, процедур, програм або кодів виробництва).

Урядове шпигунство - це таємний збір розвідувальної інформації одним урядом проти іншого з метою отримання політичної або військової переваги. Це також може включати шпигунство урядів за корпоративними структурами, такими як авіаційні компанії, консалтингові фірми, аналітичні центри або компанії, що виробляють боєприпаси. Державне шпигунство також називають збором розвідувальної інформації.

Кримінальне шпигунство - це коли громадянин Україну зраджує державну таємницю України іноземним державам.

Саботаж - описує навмисні дії, спрямовані на заподіянні шкоди фізичній або віртуальній інфраструктурі організації, включаючи недотримання процедур технічного обслуговування або IT-процедур, забруднення чистого простору, фізичне пошкодження обладнання або видалення коду з метою перешкоджання нормальному функціонуванню.

Фізичний саботаж - це навмисні дії, спрямовані на заподіяння шкоди фізичній інфраструктурі організації (наприклад, приміщенням або обладнанню).

Віртуальний саботаж - це зловмисні дії за допомогою технічних засобів, спрямовані на порушення або зупинку нормальної роботи організації.

Крадіжка це акт викрадення, будь то гроші або інтелектуальна власність.

Фінансові злочини - це несанкціоноване заволодіння або незаконне використання грошей чи майна особи, підприємства або організації з метою отримання вигоди.

Крадіжка інтелектуальної власності - це крадіжка або пограбування ідей, винаходів або творчих досягнень особи чи організації, включаючи комерційні таємниці та запатентовані продукти, навіть якщо концепції або предмети, що викрадаються, походять від самого злодія.

Кіберзагроза включає крадіжку, шпигунство, насильство та саботаж усього, що пов'язано з технологіями, віртуальною реальністю, комп'ютерами, пристроями

або інтернетом.

Ненавмисні загрози - це незловмисний (часто випадковий або ненавмисний) вплив на IT-інфраструктуру, системи та дані організації, який завдає ненавмисної шкоди організації. Приклади включають фішингові електронні листи, шкідливе програмне забезпечення та «шкідливу рекламу» (вбудовування шкідливого контенту в легальну рекламу в Інтернеті).

Навмисні загрози - це зловмисні дії зловмисних інсайдерів, які використовують технічні засоби, щоб порушити або зупинити звичайні бізнес-операції організації, виявити слабкі місця в IT, отримати захищену інформацію або іншим чином просунути план атаки через доступ до IT-систем. Ці дії можуть включати зміну даних, впровадження шкідливого програмного забезпечення або інших шкідливих програм для порушення роботи систем і мереж.

Ключовою особливістю внутрішніх загроз є складність їх виявлення. На відміну від зовнішніх атак, які можна визначити за аномаліями в мережевому трафіку чи за активністю з підозрілих IP-адрес, внутрішні загрози часто маскуються під легітимну діяльність. Традиційні засоби захисту, такі як міжмережеві екрани, системи запобігання вторгненням (IPS) та антивірусні рішення, зосереджені на периметровій безпеці і не пристосовані до аналізу поведінки уповноважених користувачів.

1.2. Аналіз підходів до виявлення внутрішньої загрози в інформаційних системах організацій

Внутрішні загрози в інформаційних системах залишаються однією з найбільш підступних проблем у сфері інформаційної безпеки. Ці загрози зазвичай виходять від людей, які мають легітимний доступ до системи, що робить їх особливо небезпечними. Відповідно, питання своєчасного ідентифікації таких загроз набуває першочергового значення, особливо у великих організаціях з розгалуженими інформаційними системами.

Виявлення внутрішніх загроз передбачає комплексний підхід, який об’єднує

кілька методологій, включаючи аналіз логів, Аналіз поведінки користувачів, машинне навчання, інтеграцію з SIEM-системами та концепцію Zero Trust. Розглянемо кожен з підходів детально.

На початку розглядаються традиційні методи, які історично використовуються для протидії внутрішнім загрозам. Ці підходи базуються на класичних принципах інформаційної безпеки, включаючи контроль доступу, моніторинг активності користувачів та використання базових засобів захисту.

Традиційні методи виявлення внутрішніх загроз залишаються основою багатьох систем захисту інформації. Вони базуються на перевірених часом підходах, таких як аналіз журналу подій, застосування систем правил і сигнатур, а також контроль доступу. Хоча ці підходи часто поступаються сучасним технологіям в ефективності, вони забезпечують фундаментальну безпеку і можуть бути корисними в комплексному захисті інформаційних систем.

Журнали подій - це основне джерело інформації про всі дії, які відбуваються в інформаційній системі [6]. Журнали подій фіксують такі аспекти, як:

спроби входу в систему (успішні та невдалі);

використання привілейованих облікових записів;

доступ до файлів, баз даних або конфіденційних ресурсів;

виконання адміністративних команд, змін конфігурації тощо.

Аналіз журналу подій допомагає виявляти аномальні дії, які можуть свідчити про внутрішню загрозу. Наприклад, якщо користувач виконує дії, що не відповідають його звичайним обов'язкам, це може бути ознакою компрометації його облікового запису.

Приклад: співробітник, який зазвичай працює з HR-документами, раптово отримує доступ до бази даних фінансових звітів, це може викликати підозру. Аналіз журналів подій дозволить виявити таку активність і ініціювати подальше розслідування.

Серед основних недоліків використання журналу подій можна виділити кілька ключових аспектів:

великі обсяги даних: сучасні інформаційні системи генерують мільйони

записів у журналах щодня;

трудомісткість аналізу: ручна обробка журналів подій вимагає значних зусиль і часто призводить до пропуску критичних сигналів;

нездатність передбачити загрози: аналіз журналу подій фокусується на вже здійснених діях, тому він не може запобігти загрозам.

Системи правил та сигнатур базуються на заздалегідь визначених шаблонах (сигнатурах) або встановлених правилах, які описують типову підозрілу активність [7]. Цей метод використовується в брандмауерах, антивірусних програмах, IDS/IPS (системах виявлення та запобігання вторгнень).

Наприклад, система може бути налаштована для виявлення таких сценаріїв:

кілька невдалих спроб входу в обліковий запис протягом короткого часу;

завантаження великих обсягів конфіденційних даних;

використання несанкціонованих пристроїв для доступу до корпоративної мережі.

Серед основних недоліків використання систем правил та сигнатур можна виділити кілька ключових аспектів:

залежність від бази сигнатур: якщо шаблон загрози не включений у базу, система його не виявить;

складність налаштування: правила повинні бути адаптовані до особливостей організації, що вимагає значних зусиль і знань;

вразливість до нових атак: зловмисники можуть використовувати нестандартні методи, які не відповідають встановленим сигнатурам.

Контроль доступу - передбачає управління доступом до інформаційних ресурсів на основі ролей та привілеїв користувачів. Реалізація контролю доступу базується на принципі мінімальних привілеїв: користувач отримує доступ лише до тих ресурсів, які потрібні для виконання його обов'язків.

Приклади реалізації:

рольовий доступ (Role-Based Access Control, RBAC): доступ до ресурсів визначається на основі ролі співробітника в організації. Наприклад, HR-відділ має доступ до персональних даних співробітників, але не до фінансових звітів.

атрибутивний доступ (Attribute-Based Access Control, ABAC): враховуються додаткові атрибути, такі як місце розташування, тип пристрою, час доступу.

Серед основних недоліків використання контролю доступу можна виділити кілька ключових аспектів:

складність управління: у великих організаціях може бути складно налаштувати та підтримувати актуальність політик доступу;

ризики компрометації облікових записів: навіть найкращі політики не гарантують захисту від зловживання легітимними обліковими записами.

Розглянемо аналіз поведінки користувачів як важливий інструмент у забезпеченні кібербезпеки.

Аналіз поведінки користувачів (UBA) - це практика збору та аналізу даних про активність користувачів для створення базової лінії їхньої нормальної поведінки та вподобань [8]. Розробляючи ці базові лінії для кожного користувача та відстежуючи їхню активність у реальному часі, UBA допомагає організаціям виявляти порушення. Коли виникає підозріла поведінка, команди можуть ідентифікувати потенційні загрози безпеці, спроби несанкціонованого доступу та витоки даних.

Основні етапи поведінкового аналізу включають в себе: формування базових моделей, моніторинг та виявлення аномалій, кореляція даних та оцінку ризиків. Розглянемо кожний з цих етапів окремо.

Формування базових моделей поведінки є ключовим етапом у впровадженні систем аналізу поведінки користувачів. Цей процес полягає у зборі та обробці даних про типову активність користувачів у межах інформаційної системи, таких як:

час і частота входу до системи;

обсяги та типи переданих даних;

джерело доступу (IP-адреса, пристрій, географічне положення);

операції з файлами (створення, видалення, копіювання);

використання привілейованих команд або ресурсів.

На основі цих даних створюються поведінкові профілі, які відображають

нормальні шаблони взаємодії з ресурсами, додатками та системами.

Такі моделі являються базовою точкою відліку для виявлення аномалій, оскільки вони дозволяють ідентифікувати дії, які виходять за межі звичайної поведінки. Це, у свою чергу, підвищує ефективність системи виявлення загроз, особливо тих, що пов’язані з внутрішніми ризиками.

Моніторинг та виявлення аномалій є невід'ємними складовими забезпечення інформаційної безпеки, особливо в контексті внутрішніх загроз. Цей процес спрямований на безперервний збір та аналіз даних про активність користувачів і систем у реальному часі для ідентифікації відхилень від типових поведінкових моделей.

Зібрані моделі використовуються як еталон для оцінки поточних дій користувачів. Якщо поведінка користувача суттєво відхиляється від базового профілю, це може бути сигналом потенційної загрози, таких як:

співробітник починає завантажувати значні обсяги даних у неробочий час;

користувач звертається до ресурсів, які не пов’язані з його звичайними завданнями;

виявляються багаторазові спроби доступу до захищених зон.

Системи моніторингу автоматично виявляють подібні аномалії, використовуючи алгоритми машинного навчання та статистичний аналіз. Це дозволяє швидко реагувати на потенційні загрози, знижуючи ризик витоків даних або інших інцидентів безпеки.

Кореляція даних є ключовим процесом в кібербезпеці, який дозволяє поєднувати різнорідні події, зібрані з різних джерел, у єдину структуру для глибокого аналізу та виявлення загроз. Мета кореляції полягає у визначенні зв’язків між на перший погляд незалежними подіями, що можуть свідчити про цілеспрямовану або аномальну активність.

Щоб уникнути помилкових спрацьовувань, системи UBA зазвичай інтегрують кілька джерел даних, включаючи:

журнали подій;

дані про мережеву активність;

інформацію про роботу кінцевих пристроїв;

дані про використання облікових записів (наприклад, зміна паролів або багатофакторна аутентифікація).

Алгоритми кореляції часто інтегруються в системи управління подіями та інформацією про безпеку (SIEM), що дозволяє автоматизувати цей процес. Такий підхід забезпечує більш швидке реагування на загрози, знижує кількість помилкових сповіщень і допомагає фахівцям з безпеки ефективніше працювати з великими обсягами даних.

Оцінка ризиків є важливим етапом у забезпеченні кібербезпеки, спрямованим на виявлення, аналіз та визначення пріоритетності потенційних загроз, що можуть негативно вплинути на організацію. Цей процес допомагає ідентифікувати слабкі місця у системах, які зловмисники або внутрішні порушники можуть використати для реалізації своїх цілей.

Сучасні системи аналізу поведінки користувача включають механізми для оцінки ризиків кожної аномалії. Це дозволяє визначити, наскільки дії користувача можуть бути небезпечними. Наприклад, одноразове завантаження великого обсягу даних може мати низький ризик, якщо воно відбувається з корпоративного пристрою. Однак, якщо завантаження виконується з нового пристрою в іншій країні, ризик буде значно вищим.

Приклади використання:

захист від витоку даних - якщо співробітник, який зазвичай працює з одним сервером, раптово завантажує великі обсяги даних з кількох серверів, система може позначити цю активність як аномалію;

виявлення компрометації облікових записів - у випадку, якщо користувач входить у систему з географічного місця, яке відрізняється від його звичайного місця роботи, це може свідчити про несанкціоноване використання облікового запису;

ідентифікація зловмисних дій інсайдерів - співробітник, який зазвичай не має справи з фінансовими даними, починає активно працювати з такими документами.

Застосування сучасних інструментів, таких як системи аналізу поведінки

користувачів або управління інформаційною безпекою, дозволяє автоматизувати процес оцінки ризиків, підвищуючи його точність і знижуючи час, необхідний для аналізу.

Регулярна та систематична оцінка ризиків дозволяє організаціям оперативно реагувати на змінні умови, підвищувати загальну стійкість до загроз та забезпечувати ефективний захист інформаційних активів.

До переваг аналізу поведінки користувачів можна віднести наступні аспекти:

гнучкість: здатність адаптуватися до нових типів загроз, які не описані в сигнатурах;

зниження помилкових спрацьовувань: аналіз контексту дозволяє більш точно оцінити ризик.

До основних недоліків використання аналітики поведінки користувача можна віднести наступні аспекти:

високі вимоги до обчислювальних ресурсів: аналіз поведінки великої кількості користувачів потребує значної потужності;

складність налаштування: система повинна бути правильно налаштована для врахування специфіки організації;

ризик втрати конфіденційності: моніторинг дій користувачів може викликати побоювання щодо приватності.

Розглянемо машинне навчання як одну з ключових технологій, що забезпечує інноваційні підходи в галузі кібербезпеки.

Машинне навчання (ML) є ключовою технологією в сучасному аналізі поведінки користувачів. Воно дозволяє автоматично виявляти аномалії, аналізувати великі обсяги даних і виявляти внутрішні загрози з мінімальним втручанням людини. У цьому контексті ML використовує моделі для аналізу звичної поведінки користувачів і визначення аномальних дій, які можуть сигналізувати про потенційні загрози, такі як компрометація облікових записів або шкідливі дії інсайдерів.

Основними аспектами застосування машинного навчання в UBA є: аналіз великих даних, створення профілів поведінки та виявлення аномалій. Розглянемо

більш детально кожен з цих аспектів.

Аналіз великих даних (Big Data) - у сучасних інформаційних системах генеруються величезні обсяги даних: журнали подій, записи мережевого трафіку, метадані файлів тощо. Машинне навчання дозволяє обробляти ці дані в реальному часі та виявляти закономірності.

Створення профілів поведінки є важливим аспектом у застосуванні методів аналізу поведінки користувачів для виявлення та запобігання внутрішнім загрозам. Цей процес передбачає збір та аналіз даних про звичайну активність користувачів у системі для формування їхніх індивідуальних профілів.

ML допомагає будувати індивідуальні профілі користувачів, які відображають:

звичний час входу в систему;

обсяги та типи переданих даних;

частоту звернення до різних ресурсів;

мережеві з'єднання та IP-адреси.

Зібрані дані дозволяють автоматично ідентифікувати відхилення від стандартної поведінки, що може вказувати на потенційно шкідливі дії або загрози. Важливо, що процес створення профілів може бути налаштований відповідно до специфіки діяльності організації, що забезпечує високу точність виявлення аномалій.

Виявлення аномалій є важливою складовою системи безпеки, що спрямована на ідентифікацію незвичайної або підозрілої активності в інформаційних системах. Цей процес включає моніторинг діяльності користувачів, систем та мереж з метою виявлення відхилень від нормальної поведінки, які можуть свідчити про потенційні загрози або інциденти безпеки.

Порівнюючи поточну поведінку користувача з його профілем, алгоритми можуть ідентифікувати аномальні дії, такі як:

завантаження великих обсягів конфіденційних даних;

доступ до незвичних ресурсів;

використання нового пристрою або входу з іншого географічного

розташування.

До переваг використання машинного навчання в аналітиці поведінки користувача можна віднести наступні аспекти:

автоматизація: зменшує навантаження на аналітиків безпеки;

виявлення складних загроз: здатність працювати з багатовимірними даними;

адаптивність: моделі можуть оновлюватися в міру надходження нових даних;

зниження кількості помилкових спрацьовувань: точніші профілі поведінки допомагають мінімізувати помилкові аномалії.

До основних недоліків використання машинного навчання можна віднести наступні аспекти:

потреба у великих обсягах даних: для навчання алгоритмів потрібні великі й якісні набори даних;

складність впровадження: налаштування ML-систем вимагає експертних знань;

можливі помилкові спрацьовування: алгоритми можуть сприймати легітимні дії як загрозу.

Розглянемо більш детально концепцію Zero Trust.

Концепція «нульової довіри» переглядає робочі процеси на основі відсутності довіри до будь-якого користувача перед початком кожної операції. Для цього система повинна автоматично проводити процедуру автентифікації та авторизації користувача, перш ніж надати йому доступ до будь-якого застосунку, бази даних або інших ресурсів компанії. Крім того, у процесі роботи з додатками і даними статус авторизації кожного користувача постійно перевіряється ще раз.

Принципи роботи моделі Zero Trust [9]:

зловмисники всюди - передбачається, що хакери діють як зовні, так і всередині мережі, отже, жодному пристрою або користувачеві за замовчуванням не можна довіряти.

недовіра до кінцевих пристроїв - якщо пристрій оснащений адекватними засобами управління безпекою, адміністратор кінцевих точок повинен провести їхню перевірку. Захист кінцевих пристроїв має поширюватися і на аутентифікатор,

щоб гарантувати, що використовуються тільки перевірені пристрої, а особисті ключі захищені належним чином;

мінімум доступу для користувачів - якщо користувачам дозволено доступ тільки до тих даних, які їм необхідні, мінімізується взаємодія між ними і конфіденційними даними в мережі. Принципи «довіряй усім усередині периметра» або «довіряй, але перевіряй» більше не працюють;

мікросегментація для безпеки - передбачає поділ кожної частини мережі на більш дрібні сегменти - за типом даних - і для кожного з цих сегментів окреме налаштування параметрів безпеки та відокремлений доступ. Це гарантує, що користувачі не зможуть отримати доступ до інших зон без додаткової аутентифікації;

управління доступом для зменшення поверхні атаки - застосовуючи жорстке управління доступом користувачів і пристроїв до своєї мережі, організація зменшує поверхню атаки. Важливо стежити за тим, як пристрої отримують доступ до мережі, щоб гарантувати, що кожен з них пройшов авторизацію. Управління доступом має захищати ключові системи шляхом надання мінімуму привілеїв, необхідного для виконання завдань;

багатофакторна аутентифікація (MFA) - перш ніж отримати доступ, користувачі повинні пройти перевірку за допомогою надійної аутентифікації. Двофакторна автентифікація (2FA) вважається менш надійною, ніж MFA, і не відповідає стандартам Zero Trust, оскільки може помилково підтвердити особу користувача;

До основних переваг використання концепції Zero Trust можна віднести наступні аспекти:

підвищення точності виявлення загроз - завдяки постійному аналізу поведінки користувачів і контексту їхніх дій знижуються ризики пропуску загроз;

захист від інсайдерських загроз - навіть користувачі з привілейованим доступом підлягають перевірці. User Behavior Analytics дозволяє ідентифікувати нетипову поведінку, навіть якщо дії формально відповідають політикам доступу;

мінімізація потенційного збитку - сегментація доступу та обмеження

привілеїв унеможливлюють масштабний вплив компрометації одного користувача чи пристрою;

підтримка динамічних робочих середовищ - Zero Trust легко адаптується до сучасних хмарних інфраструктур і віддалених робочих середовищ, де традиційні моделі периметральної безпеки є малоефективними.

До основних недоліків використання концепції Zero Trust можна віднести наступні аспекти:

складність впровадження - реалізація Zero Trust потребує значного перегляду інфраструктури безпеки організації;

високі вимоги до даних - ефективний аналіз поведінки потребує доступу до великих обсягів якісних даних, що може ускладнюватися через різнорідність джерел;

людський фактор - навіть найкращі технології можуть бути малоефективними без належної підготовки співробітників і їхнього розуміння концепції Zero Trust.

1.3. Аналіз існуючих рішень для виявлення внутрішньої загрози в інформаційних системах організацій

Оскільки на сучасному ринку представлено надзвичайно широкий спектр інструментів кібербезпеки, вибір оптимального рішення для управління внутрішніми загрозами стає складним завданням. Необхідність звузити цей вибір до певної лінії захисту та визначити програмне забезпечення, яке забезпечуватиме максимальну ефективність за мінімальних зусиль, є актуальним викликом для організацій. Серед найбільш затребуваних інструментів та заходів для протидії внутрішнім ризикам можна виокремити п’ять ключових напрямів: навчання та обізнаність користувачів , запобігання втраті даних (DLP), безпека та керування подіями (SIEM), керування привілейованим доступом (PAM) і аналітика поведінки користувачів (UBA).

Як показано на рисунку 1.4, ці п’ять напрямів визнані найефективнішими у

боротьбі з внутрішніми ризиками відповідно до глобального звіту про внутрішні загрози, підготовленого Інститутом Ponemon у 2023 році. Їхня популярність зумовлена не лише високим рівнем витрат на впровадження, але й значними перевагами у виявленні та запобіганні потенційним загрозам, що робить їх основними складовими сучасної стратегії кіберзахисту.

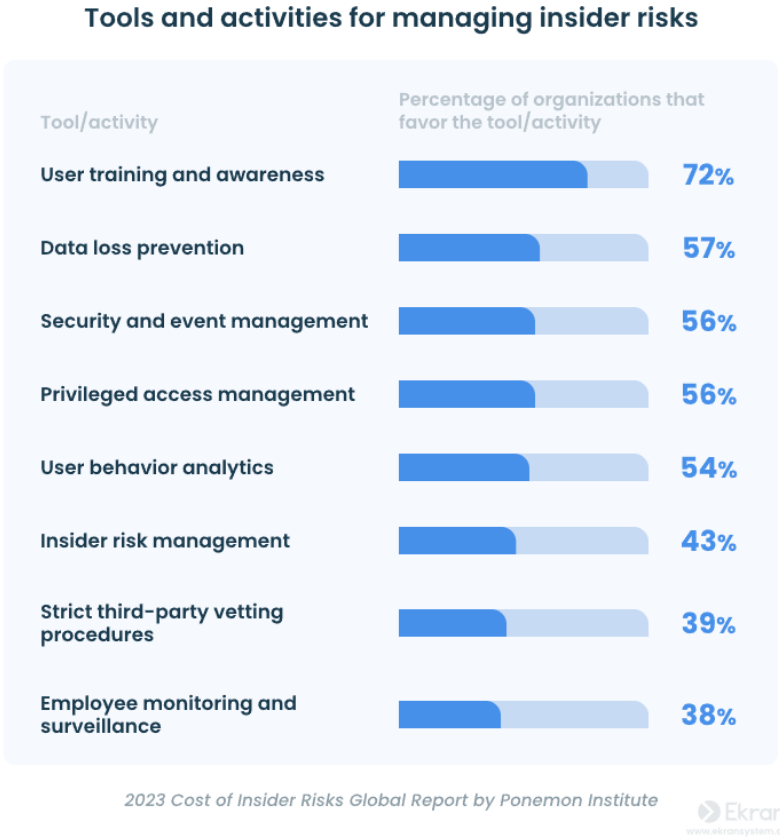

Рис. 1.4. Інструменти та заходи для управління внутрішніми ризиками [4]

Рішення для виявлення внутрішніх загроз можна умовно класифікувати за кількома основними категоріями, кожна з яких орієнтована на вирішення конкретних завдань із забезпечення інформаційної безпеки в організаціях, такими як: навчання та обізнаність користувачів, User Behavior Analytics, SIEM-рішення, Data Loss Prevention , Privileged Access Management. Детально розглянемо кожне з цих рішень.

Навчання та обізнаність користувачів є одним із ключових компонентів у забезпеченні кібербезпеки, оскільки воно спрямоване на мінімізацію ризиків, пов’язаних із людським фактором. Незважаючи на технологічну складність систем

захисту, працівники організації часто залишаються найуразливішою ланкою, через яку можуть бути реалізовані атаки, зокрема фішинг, соціальна інженерія або ненавмисне порушення правил безпеки.

Основними функціями навчання та обізнаності користувачів є:

проведення регулярних тренінгів з кібербезпеки для співробітників;

імітація фішингових атак для підвищення обізнаності користувачів;

надання актуальної інформації про сучасні загрози та способи їх уникнення;

створення культури безпеки, яка мотивує користувачів дотримуватися політик організації.

До переваг методу навчання та обізнаність користувачів можна віднести наступні аспекти:

зменшення ризику інцидентів через людські помилки;

підвищення загальної обізнаності співробітників щодо актуальних загроз;

створення першої лінії захисту, що зменшує навантаження на технічні системи безпеки.

До основних недоліків методу можна віднести наступне:

високі витрати часу та ресурсів на організацію навчальних заходів;

можливість зниження ефективності без постійного оновлення тренінгів;

різний рівень сприйняття матеріалу серед співробітників.

User Behavior Analytics орієнтовані на детальний аналіз поведінкових моделей користувачів і автоматичне виявлення аномалій, які можуть свідчити про потенційні загрози безпеці. Ці моделі базуються на зборі та обробці великих обсягів даних про активність користувачів у інформаційній системі, таких як час входу в систему, доступ до файлів, використання програмного забезпечення, мережеві підключення, що робить їх потужним інструментом у забезпеченні кібербезпеки в контексті виявлення внутрішніх загроз.

Основними функціями моделі User Behavior Analytics є:

використання методів машинного навчання для створення поведінкових профілів;

інтеграція великих даних для адаптації до нових загроз;

пріоритезація подій для зниження помилкових спрацьовувань.

До основних переваг використання моделі UBA можна віднести :

здатність проактивного виявлення загроз;

мінімізація втручання у конфіденційність через анонімізацію аналізу.

До основних недоліків даної системи часто відносять:

високі вимоги до впровадження;

залежність від якісних даних для ефективного навчання моделей.

Системи управління інформацією та подіями безпеки представляють собою комплексні рішення, які забезпечують інтегрований підхід до виявлення та аналізу загроз інформаційної безпеки. Вони поєднують можливості кореляції подій з елементами поведінкового аналізу, що дозволяє отримувати більш детальну картину стану безпеки в організації.

Основним завданням SIEM-систем є:

централізоване збирання, обробка та аналіз даних із різних джерел, таких як журнали подій, мережевий трафік, активність користувачів та інші показники;

автоматизація процесу реагування на інциденти, що включає генерацію сповіщень, запуск заздалегідь налаштованих сценаріїв реагування та інтеграцію з іншими системами безпеки для швидкого усунення виявлених загроз.

До основних переваг SIEM-систем можна віднести наступне:

комплексне рішення з широкими можливостями інтеграції;

централізований контроль безпеки.

До основних недоліків SIEM-систем можна віднести наступне:

висока вартість;

потребує досвідченого персоналу для налаштування та підтримки.

Системи запобігання втраті даних призначені для забезпечення захисту конфіденційної інформації від несанкціонованого доступу, витоку або передачі за межі організації. Ці рішення спрямовані на виявлення, контроль і запобігання як умисним, так і випадковим діям співробітників, які можуть призвести до компрометації даних.

Основними функціями DLP-системи є:

контроль передачі даних через електронну пошту, USB, хмарні сервіси тощо;

моніторинг, класифікація та захист чутливих даних відповідно до політик організації;

налаштування політик для блокування дій або попередження користувачів.

До основних переваг DLP-систем можна віднести наступне:

висока ефективність у запобіганні витоків даних;

дозволяє виявити спроби несанкціонованого доступу до даних;

легко інтегрується з іншими рішеннями для інформаційної безпеки.

До основних недоліків DLP-систем можна віднести наступне:

відсутність можливостей для поведінкового аналізу;

потребує значних зусиль для налаштування політик і навчання персоналу;

можливість блокування легітимних дій, що може впливати на продуктивність.

Система управління привілейованим доступом є інструментом, призначеним для забезпечення контролю, моніторингу та управління обліковими записами користувачів, які мають розширені права доступу до критично важливих систем і даних.

До основних функцій PAM-систем можна віднести:

централізоване управління обліковими записами з привілейованим доступом;

надання тимчасового доступу до критичних систем за запитом;

моніторинг та запис сесій для виявлення аномальної поведінки;

впровадження принципу найменших привілеїв для зниження ризиків.

До основних переваг PAM-систем можна віднести наступне:

забезпечення контролю за обліковими записами з високим рівнем доступу;

зниження ризику витоку критичної інформації;

інтеграція з іншими засобами безпеки для розширеного моніторингу.

Основними недоліками PAM-систем є:

складність у впровадженні та підтримці системи;

залежність від правильної конфігурації для запобігання помилкам;

потреба в навчанні персоналу для ефективного використання.

Порівняння вищезазначених програм та методів зображено на таблиці 1.1.

Таблиця 1.1

Порівняльна таблиця засобів боротьби з внутрішніми загрозами

Характеристика	Навчання та обізнаність користувачів	UBA (User Behavior Analytics)	SIEM (Security Information and Event Management)	DLP (Data Loss Prevention)	PAM (Privileged Access Management)
Основна мета	Підвищення знань співробітників про загрози	Виявлення аномалій у поведінці користувачів	Інтеграція подій безпеки з різних джерел	Захист від втрат даних та контроль передачі	Захист і контроль привілейованих облікових записів
Підхід до виявлення загроз	Освітній: запобігання людським помилкам	Аналіз поведінкових моделей користувачів	Кореляція даних із журналів і подій	Моніторинг і контроль доступу до даних	Управління та моніторинг сесій привілейованих користувачів
Придатність для проактивного захисту	Слабка (залежить від рівня знань користувачів)	Сильна (ідентифікація аномальної поведінки)	Помірна (залежить від правил кореляції)	Середня (обмеження доступу та запобігання передачі)	Сильна (обмеження доступу та моніторинг)
Область застосування	Людський фактор, фішинг, базові знання безпеки	Виявлення внутрішніх загроз і аномалій	Централізований аналіз подій і реагування	Захист конфіденційної інформації	Захист критичних облікових записів і сесій
Сумісність з іншими рішеннями	Висока (може доповнювати технічні засоби)	Висока (інтеграція з SIEM та іншими інструментами)	Висока (підтримка інтеграції з UBA, DLP тощо)	Помірна (потрібна інтеграція з іншими системами)	Висока (інтеграція з SIEM та іншими засобами)
Роль у боротьбі з внутрішніми загрозами	Навчання користувачів знижує ймовірність помилок	Виявлення прихованих аномалій у поведінці	Швидке реагування та аналіз інцидентів	Запобігання витоку критичних даних	Обмеження доступу до критичних систем

Результати аналізу рішень для протидії внутрішнім загрозам в інформаційних системах організацій свідчать про їхній широкий функціональний потенціал і різноманітність підходів. Це забезпечує можливість адаптивного

вибору інструментів, які найкраще відповідають специфічним потребам та вимогам кожної організації, зокрема з урахуванням її розміру, структури та рівня ризиків.

Навчання та обізнаність користувачів відіграють важливу роль у запобіганні загрозам, зосереджуючись на людському факторі. Вони сприяють зниженню ймовірності помилок шляхом освітніх програм, однак ефективність цього методу залежить від регулярності навчання та дисципліни співробітників.

UBA вирізняється своєю проактивністю, оскільки забезпечує ідентифікацію прихованих загроз через аналіз поведінкових аномалій. Ці системи знижують ризики складних атак завдяки використанню методів машинного навчання, але вимагають значних ресурсів для впровадження та якісних даних для ефективної роботи.

SIEM є базовим компонентом інтегрованого підходу до кібербезпеки, забезпечуючи централізований збір і аналіз подій. Попри широкий функціонал і можливість інтеграції з іншими рішеннями, ефективність SIEM залежить від рівня компетенцій команди з безпеки та складності налаштування.

DLP фокусується на захисті конфіденційної інформації, попереджаючи витоки даних через контроль каналів передачі. Це рішення обмежене у можливостях виявлення загроз, не пов'язаних безпосередньо з витоками, але є ефективним у захисті інформаційних активів організації.

PAM орієнтоване на жорсткий контроль і моніторинг привілейованих облікових записів. Завдяки зниженню ризиків, пов'язаних зі зловживанням доступом до критичних систем, PAM є важливим компонентом у захисті від внутрішніх загроз, хоча впровадження цих систем вимагає високих ресурсів і складного налаштування.

Таким чином, ефективний захист від внутрішніх загроз потребує комплексного підходу, який включає як технологічні рішення (UBA, SIEM, DLP, PAM), так і освітні ініціативи, спрямовані на підвищення обізнаності співробітників. Поєднання цих інструментів забезпечує багаторівневий захист і дозволяє адаптуватися до динамічних викликів кіберзагроз.

У подальшому буде здійснено порівняльний аналіз наявних рішень, що

використовуються для протидії внутрішнім загрозам, з метою оцінки їх функціональних можливостей та ефективності, таких як: Microsoft Defender for Identity, Splunk User Behavior Analytics, InsightIDR, Exabeam User and Entity Behavior Analytics та IBM QRadar User Behavior Analytics.

Microsoft Defender for Identity (раніше відомий як Azure Advanced Threat Protection) є сучасним рішенням, спрямованим на аналіз дій користувачів з метою виявлення потенційно шкідливої активності в гібридних та хмарних середовищах. Завдяки використанню поведінкового аналізу, цей інструмент дозволяє ідентифікувати аномалії, які можуть свідчити про внутрішні або зовнішні загрози, забезпечуючи таким чином проактивний підхід до захисту ідентичностей у корпоративних системах.

До особливостей Microsoft Defender for Identify можна віднести:

аналіз ризиків облікових записів: Виявлення компрометацій облікових записів та неприродної активності;

інтеграція з Microsoft 365: Аналіз дій користувачів у середовищі Office, Azure Active Directory тощо;

прогнозування загроз: Побудова моделей поведінки для раннього попередження.

Microsoft Defender for Identify має наступні переваги:

глибока інтеграція з хмарними та локальними продуктами Microsoft;

висока точність аналізу завдяки взаємодії з Azure AD;

простота розгортання для організацій, що використовують екосистему Microsoft.

Microsoft Defender for Identify має наступні недоліки:

менш ефективне використання в організаціях, що не залежать від Microsoft;

залежність від ліцензування Microsoft 365 і Azure.

Splunk UBA є високоефективним інструментом для аналізу поведінкових шаблонів користувачів, який розроблено на основі методів машинного навчання та статистичного аналізу. Це рішення забезпечує автоматичне виявлення аномалій у поведінці користувачів, які можуть свідчити про внутрішні загрози, включаючи

спроби несанкціонованого доступу або інші потенційно шкідливі дії. Splunk UBA дозволяє організаціям отримувати глибоке розуміння активності користувачів і забезпечує своєчасне реагування на інциденти, що підвищує загальний рівень кібербезпеки.

До особливостей Splunk UBA можна віднести:

машинне навчання: Алгоритми автоматично створюють профілі нормальної поведінки кожного користувача;

виявлення аномалій: Система сигналізує про підозрілу активність, наприклад, доступ до великих обсягів конфіденційних даних у неробочий час;

інтеграція: Splunk UBA інтегрується з іншими продуктами Splunk, зокрема з Splunk SIEM.

Splunk UBA має наступні переваги:

висока точність аналізу завдяки адаптивному машинному навчанню;

мінімізація хибнопозитивних спрацювань.

Splunk UBA має наступні недоліки:

висока вартість впровадження та підтримки;

потребує значних обчислювальних ресурсів для роботи.

InsightIDR це інструмент для аналізу та реагування на інциденти, розроблений компанією Rapid7, є інтегрованим рішенням, яке поєднує функціональність аналітики поведінки користувачів та систем управління інформацією й подіями безпеки. Цей інструмент забезпечує детальний поведінковий аналіз активності користувачів і автоматизоване виявлення аномалій, а також пропонує засоби для оперативного реагування на загрози. InsightIDR спрямований на прискорення ідентифікації інцидентів безпеки та підвищення ефективності їх нейтралізації, що робить його цінним компонентом комплексної системи захисту інформаційних ресурсів.

До особливостей InsightIDR можна віднести:

інтегрована UEBA: Використання поведінкових моделей для моніторингу користувачів і облікових записів;

автоматизація реагування: Швидке генерування інцидентів із підтримкою

SOAR.

InsightIDR має наступні переваги:

простота впровадження у мультихмарних середовищах;

наявність інструментів для активного пошуку загроз;

висока швидкість обробки даних.

InsightIDR має наступні недоліки:

потребує спеціалізованого налаштування для ефективної роботи;

відносно менша масштабованість у порівнянні з конкурентами.

Exabeam UEBA є спеціалізованим рішенням, орієнтованим на аналіз поведінкових моделей користувачів і об'єктів у межах інформаційних систем організації. Використовуючи передові алгоритми машинного навчання, цей інструмент здійснює прогнозування та виявлення потенційних загроз. Завдяки можливостям автоматичного виявлення аномалій, Exabeam UEBA дозволяє значно підвищити ефективність заходів безпеки та забезпечити своєчасне реагування на підозрілу активність.

До особливостей Exabeam UEBA можна віднести:

ідентифікація аномалій: Система виділяє аномальні активності, що виходять за межі нормального поведінкового профілю.

інтеграція з іншими SIEM-рішеннями: Підтримка інтеграції з популярними SIEM-продуктами.

автоматизований аналіз: Швидка обробка великих обсягів даних.

Exabeam UEBA має наступні переваги:

незалежність від конкретної SIEM-платформи;

широкі можливості адаптації під індивідуальні сценарії;

інтуїтивна візуалізація для розуміння загроз.

Exabeam UEBA має наступні недоліки:

потребує значних ресурсів для обробки великих даних;

відсутність вбудованих засобів реагування на інциденти.

QRadar User Behavior Analytics є розширенням для платформи SIEM, розробленої компанією IBM. Це рішення інтегрує функціонал аналізу поведінки

користувачів із традиційними можливостями SIEM, що дозволяє отримувати детальне розуміння активності користувачів у межах інформаційної системи організації. Завдяки поєднанню поведінкової аналітики та потужного інструментарію SIEM, QRadar UBA ефективно ідентифікує внутрішні загрози, підвищуючи рівень інформаційної безпеки та забезпечуючи проактивний підхід до управління ризиками.

До особливостей QRadar UBA можна віднести:

аналітика поведінки: Система використовує UBA для створення поведінкових профілів і виявлення відхилень;

централізація даних: Усі журнали подій об’єднуються на платформі QRadar для аналізу в реальному часі;

інтеграція з існуючими інфраструктурами: Підтримка різних джерел даних, таких як системи автентифікації, журнали доступу та UAM.

QRadar UBA має наступні переваги:

гнучкість і адаптивність завдяки масштабованості SIEM;

можливість автоматизації реагування на інциденти.

QRadar UBA має наступні недоліки:

висока складність налаштування;

вимоги до компетенцій команди з кібербезпеки.

Порівняння вищезазначених існуючих рішень представлені у вигляді таблиці 1.2.

Таблиця 1.2

Порівняння існуючих рішень

Характеристика	QRadar User Behavior Analytics	Splunk User Behavior Analytics	Microsoft Defender for Identity	InsightIDR	Exabeam (UEBA)
Тип рішення	Інтеграція UBA із SIEM	Інтеграція UBA із SIEM	Інструмент захисту Active Directory	Інтегроване рішення для SIEM та UBA	Незалежне UEBA-рішення

Продовження таблиці 1.2

Характеристика	QRadar User Behavior Analytics	Splunk User Behavior Analytics	Microsoft Defender for Identity	InsightIDR	Exabeam (UEBA)
Методології виявлення	Машинне навчання, поведінковий аналіз, кореляція подій	Машинне навчання, поведінковий аналіз, аналітика великих даних	Поведінковий аналіз, сигнатурний підхід	Машинне навчання, поведінковий аналіз, сигнатурний підхід	Машинне навчання, поведінковий аналіз, автоматизація
Особливості	Інтеграція з широким спектром джерел даних	Гнучкість у налаштуванні, аналіз великих обсягів даних	Глибока інтеграція з Azure та Active Directory	Аналіз мережевих аномалій, спрощення реагування	Автоматизація розслідувань, створення детальних профілів
Переваги	Централізація даних, глибокий аналіз загроз, адаптивність	Швидке налаштування, підтримка широкого спектру інтеграцій	Оптимізовано для роботи з Azure, спрощує захист від загроз	Простота у використанні, інтуїтивний інтерфейс	Висока автоматизація, гнучкість у масштабуванні
Недоліки	Висока складність налаштування, вимоги до досвідченого персоналу	Висока вартість, вимоги до досвіду в аналізі великих даних	Обмежена підтримка інтеграції із сторонніми системами	Обмежена масштабованість для великих організацій	Висока вартість впровадження
Цільова аудиторія	Великі організації з розвиненою IT-інфраструктурою	Організації, які потребують адаптивної аналітики	Організації, які використовують інфраструктуру Microsoft	Середні компанії з обмеженими ресурсами	Організації, які потребують спеціалізованого UEBA-рішення

Вибір рішення залежить від потреб організації, її інфраструктури та бюджету. Організаціям зі складними середовищами і великими обсягами даних варто розглянути QRadar UBA чи Splunk UBA. Менші компанії або ті, хто працює у хмарному середовищі Microsoft, можуть знайти оптимальне рішення в Microsoft Defender for Identity або InsightIDR. Для гнучких та незалежних сценаріїв використання ефективним є Exabeam UEBA.

Інтеграція цих рішень із іншими інструментами, як-от DLP або PAM, може

суттєво посилити загальну безпеку організації.

Gartner [10] зазначає, що IBM визнана лідером у магічному квадранті Gartner 2024 для SIEM.

IBM була визнана лідером і оцінена за свій QRadar SIEM в 2024 Gartner Magic Quadrant для управління інформацією та подіями безпеки (SIEM), відзначивши 14-й раз поспіль, коли IBM була названа лідером в цьому звіті. Результати звіту представлені у вигляді рисунку 1.5.

Рис. 1.5. Gartner Magic Quadrant 2024 [10]

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ВНУТРІШНЬОЇ ЗАГРОЗИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОРГАНІЗАЦІЇ НА БАЗІ QRADAR USER BEHAVIOR ANALYTICS

2.1. Призначення та основні функції рішення IBM QRadar SIEM

IBM QRadar SIEM (Security Information and Event Management) є передовою платформою для централізованого моніторингу, аналізу та управління подіями безпеки в інформаційних системах організацій. Основна мета цієї системи — виявлення загроз, кореляція подій, автоматизація реагування на інциденти та забезпечення відповідності нормативним вимогам. QRadar SIEM забезпечує глибокий рівень інтелектуальної аналітики, інтегруючи дані з різних джерел для створення єдиного центру кібербезпеки.

IBM QRadar SIEM використовує кілька рівнів ШІ та автоматизації для поліпшення збагачення сповіщень, пріоритизації загроз і кореляції інцидентів, представляючи пов'язані сповіщення в єдиній панелі моніторингу, знижуючи шум і заощаджуючи час. QRadar SIEM допомагає максимізувати продуктивність вашої команди безпеки, надаючи уніфікований досвід для всіх інструментів SOC з інтегрованими, передовими можливостями ШІ та автоматизації. [11]

Нещодавно компанія Forrester Consulting за замовленням IBM провела дослідження Total Economic Impact™ (TEI) IBM Security QRadar SIEM, щоб вивчити потенційну окупність інвестицій (ROI), яку підприємства можуть отримати, впровадивши це рішення. Щоб краще зрозуміти переваги, витрати та ризики, пов'язані з цими інвестиціями, Forrester опитала чотирьох представників, які мають досвід використання QRadar SIEM, і об'єднала результати, щоб сформувати єдину складову організацію.

Деякі ключові кількісні переваги, зазначені в дослідженні на основі трирічної приведеної вартості з поправкою на ризик, зображені на рисунку 2.1:

рентабельність інвестицій (ROI) 239% і окупність <6 місяців;

чиста приведена вартість (NPV) становить 4,31 млн доларів США;

економія часу понад 90% для аналітиків, які розслідують інцидент.

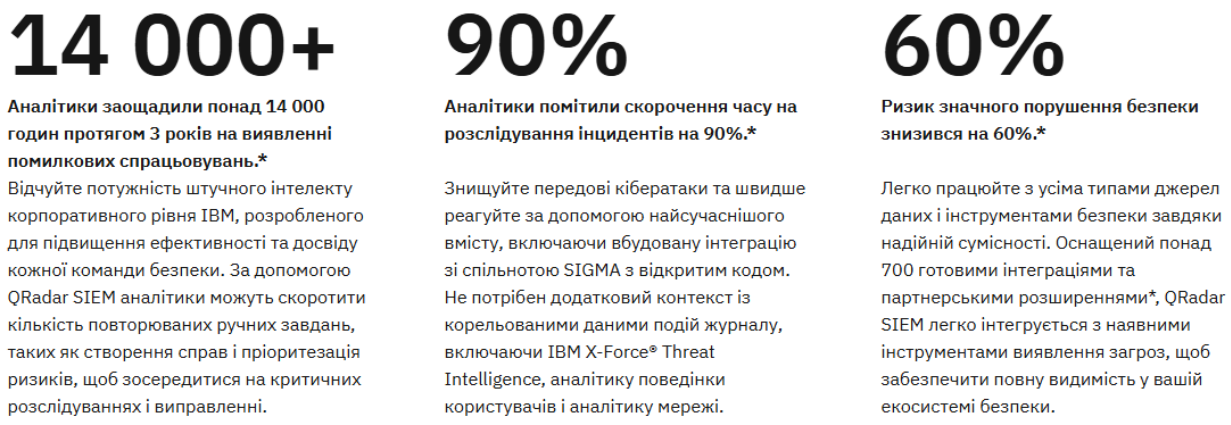

Рис. 2.1 TEI QRadar SIEM [11]

Рішення IBM QRadar SIEM виконує низку основних функцій, серед яких пріоритезація оповіщень на основі ризиків, sigma-правила, федеративний пошук, аналіз поведінки користувачів, аналітика мережевих загроз.

Пріоритезація оповіщень на основі ризиків: IBM QRadar застосовує вдосконалений підхід до управління оповіщеннями завдяки інтеграції механізмів штучного інтелекту корпоративного рівня. Система автоматично оцінює ризик кожного інциденту за допомогою багаторівневої шкали, що враховує контекст і потенційний вплив на організацію. Це дозволяє знизити навантаження на аналітиків, виділяючи для них лише ті інциденти, які мають критичне значення. У результаті підвищується ефективність реагування на загрози, оскільки фахівці з безпеки можуть концентрувати зусилля на високопріоритетних інцидентах.

Такий підхід мінімізує проблему «втоми від сповіщень», коли аналітики змушені працювати з великою кількістю нерелевантних або низькопріоритетних сигналів. У практичному аспекті це означає, що час на реагування скорочується, а якість аналізу суттєво зростає, забезпечуючи більш швидке й точне усунення загроз.

Sigma-правила: IBM QRadar підтримує інтеграцію з Sigma-правилами - універсальним форматом опису шаблонів загроз для SIEM-систем. Завдяки цьому аналітики отримують можливість швидко впроваджувати нові правила, розроблені

та перевірені глобальною спільнотою спеціалістів з інформаційної безпеки. Sigma-правила є відкритим стандартом, який забезпечує оперативну адаптацію до нових загроз шляхом імпорту специфічних інструкцій для виявлення аномалій.

Це сприяє створенню динамічного середовища безпеки, де організації можуть оперативно реагувати на нові типи атак, не витрачаючи значний час на розробку власних правил. Використання краудсорсингових напрацювань гарантує, що система буде відповідати сучасним вимогам безпеки, зберігаючи свою адаптивність до нових викликів.

Федеративний (глобальний) пошук: QRadar пропонує унікальну функцію федеративного пошуку, яка дозволяє об'єднувати розрізнені джерела даних, не вимагаючи їх централізованого зберігання. Це забезпечує гнучкість у виборі критично важливих даних, які необхідно інтегрувати в систему, та дозволяє знижувати витрати на обробку великих обсягів інформації.

Цей підхід особливо ефективний для організацій із розподіленою інфраструктурою, таких як мультинаціональні корпорації, які часто мають дані, розподілені між різними географічними локаціями чи платформами. Глобальний пошук значно підвищує точність розслідувань, дозволяючи аналізувати дані в їхньому початковому контексті. Це, у свою чергу, знижує ризик пропуску критичних інцидентів, які можуть залишитися непоміченими в ізольованих системах.

Аналіз поведінки користувачів: однією з ключових функцій QRadar є вбудований User Behavior Analytics, який дозволяє виявляти аномальні дії користувачів, що можуть свідчити про інсайдерські загрози. Ця функція використовує алгоритми машинного навчання для створення поведінкових профілів кожного користувача, визначаючи типову активність і виявляючи відхилення.

User Behavior Analytics допомагає не лише у виявленні потенційних інсайдерських загроз, але й у прогнозуванні ризикових сценаріїв. Наприклад, система може ідентифікувати співробітників, які виявляють підвищену активність, що нетипова для їхніх ролей, і повідомляти про це адміністраторам безпеки. Таким

чином, UBA забезпечує більш глибоке розуміння поведінки користувачів і допомагає у створенні превентивних заходів.

Аналітика мережевих загроз: функціонал IBM QRadar Network Detection and Response (NDR) спрямований на аналіз мережевої активності в режимі реального часу. Ця функція об’єднує дані про трафік із різних джерел, забезпечуючи розширений огляд усієї мережевої інфраструктури.

QRadar NDR використовує аналітичні алгоритми для виявлення складних мережевих атак, таких як APT (Advanced Persistent Threats) чи розподілені атаки на відмову в обслуговуванні (DDoS). Система також дозволяє ідентифікувати витік даних через нетипові маршрути мережевого трафіку.

Перевага цієї функції полягає у здатності забезпечувати проактивний захист, що дозволяє запобігати атакам до того, як вони можуть завдати шкоди. Глибока інтеграція із загальною аналітичною платформою QRadar дозволяє отримати повний контекст інцидентів, включаючи поведінку користувачів та кінцевих точок.

Ці функціональні можливості IBM QRadar роблять його потужним інструментом для забезпечення кібербезпеки, особливо в контексті виявлення та реагування на внутрішні загрози. Система поєднує передові технології аналізу, інтеграції та автоматизації, що дозволяє організаціям ефективно захищати свої інформаційні ресурси.

2.2. Архітектура рішення IBM QRadar SIEM

Треба підкреслити, що IBM QRadar SIEM - це модульна архітектура, яка забезпечує видимість вашої IT-інфраструктури в режимі реального часу, яку ви можете використовувати для виявлення загроз і визначення пріоритетів. Ви можете масштабувати QRadar, щоб задовольнити ваші потреби у зборі та аналізі журналів і потоків. Ви можете додати інтегровані модулі до вашої платформи QRadar, такі як QRadar Risk Manager, QRadar Vulnerability Manager і QRadar Incident Forensics.

Робота платформи аналітики безпеки QRadar складається з трьох рівнів і застосовується до будь-якої структури розгортання QRadar, незалежно від її

розміру і складності. На рисунку 2.2 показано три рівня, які складають архітектуру QRadar [12].

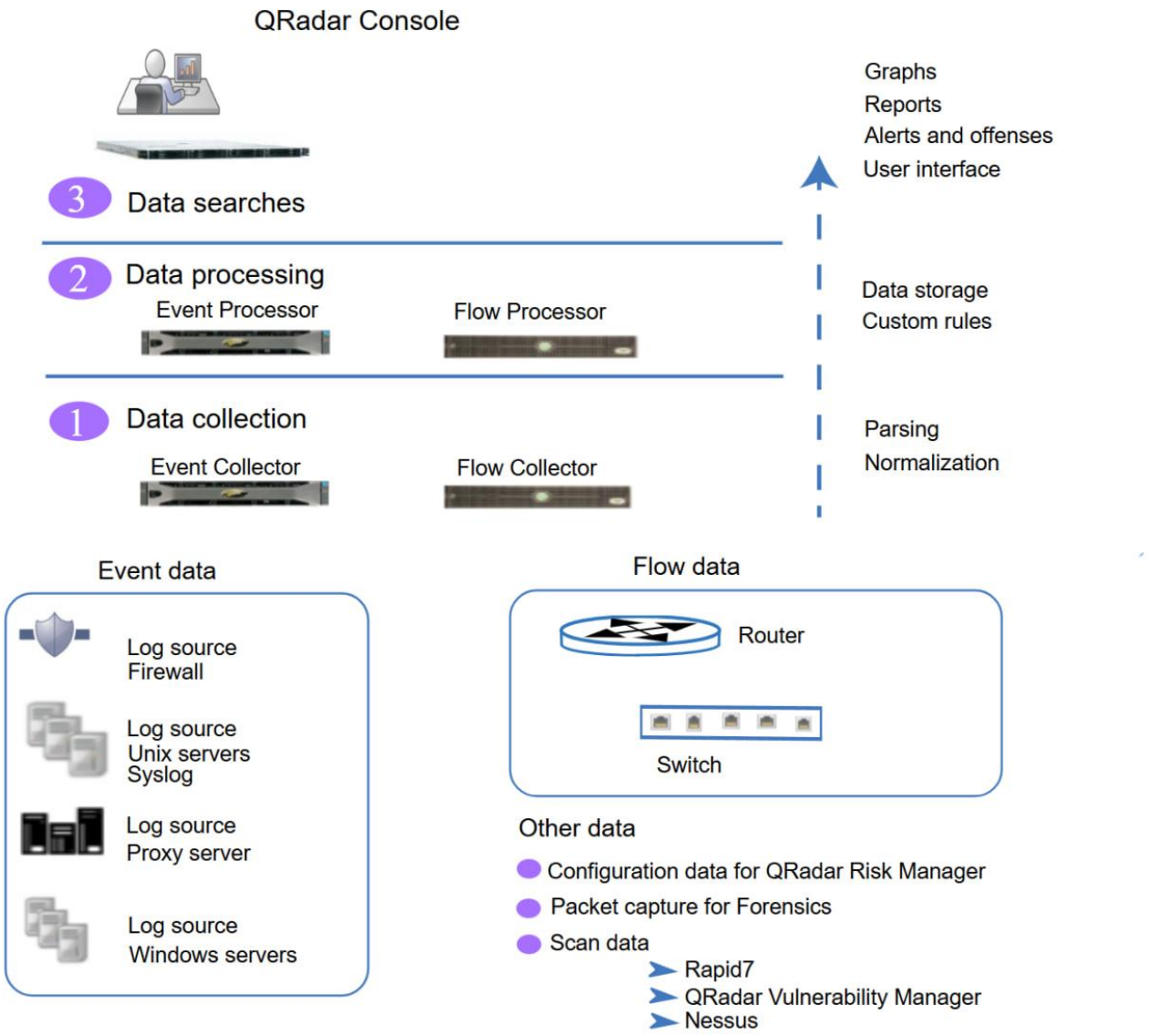

Рис. 2.2. Архітектура QRadar SIEM [12]

Збір даних - це перший рівень, на якому з вашої мережі збираються такі дані, як події або потоки. Для збору даних безпосередньо з вашої мережі можна використовувати пристрій «Все в одному», або ви можете використовувати колектори, такі як QRadar Event Collector або QRadar Flow Collector, для збору даних про події або потоки. Дані аналізуються і нормалізуються перед тим, як вони потрапляють на рівень обробки. Коли необроблені дані аналізуються, вони нормалізуються, щоб представити їх у структурованому та зручному для використання форматі.

Основна функціональність QRadar SIEM зосереджена на зборі даних про події та збір потоків.

Дані про події - це події, які відбуваються в певний момент часу в середовищі користувача, такі як входи в систему, електронна пошта, VPN-з'єднання, заборони брандмауера, проксі-з'єднання і будь-які інші події, які ви хочете зареєструвати в журналах вашого пристрою.

Дані потоку - це інформація про мережеву активність або інформація про сеанс між двома хостами в мережі, яку QRadar перетворює в записи потоку. QRadar перетворює або нормалізує необроблені дані в IP-адреси, порти, кількість байт і пакетів та іншу інформацію в записи потоку, які фактично представляють сеанс між двома хостами. На додаток до збору інформації про потік за допомогою колектора потоку, повне захоплення пакетів доступне за допомогою компонента QRadar Incident Forensics.

Обробка даних - після збору даних, на другому рівні, або рівні обробки даних, дані про події та потоки даних проходять через механізм користувацьких правил (CRE), який генерує правопорушення та оповіщення, а потім дані записуються до сховища.

Дані про події та потокові дані можуть оброблятися пристроєм «Все в одному» без необхідності додавання процесорів подій або процесорів потоків. Якщо пропускна здатність пристрою «Все в одному» перевищена, вам може знадобитися додати процесори подій, потокові процесори або будь-який інший пристрій для обробки додаткових вимог. Вам також може знадобитися більше місця для зберігання даних, що можна вирішити, додавши вузли даних.

Інші функції, такі як QRadar Risk Manager, QRadar Vulnerability Manager або QRadar Incident Forensics, збирають різні типи даних і надають більше функцій.
QRadar Risk Manager збирає конфігурацію мережевої інфраструктури і надає карту топології вашої мережі. Ви можете використовувати ці дані для управління ризиками, моделюючи різні мережеві сценарії шляхом зміни конфігурацій і впровадження правил у вашій мережі.

Використовуйте QRadar Vulnerability Manager для сканування вашої мережі

та обробки даних про вразливості або для управління даними про вразливості, зібраними за допомогою інших сканерів, таких як Nessus і Rapid7. Зібрані дані про вразливості використовуються для виявлення різних ризиків безпеки у вашій мережі.

Використовуйте QRadar Incident Forensics для проведення поглиблених криміналістичних розслідувань і відтворення повних мережевих сесій.

3. На верхньому рівні, дані, які збираються і обробляються QRadar, доступні користувачам для пошуку, аналізу, звітності та оповіщення або розслідування правопорушень. Користувачі можуть здійснювати пошук і керувати завданнями адміністрування безпеки для своєї мережі з користувацького інтерфейсу на консолі QRadar Console.

У системі «Все в одному» всі дані збираються, обробляються і зберігаються на пристрої «Все в одному».

У розподілених середовищах консоль QRadar не виконує обробку подій і потоків або зберігання. Замість цього, консоль QRadar Console використовується в першу чергу як користувальницький інтерфейс, де користувачі можуть використовувати її для пошуку, звітів, сповіщень і розслідувань.

2.3. Призначення та основні функції рішення QRadar User Behavior Analytics

QRadar UBA є високоспеціалізованим рішенням, створеним для здійснення детального аналізу поведінкових моделей користувачів з метою підвищення рівня безпеки інформаційних систем організацій. Це програмне забезпечення інтегрується з платформою IBM QRadar SIEM, що дозволяє поєднувати традиційні підходи до кореляції подій із передовими методами поведінкової аналітики.

Основною метою QRadar UBA є виявлення аномальної активності користувачів, яка може свідчити про потенційні внутрішні загрози, такі як інсайдерські атаки, компрометація облікових записів або навмисні чи випадкові зловмисні дії співробітників. Інструмент використовує методи машинного

навчання та статистичного аналізу для визначення відхилень від нормальної поведінки, формування поведінкових профілів і оперативного ідентифікування ризиків [13].

Завдяки здатності автоматично аналізувати значний обсяг даних у реальному часі, QRadar UBA сприяє зниженню часу на виявлення та нейтралізацію загроз, що є критично важливим у сучасному кібербезпековому середовищі. Це рішення також забезпечує створення прозорої аудиторської траси для подальшого розслідування інцидентів і формування звітності, відповідної до нормативних вимог. Популярність QRadar UBA можна побачити на рисунку 2.3.

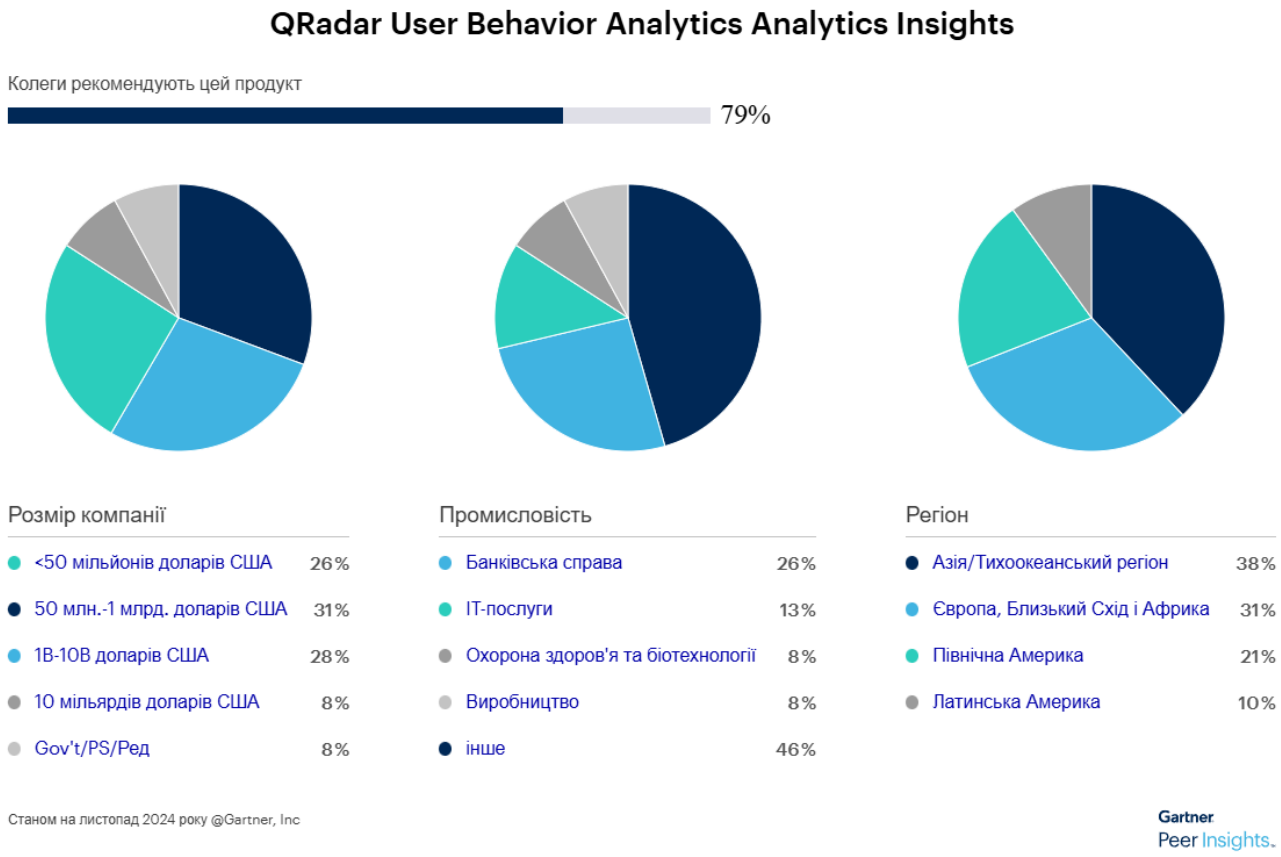

Рис. 2.3. Статистика використання QRadar User Behavior Analytics від Gartner [14]

Можна відмітити наступні призначення QRadar User Behavior Analytics, такі як: забезпечення глибокої видимості користувацької активності, створення поведінкових профілів користувачів, виявлення аномальної активності, ідентифікація внутрішніх загроз, протидія компрометації облікових записів,

пріоритезація ризиків, автоматизація та спрощення роботи аналітиків, забезпечення відповідності нормативним вимогам. Розглянемо кожний з описаних пунктів.

Забезпечення глибокої видимості користувацької активності: QRadar UBA збирає та аналізує дані про всі дії користувачів у системі, зокрема входи в систему, спроби доступу до файлів, переміщення великих обсягів даних і взаємодію з критично важливими системами. Це забезпечує аналітикам повну картину активності в інформаційній системі організації.

Створення поведінкових профілів користувачів: Рішення використовує алгоритми машинного навчання для побудови індивідуальних поведінкових профілів на основі типових дій кожного користувача. Ці профілі адаптуються з часом, забезпечуючи точність навіть за умов динамічних змін у поведінці співробітників.

Виявлення аномальної активності: Однією з ключових цілей QRadar UBA є виявлення відхилень від звичайної поведінки. Наприклад:

використання облікового запису в незвичних часових рамках;

доступ до конфіденційної інформації без явної потреби;

нестандартні дії під час роботи з корпоративними ресурсами.

Ідентифікація внутрішніх загроз: QRadar UBA допомагає виявляти потенційні внутрішні атаки, які зазвичай важко ідентифікувати за допомогою традиційних інструментів кібербезпеки. Система фокусується на поведінці, що може бути ознакою зловмисних дій, наприклад, спроби масового завантаження конфіденційних даних або пошук у системі файлів, до яких користувач раніше не звертався.

Протидія компрометації облікових записів: завдяки виявленню дій, які не відповідають типовій поведінці користувача, система може швидко сигналізувати про можливу компрометацію облікових даних, наприклад, використання облікового запису з невідомої IP-адреси або доступ із незвичної геолокації.

Пріоритезація ризиків: QRadar UBA оцінює кожну виявлену аномалію на основі ризику та потенційного впливу на організацію. Це дозволяє аналітикам

зосереджуватися на найбільш критичних інцидентах, оптимізуючи використання ресурсів.

Автоматизація та спрощення роботи аналітиків: інструмент автоматично генерує інциденти безпеки на основі поведінкових аномалій, що спрощує роботу аналітиків. Також він інтегрується з платформами управління інцидентами, такими як SOAR, що дозволяє автоматизувати реагування на загрози.

Забезпечення відповідності нормативним вимогам: QRadar UBA сприяє виконанню вимог стандартів безпеки (наприклад, GDPR, HIPAA, ISO 27001), які передбачають постійний моніторинг активності користувачів та забезпечення цілісності інформації.

Розглянемо роль машинного навчання в QRadar User Behavior Analytics.

QRadar UBA активно використовує алгоритми машинного навчання для аналізу поведінкових патернів користувачів та виявлення аномалій, які можуть свідчити про внутрішні загрози. Машинне навчання є центральним компонентом цього рішення, забезпечуючи проактивний підхід до моніторингу активності в інформаційних системах [15].

Створення поведінкових профілів є важливим етапом у забезпеченні інформаційної безпеки за допомогою систем аналізу користувацької активності, таких як QRadar UBA. Завдяки застосуванню методів машинного навчання, система здатна автоматично формувати детальні поведінкові профілі користувачів, ґрунтуючись на аналізі історичних даних:

аналіз звичайної поведінки: ML-моделі вивчають типові дії кожного користувача, такі як час і частота входу в систему, доступ до певних файлів, використання додатків, IP-адреси та геолокації;

індивідуальні та групові профілі: система створює профілі як для окремих користувачів, так і для груп з подібними функціональними обов'язками, що підвищує точність аналізу.

Ці профілі є базою для подальшого виявлення аномалій.

Виявлення аномалій є одним із ключових завдань у забезпеченні кібербезпеки, що реалізується за допомогою QRadar UBA. Завдяки використанню

сучасних алгоритмів машинного навчання система здатна ідентифікувати відхилення від стандартних шаблонів поведінки користувачів, що можуть вказувати на потенційні ризики:

динамічні пороги: ML дозволяє адаптувати пороги для аномалій залежно від контексту, наприклад, звичайного робочого графіка або змін у мережевій інфраструктурі;

контекстуальний аналіз: алгоритми враховують контекст подій, наприклад, час, місце, обсяг і характер операцій, для оцінки їх ризиків.

Машинне навчання є ключовою технологією, що дозволяє QRadar UBA ефективно розрізняти легітимну активність користувачів і дії, які можуть свідчити про потенційні загрози, такі як компрометація облікових записів або зловмисна активність співробітників. Алгоритми аналізують поведінкові патерни, виявляючи найменші відхилення від встановлених норм, що може свідчити про ризики для інформаційної безпеки:

раннє виявлення інсайдерів: система може ідентифікувати поведінку, яка характерна для інсайдерів, наприклад, поступове накопичення доступу до чутливих даних або спроби змінити конфігурації систем;

компрометація облікових записів: ML допомагає виявляти дії, які можуть бути результатом використання вкрадених або скомпрометованих облікових записів.

QRadar UBA застосовує методи машинного навчання для автоматизованої оцінки ризиків, що дозволяє визначати рівень загрози для кожного інциденту з високою точністю. Система аналізує виявлені аномалії у контексті поведінкового профілю користувача, типу активності, її масштабу та інших ключових факторів, що можуть свідчити про загрозу безпеці:

інтеграція з ризиковими моделями: ML-моделі оцінюють ймовірність того, що аномальна активність є загрозою;

пріоритезація сповіщень: завдяки ML, система забезпечує аналітиків безпеки тільки релевантними сповіщеннями, що дозволяє зосередити увагу на найкритичніших загрозах.

Однією з ключових переваг застосування машинного навчання у системах кібербезпеки, є здатність до безперервного вдосконалення та адаптації до динамічних умов загроз. Система аналізує нові дані, постійно оновлюючи поведінкові моделі та алгоритми виявлення аномалій, що забезпечує актуальність її роботи навіть у швидко змінюваних середовищах.

Цей механізм дозволяє системі ефективно протидіяти як відомим, так і раніше невідомим типам атак, включаючи складні багатоступеневі загрози, які еволюціонують разом із розвитком технологій. У результаті організації отримують надійний інструмент, здатний забезпечити проактивний підхід до забезпечення інформаційної безпеки:

навчання на нових даних: QRadar UBA регулярно оновлює свої моделі, інтегруючи інформацію про нові види загроз або зміни в поведінці користувачів;

виявлення довготривалих загроз: ML може виявляти патерни поведінки, які розтягуються на тривалий період, наприклад, спроби поступового впровадження шкідливих дій.

Машинне навчання виступає фундаментальною технологією для забезпечення інтеграції QRadar UBA із платформами автоматизації, такими як SOAR. Це дозволяє системі не лише ідентифікувати потенційні загрози, але й автоматично ініціювати процеси реагування, що значно скорочує час від виявлення інциденту до його нейтралізації.

Завдяки такій інтеграції забезпечується високий рівень оперативності та ефективності реагування на загрози, а також знижується потреба у ручному втручанні, що оптимізує роботу фахівців з інформаційної безпеки:

автоматичне реагування: ML-моделі можуть ініціювати автоматичні дії, такі як блокування доступу або ізоляція облікового запису, без участі людини;

інтелектуальне рішення конфліктів: алгоритми здатні розрізняти справжні загрози від помилкових сповіщень, що зменшує кількість хибних тривог.

Ось всі моделі моделі машинного навчання які використовуються в QRadar User Behavior Analytics: індивідуальні (числові) моделі користувачів, індивідуальні (спостережувані) моделі користувачів та моделі груп рівних.

Індивідуальні (числові) моделі користувача обчислюють конкретне числове значення для користувача за останні 10 днів [15]. Коли користувач відхиляється за межі прогнозованого діапазону, модель машинного навчання з високим рівнем достовірності визначає, що подія є аномальною. Їх назви та опис дії описано в таблиці 2.1.

Таблиця 2.1

Індивідуальні (числові) моделі

Назва моделі	Опис моделі
Access activity	Модель Access activity відстежує активність користувача у високорівневій категорії доступу і створює вивчену модель поведінки для кожної години дня.
Aggregated Activity	Модель Aggregated Activity відстежує загальну активність користувача за часом і створює модель для прогнозованої тижневої поведінки.
Authentication Activity	Модель Authentication Activity відстежує активність користувача в високорівневій категорії автентифікації і створює вивчену модель поведінки для кожної години дня.
Data Downloaded	Модель Data Downloaded відстежує дані, які завантажуються для кожного користувача, а потім сповіщає про аномальну поведінку.
Data Uploaded to Remote Networks	Модель Data Uploaded to Remote Networks відстежує використання даних зовнішнього домену для кожного користувача і попереджає про ненормальну поведінку.
DDL events	Модель подій DDL (Data Definition Language) Events відстежує DDL-події користувача в часі і створює модель для прогнозованого тижневого результату.
DML events	Модель подій DML (мова маніпулювання даними) відстежує події DML користувача в часі і створює модель для прогнозованого тижневого результату.
HTTP Data Transfer Activity	Модель активності передачі даних HTTP відстежує події передачі даних HTTP користувача в часі і створює модель для прогнозованої тижневої оцінки.
Outbound Transfer Attempts	Модель машинного навчання Outbound Transfer Attempts відстежує використання вихідного трафіку для кожного користувача і попереджає про аномальну поведінку.
Risk Posture	Модель Risk Posture відстежує ризиковану активність користувача за частотою генерування сенсорних подій і створює базову модель.
Successful Access and Authentication Activity	Модель Successful Access and Authentication Activity відстежує події успішної автентифікації та доступу користувача за часом і створює модель прогнозованої тижневої поведінки.
Suspicious Activity	Модель Suspicious Activity відстежує активність користувача у високорівневій категорії «Підозріла активність» і створює вивчену модель поведінки для кожної години дня.

Моделі індивідуальних (спостережуваних) користувачів обчислюють набір атрибутів і відповідну їм кількість подій для користувача за останні 10 днів [15]. Коли користувач відхиляється за межі прогнозованого діапазону або використовує нове значення, модель ML з високим рівнем достовірності визначає, що подія є аномальною. Їх назви та опис дії описано в таблиці 2.2.

Таблиця 2.2

Індивідуальні (спостережувані) моделі

Назва моделі	Опис моделі
Lateral Movement: Internal Asset Usage	Модель «Бічний рух: внутрішнє використання активів» відстежує активність користувача у внутрішньому порту призначення за часом і створює модель для прогнозованої тижневої поведінки.
Lateral Movement: Internal Destination Port Activity	Модель «Бічний рух: внутрішня активність у порту призначення» відстежує активність користувача у внутрішньому порту призначення за часом і створює модель для прогнозованої тижневої поведінки.
Lateral Movement: Network Zone Activity	Модель Lateral Movement: Активність мережевої зони визначає, чи мережева зона користувача суттєво відрізняється від визначеної ним групи.
Process Usage	Модель «Process Usage» відстежує активність користувача у використанні процесів у часі та створює модель для прогнозування щотижневих моделей поведінки.

Моделі груп однолітків обчислюють набір атрибутів з відповідним числовим значенням кількості подій для користувача за останні 30 днів [15]. Модель ML з високим рівнем достовірності визначає, що користувач відхилився від групи. Їх назви та опис дії описано в таблиці 2.3.

Таблиця 2.3

Моделі груп рівних

Назва моделі	Опис моделі
Activity Distribution	Модель розподілу активності вивчає кластери поведінки на основі визначення групи LDAP і шукає відхилення від нормального розподілу цих кластерів у часі.
Defined Peer Group	Модель Defined Peer Group показує, наскільки активність подій користувача відхиляється від активності подій визначеної групи однорангових користувачів.

Продовження таблиці 2.3

Internal Asset Access by Peer Group	Модель Internal Asset Access by Peer Group визначає, чи суттєво відрізняється внутрішній доступ користувача до ресурсів від визначеної ним групи.
Internal Destination Ports by Peer Group	Модель Internal Destination Ports by Peer Group визначає, чи доступ користувача до внутрішніх портів призначення суттєво відрізняється від визначеної ним групи. Якщо доступ користувача вважається підозрілим, генерується Сенсорна подія, яка збільшує оцінку ризику користувача.
Learned Peer Group	Модель Learned Peer Group ідентифікує користувачів, які займаються схожою діяльністю, а потім об'єднує їх у групи однолітків.
Network Zones by Peer Group	Модель Network Zones by Peer Group визначає, чи суттєво мережева зона користувача відрізняється від визначеної ним групи.
Process Execution by Peer Group	Модель «Виконання процесу групою однорангових» визначає, чи використання процесу користувачем суттєво відрізняється від визначеної ним групи.

QRadar UBA є потужним інструментом для аналізу поведінки користувачів, спрямованим на виявлення аномалій, які можуть свідчити про внутрішні загрози. Основні функції QRadar UBA забезпечують широкий спектр можливостей для моніторингу, аналізу та реагування на загрози, пов’язані з діяльністю користувачів в інформаційних системах організацій [16].

Основними функціями QRadar UBA можна назвати: аналіз поведінки користувачів, оцінка ризику і пріоритезація загроз, ідентифікація компрометації облікових записів, генерація поведінкових інцидентів та гнучкість в адаптації до специфічних потреб організацій.

Для аналізу поведінки користувачів QRadar UBA здійснює збір даних про дії користувачів з різних джерел, таких як журнали подій, файли аудиту та мережевий трафік. Ці дані використовуються для створення індивідуальних поведінкових профілів:

побудова профілів користувачів: система враховує типові дії кожного користувача, такі як час входу в систему, IP-адреси, геолокації, доступ до ресурсів і тип виконуваних завдань;

виявлення аномалій: будь-яке відхилення від нормальної поведінки автоматично позначається як потенційна загроза. Наприклад, доступ до даних у позаурочний час або спроби обійти обмеження доступу.

Для оцінки ризику і пріоритезації QRadar UBA надає спеціальні функції оцінювання на кожний інцидент:

ризикові коефіцієнти: система оцінює поведінкові аномалії за рівнем ризику, враховуючи, наскільки серйозно вони можуть вплинути на безпеку організації;

пріоритезація інцидентів: аналітики отримують сповіщення лише про найкритичніші випадки, що дозволяє їм зосереджуватися на загрозах, які потребують негайного реагування.

QRadar UBA ефективно виявляє дії, які можуть свідчити про компрометацію облікових даних:

використання сторонніх IP-адрес: система генерує попередження, якщо обліковий запис використовується з невідомих або підозрілих IP-адрес;

аномальні спроби входу: QRadar UBA відстежує багатократні невдалі спроби входу або використання облікових записів у незвичайних умовах.

QRadar UBA автоматично створює інциденти на основі поведінкових аномалій. Основні аспекти цієї функції:

інтеграція з QRadar SIEM: інциденти UBA відображаються в загальній панелі QRadar SIEM для повноцінного аналізу;

деталізація інцидентів: кожен створений інцидент містить детальну інформацію про підозрілу активність, включаючи час, джерело, користувача та тип аномалії.

QRadar UBA дозволяє кастомізувати правила та поведінкові моделі відповідно до особливостей організації:

імпорт правил Sigma: аналітики можуть додавати нові правила з відкритих джерел безпеки, адаптуючи систему до актуальних загроз;

налаштування порогів: організації можуть самостійно встановлювати пороги для генерації інцидентів, враховуючи специфіку роботи.

3 ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ВНУТРІШНЬОЇ ЗАГРОЗИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОРГАНІЗАЦІЇ НА БАЗІ QRADAR USER BEHAVIOR ANALYTICS

3.1. Порядок застосування рішення QRadar User Behavior Analytics

Перш за все QRadar User Behavior Analytics являється модулем до IBM QRadar SIEM. А от же щоб встановити його нам потрібно мати розгорнуту версію SIEM, в мене це QRadar SIEM Community Edition V7.5.0.

QRadar SIEM Community Edition V7.5.0 - це безкоштовна версія платформи IBM QRadar, яка забезпечує потужні функції аналізу подій і управління інформацією безпеки (SIEM). Вона призначена для навчальних, тестових або невеликих комерційних середовищ і дозволяє користувачам досліджувати функціональність QRadar, включаючи виявлення аномалій, аналіз журналів і кореляцію подій.

Особливості:

1. Аналіз і кореляція подій: система здатна обробляти та аналізувати дані журналів, мережеві потоки та виявляти загрози в реальному часі.

2. Можливості розширення: підтримує інтеграцію з широким спектром систем безпеки через спеціальні DSM (Device Support Modules) і Flow Processors.

3. Обмеження: Community Edition має обмеження за обсягом даних (до 50 ГБ на день) і кількістю оброблюваних джерел.

Системні вимоги QRadar Community Edition V7.5.0 Update Package 10:

мінімальні вимоги до пам'яті: 24 ГБ;

мінімальний обсяг дискового простору: 250 ГБ;

процесор: 4 ядра (мінімум) або 6 ядер (рекомендується);

потрібен один мережевий адаптер з доступом до Інтернету;

для забезпечення належного зв'язку та функціональності для QRadar Community Edition потрібні статичні IP-адреси;

призначене ім'я хосту повинно бути повністю кваліфікованим доменним ім'ям;

Розгортання системи SIEM було здійснено на віртуальній машині із застосуванням програмного забезпечення VMware Workstation Pro. Для забезпечення стабільної та ефективної роботи системи було виділено наступні системні ресурси, які можна побачити на рисунку 3.1:

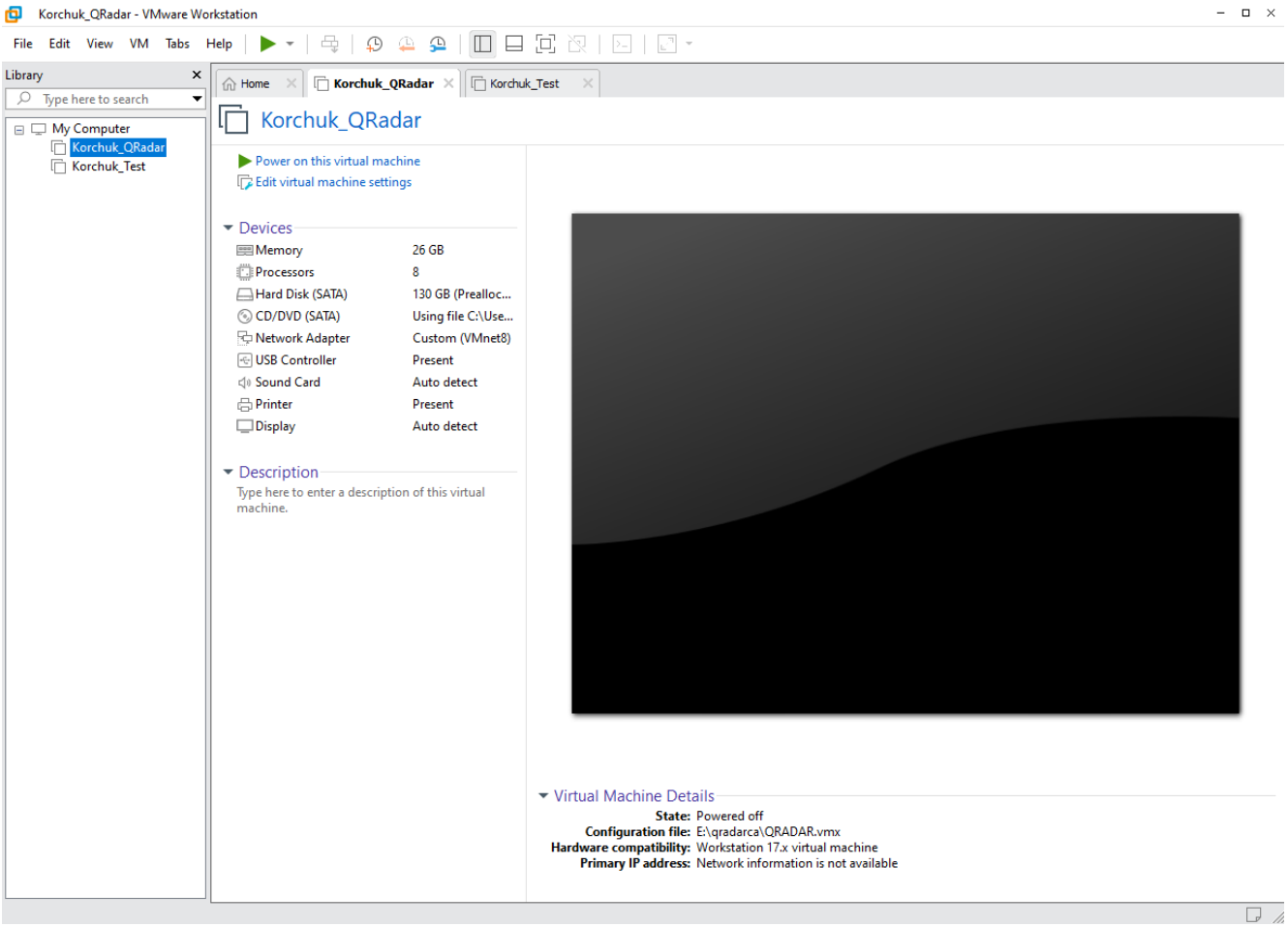

Рис. 3.1. Налаштування QRadar SIEM

Віртуальній машині було надано такі апаратні характеристики, які визначають її продуктивність і можливості виконання операцій у межах заданого середовища:

26 ГБ ОЗУ;

130 ГБ накопичувача;

8 ядер;

доступ до мережі Інтернет.

Після успішної авторизації в системі користувач отримує доступ до інформації, яка відображає дані про обліковий запис, використаний для входу, що зображено на рисунку 3.2. Це забезпечує прозорість і контроль за процесом ідентифікації користувача в межах системи.

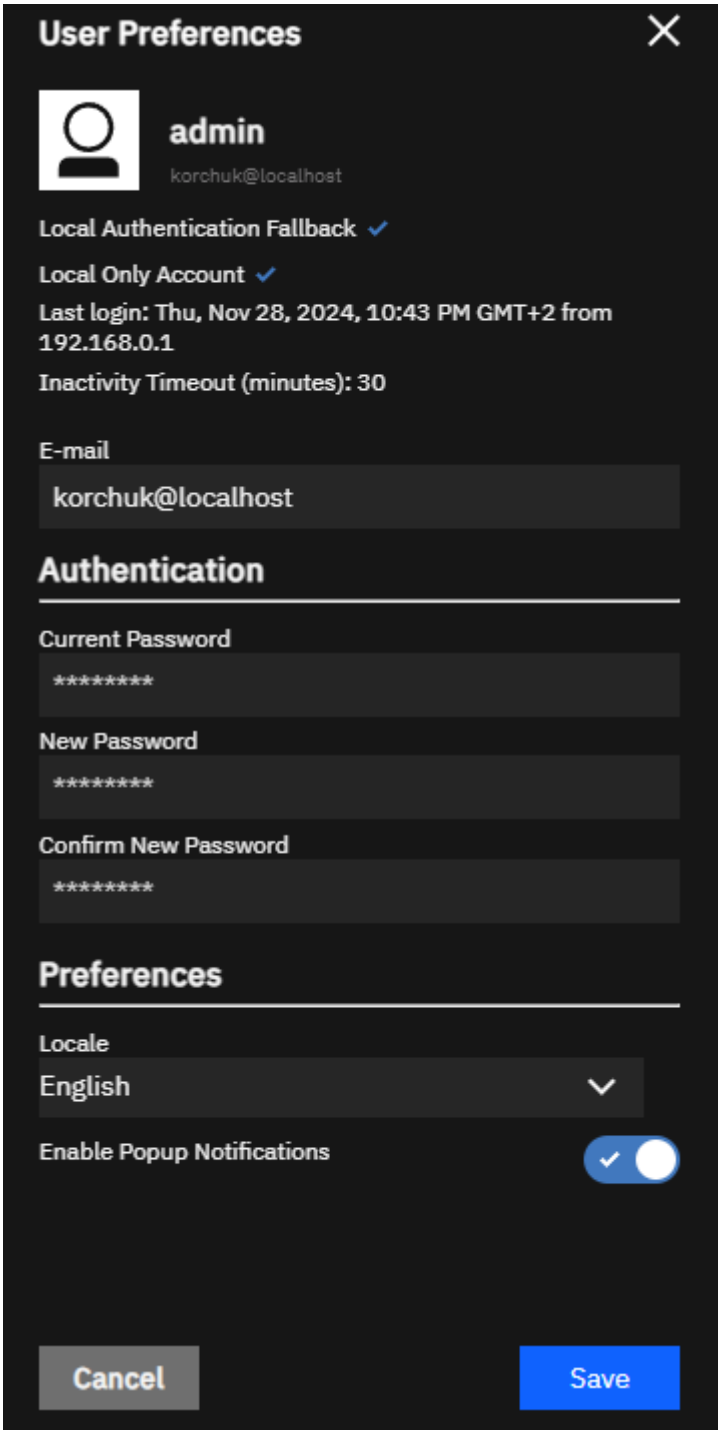

Рис. 3.2. Налаштування користувача

Використовуючи головну панель переходимо до Admin-налаштувань, яка зображена на рисунку 3.3, де за допомогою додатку Extensions Management (Управління розширеннями) додаємо раніше завантажений модуль QRadar UBA:

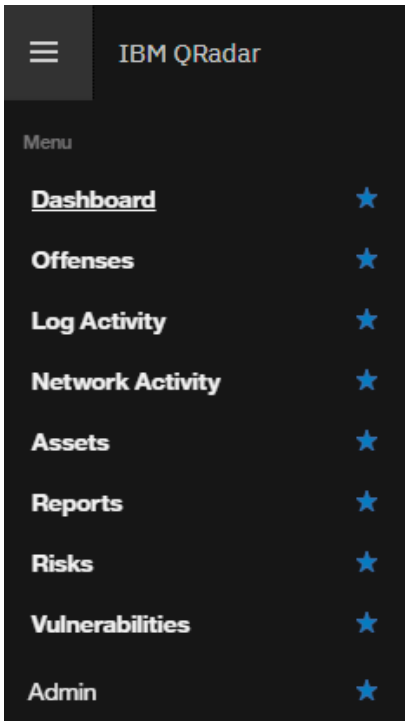

Рис. 3.3. Admin-панель та встановлення модулю UBA

Модуль обирається з системи користувача. Після цього здійснюється його завантаження у відповідне середовище виконання, що забезпечує можливість його подальшого аналізу та інтеграції з іншими компонентами системи, як зображено на рисунку 3.4. Цей процес включає етапи перевірки доступності модуля, автентифікації запиту, а також перевірки сумісності модуля з поточними параметрами обчислювальної системи.

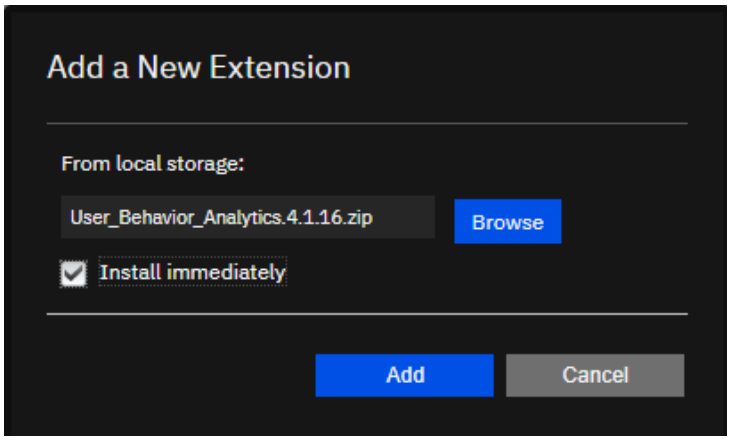

Рис. 3.4. Встановлення модулю UBA

Після декількох хвилин на рисунку 3.5 можна побачити, що наш модуль успішно встановленно:

Рис. 3.5. Показ встановленного модулю

Потім треба створити та додати токен авторизації для User Behavior Analytics, щоб можна було додавати користувачів до системи, що зображено на рисунку 3.6:

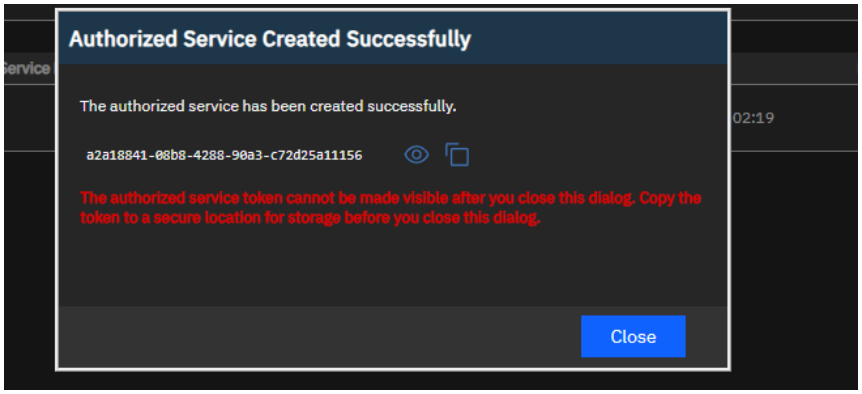

Рис. 3.6. Токен авторизації

У розділі «Правила та налаштування», які зображені на рисунках 3.7 представлено великий перелік, що включає 216 різноманітних правил.

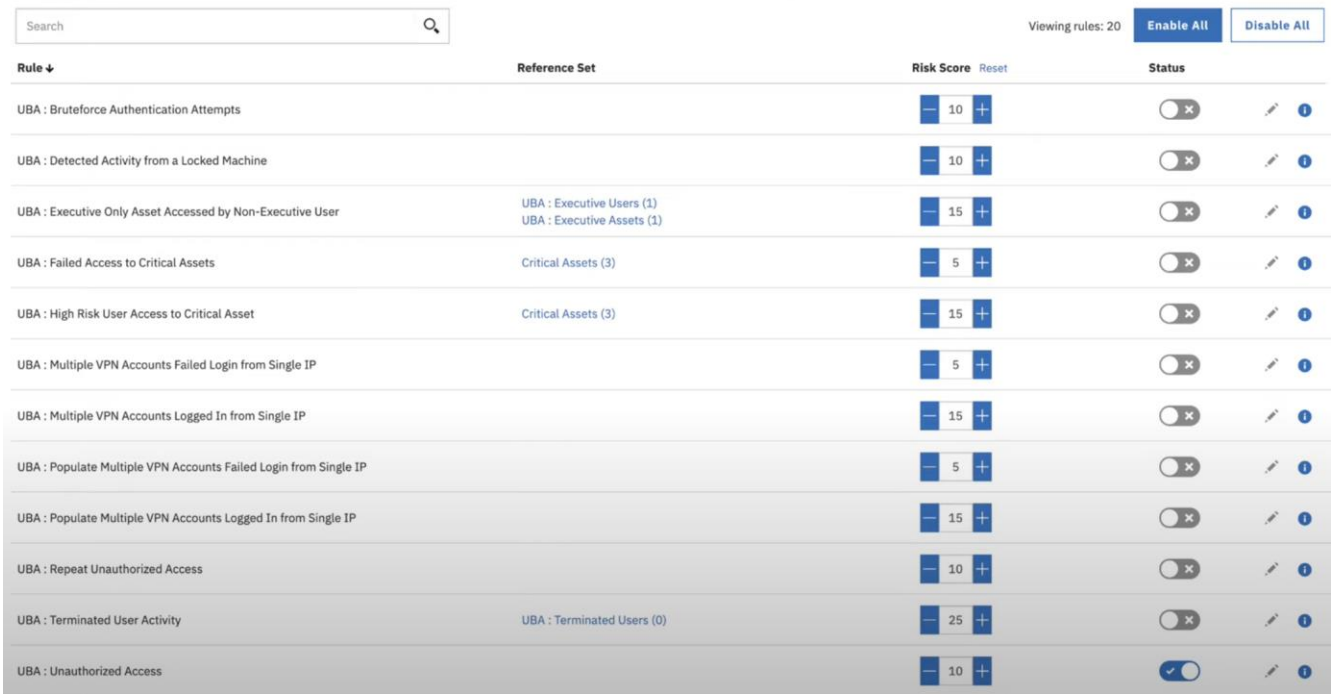

Рис. 3.7. Правила UBA

Для зручності роботи з цим переліком передбачено функціональний механізм фільтрації, який забезпечує легкий і швидкий доступ до необхідних елементів. Такий підхід сприяє оптимізації процесу навігації та підвищуєефективністьуправління налаштуваннями системи.

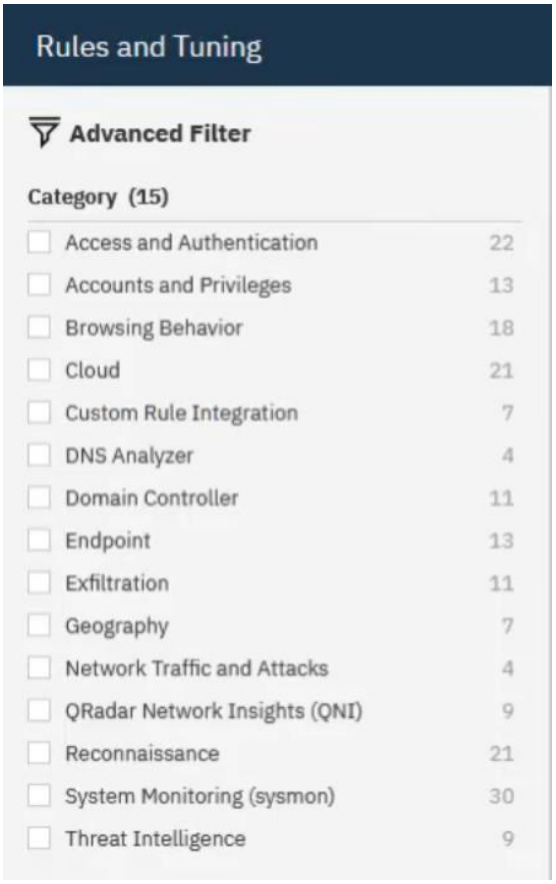

Рис. 3.8. Фільтр пошуку та правила QRadar UBA

Також можна відфільтрувати за ризиком

Рис. 3.9. Оцінка ризику

Кожне правило може бути детально налаштоване відповідно до специфічних вимог організації або чинних нормативно-правових документів. Такий рівень гнучкості дозволяє адаптувати систему до унікальних потреб компанії, забезпечуючи повну відповідність як внутрішнім стандартам, так і зовнішнім регуляторним вимогам, які зображені на рисунку 3.10-11.

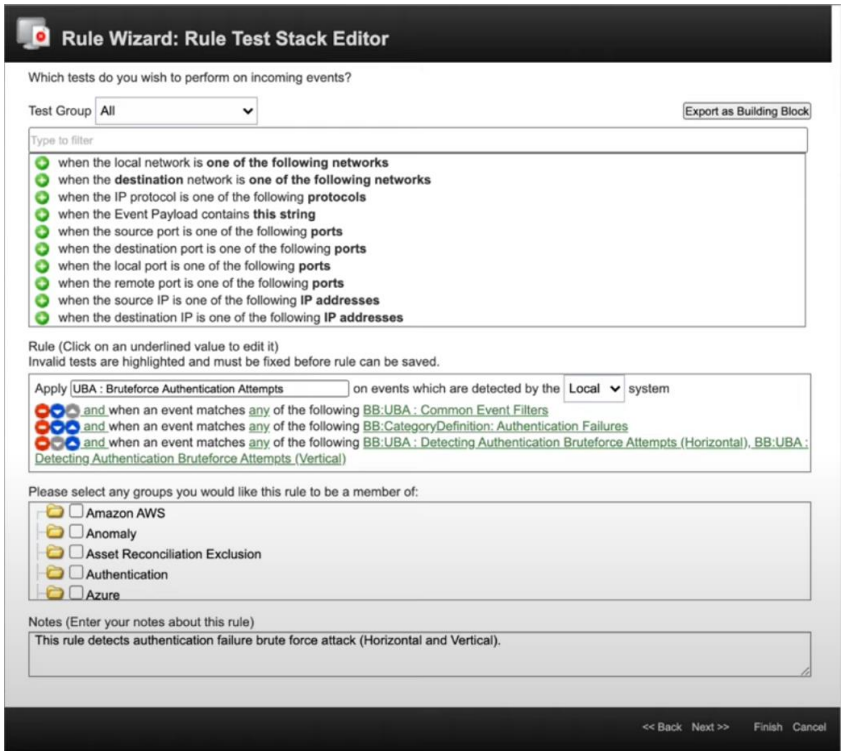

Рис. 3.10. Редактор правил

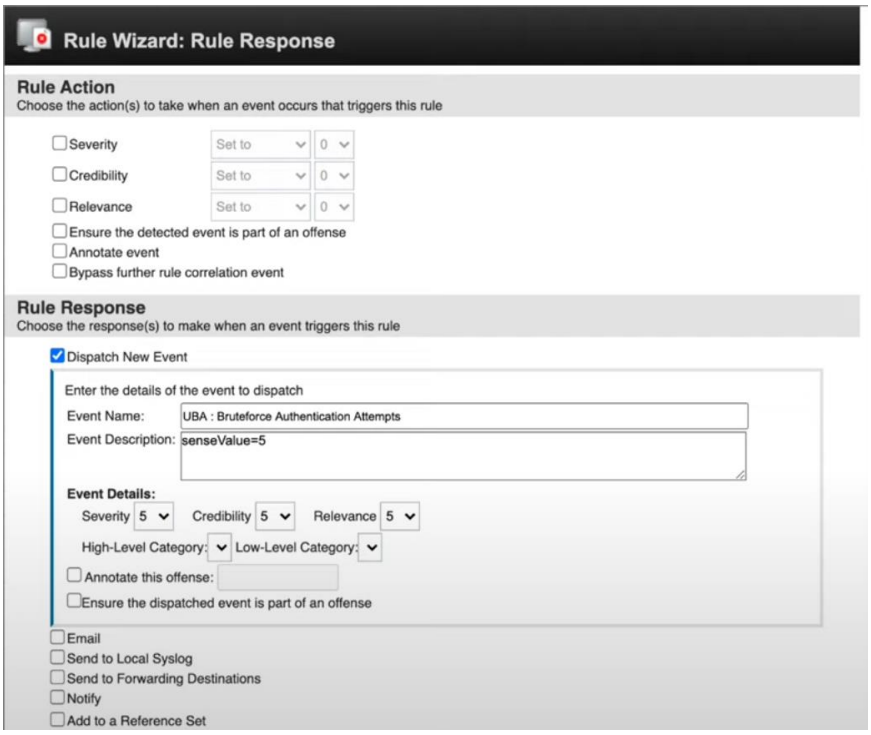

Рис. 3.11. Налаштування відповіді на порушення правила

3.2. Технологія виявлення внутрішньої загрози в інформаційних системах організацій

Для демонстрації функціональних можливостей системи буде створено спеціального тестового користувача з логіном Korchuk Test на операційній системі Windows 10, характеристики системи зображені на рисунку 3.12. Цей обліковий запис умовно імітує поведінку потенційного зловмисника, головна мета якого – отримати доступ до конфіденційних даних та здійснити їх викрадення, водночас залишаючись непоміченим системою моніторингу.

Такий сценарій є надзвичайно важливим для тестування можливостей системи виявлення аномальної активності, оцінки ефективності правил кореляції, а також аналізу дій зловмисників у контексті реальних внутрішніх загроз. Використання подібних тестових сценаріїв дозволяє не лише перевірити працездатність налаштувань безпеки, але й адаптувати систему до можливих нетипових дій, покращуючи її загальну стійкість до внутрішніх ризиків.

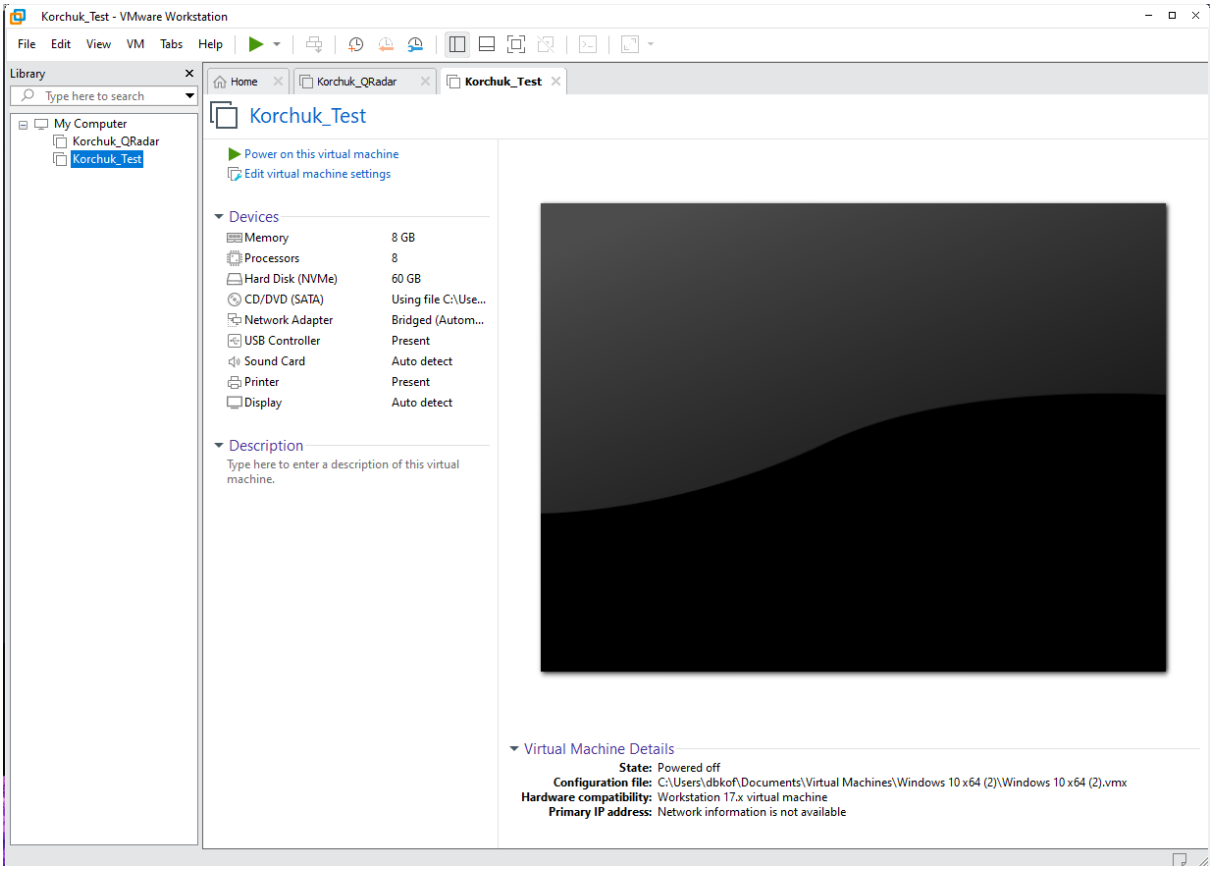

Рис. 3.12. Віртуальна випробувальна машина на базі ОС Windows 10

Запускаємо віртуальну машину, здійснюємо авторизацію за допомогою власного логіна та пароля й розпочинаємо моделювання сценарію, у якому користувач виконує дії, що представляють внутрішню загрозу для організації. У даному випадку метою є завантаження анонімного браузера на робочий комп'ютер, що потенційно може використовуватися для обходу засобів моніторингу та виведення конфіденційної інформації за межі системи.

Для цього, за допомогою штатного браузера Microsoft Edge, виконується пошук програмного забезпечення Tor, яке є популярним інструментом для анонімізації активності в мережі. Процес пошуку, завантаження та підготовки до встановлення браузера Tor детально ілюстровано на рисунках 3.13–3.14.

Цей сценарій дозволяє дослідити, як система реагує на потенційно небезпечну поведінку співробітника, та оцінити ефективність налаштованих політик і правил моніторингу, спрямованих на виявлення подібних загроз.

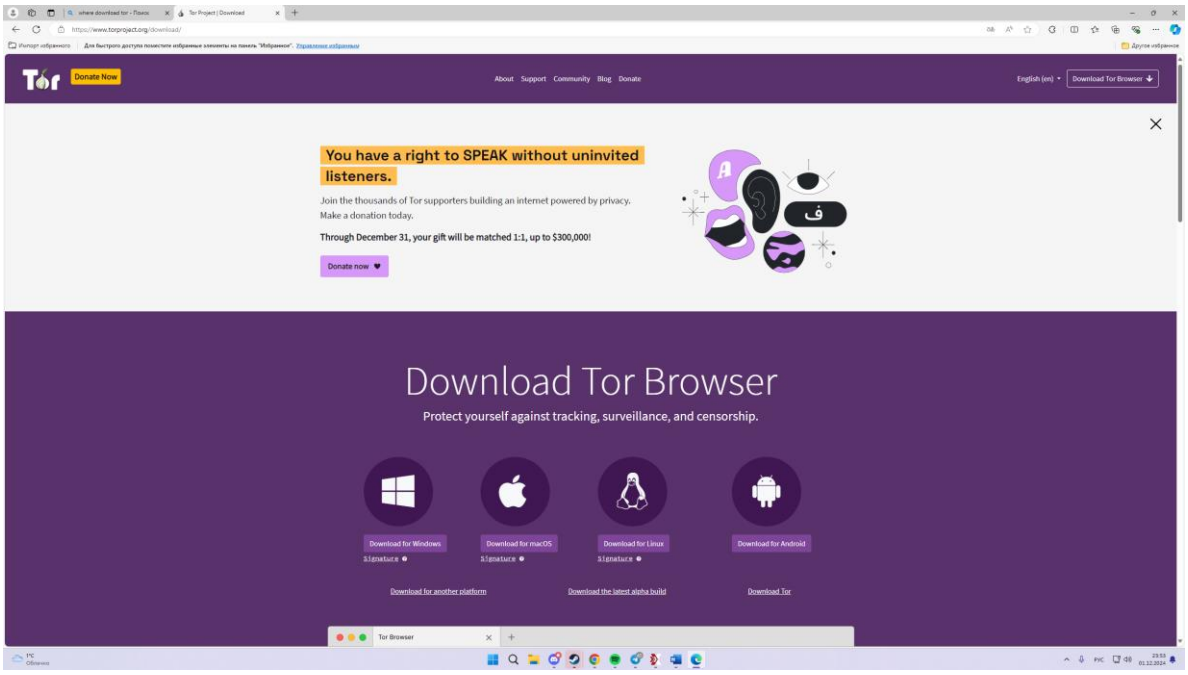

Рис.3.13. Візит потенційно небезпечного веб-сайту

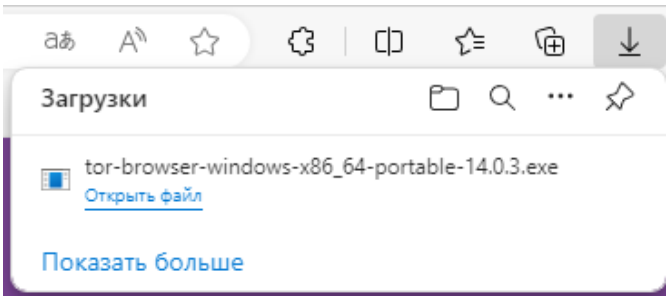

Рис. 3.14. Завантаження потенційно небезпечного ПЗ

На головній панелі модуля User Behavior Analytics, яка продемонстрована на рисунку 3.15, чітко відображається підвищення рівня ризику для користувача з логіном Korchuk Test, що сигналізує про потенційну небезпеку його дій. Цей індикатор є важливим елементом моніторингу, дозволяючи своєчасно ідентифікувати підозрілу активність.

Крім того, у розділі «Нещодавні правопорушення» з'являється відповідне сповіщення, яке вказує на можливе виявлене правопорушення. Це повідомлення надає додаткову інформацію про природу інциденту, допомагаючи аналітикам безпеки швидко проаналізувати ситуацію та вжити необхідних заходів.

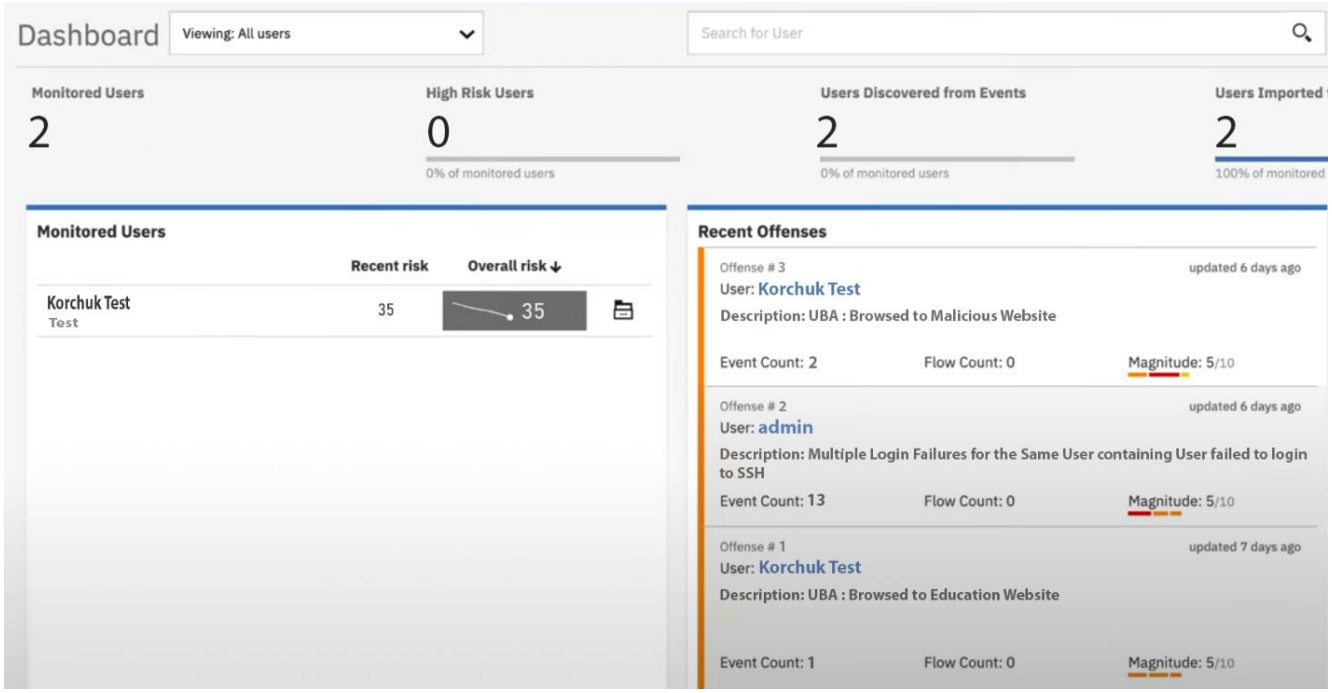

Рис. 3.15. Головна панель User Behavior Analytics

Подібна функціональність дозволяє ефективно реагувати на дії користувачів, які виходять за рамки встановлених норм, і сприяє загальному підвищенню рівня захищеності інформаційної системи.

Детальну інформацію про користувача та зафіксований інцидент можна отримати, перейшовши до його профілю в системі. У профілі, відображеному на рисунку 3.16, представлено ключові дані, що дозволяють провести поглиблений аналіз поведінки користувача, включаючи історію його дій, пов'язані ризики та деталі зафіксованого інциденту.

Ця функція є важливим інструментом для аналітиків інформаційної безпеки, оскільки дозволяє виявляти закономірності, що можуть вказувати на небезпечні тенденції, а також оперативно приймати рішення щодо реагування на потенційні загрози. Наявність такого рівня деталізації сприяє підвищенню загальної ефективності системи моніторингу та протидії внутрішнім загрозам.

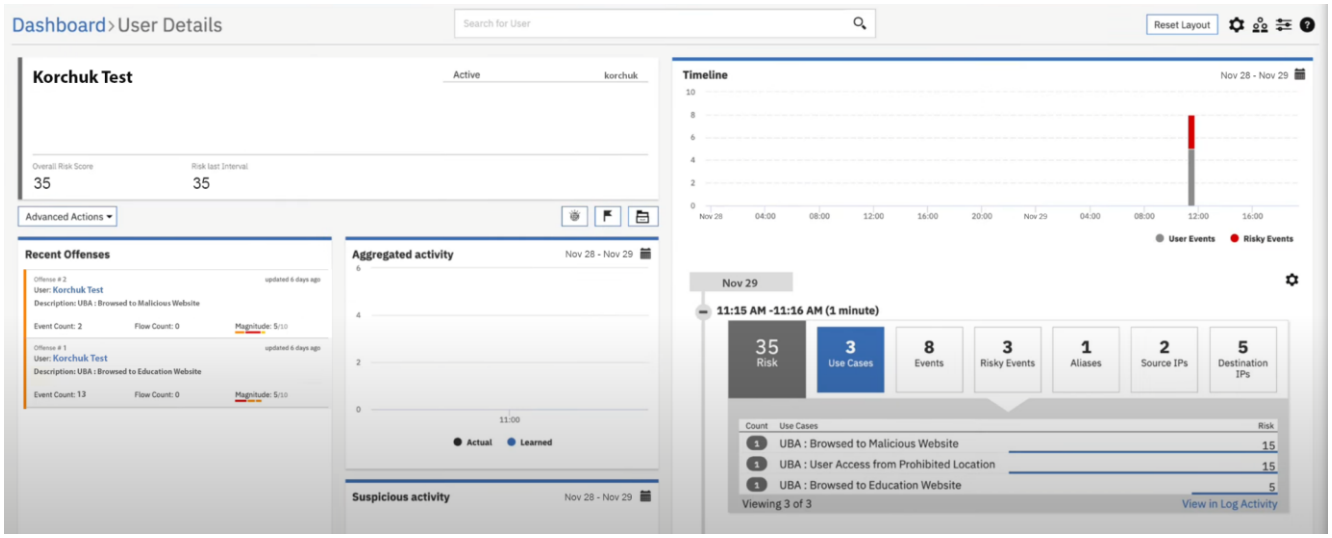

Рис. 3.16. Профіль користувача Korchuk Test

Розглянемо детальніше функціонал модуля «Timeline», зображеного на рисунку 3.17. Цей модуль являє собою часову шкалу, яка відображає два типи подій, пов’язаних із активністю користувача. Дії, що не виходять за межі його поведінкового профілю, позначаються сірим кольором, тоді як червоним виділяються події, які є нетиповими для даного користувача або потенційно свідчать про протиправні наміри.

Під часовою шкалою розташована інтерактивна панель подій, яка надає аналітикам інформаційної безпеки всебічні можливості для глибокого аналізу інцидентів та загроз. Ця панель містить детальну інформацію про ключові показники, серед яких: загальний ризик, асоційований із зафіксованими подіями, специфічні сценарії кореляції, окремі події, а також дії, що класифікуються як ризикові.

Інтерфейс панелі реалізований з урахуванням сучасних принципів гнучкості та адаптивності, що дає змогу спеціалістам налаштовувати її відповідно до

унікальних потреб організації та специфіки робочих процесів. Така модульність забезпечує ефективну інтеграцію з іншими аналітичними інструментами та підвищує продуктивність процесу прийняття рішень в умовах інформаційної безпеки.

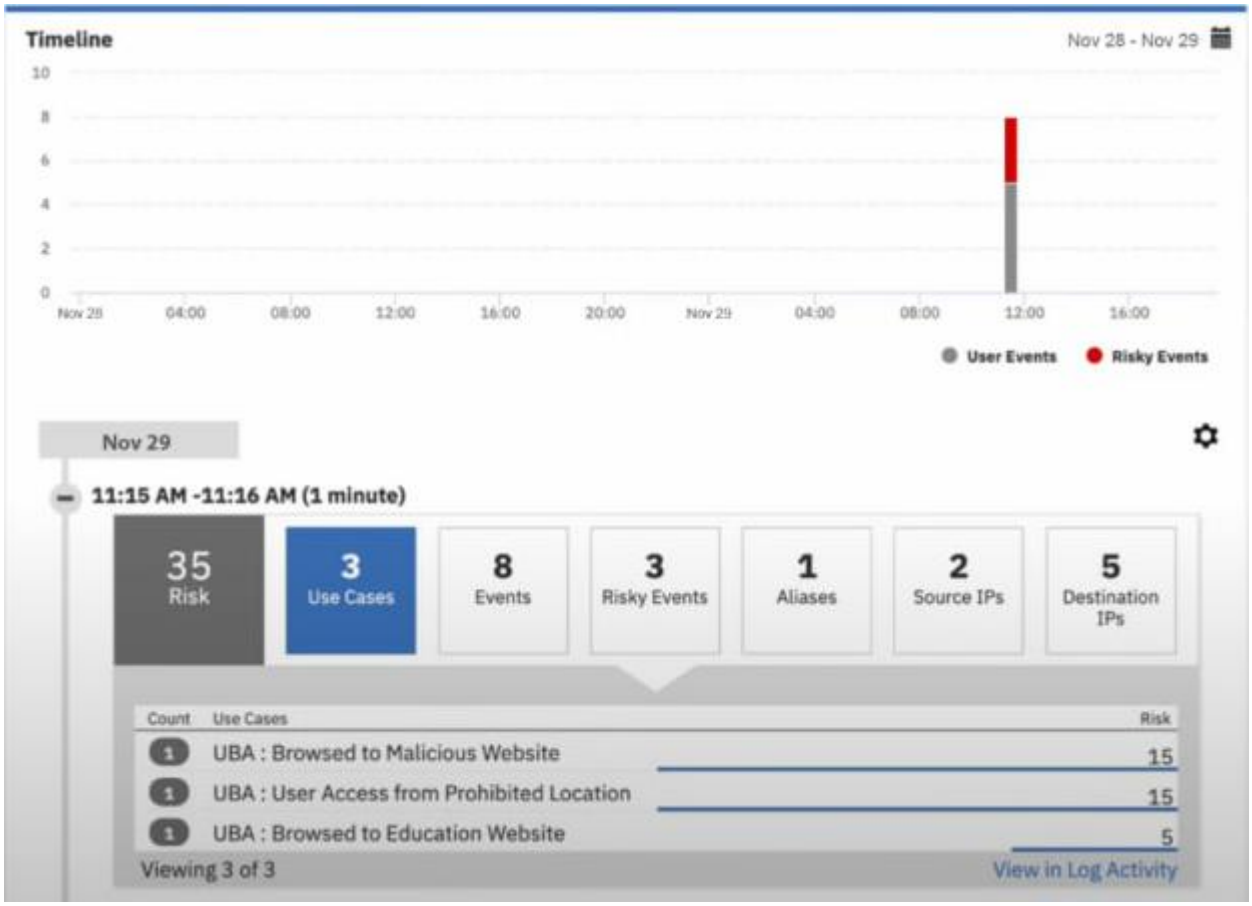

Рис. 3.17. Часова шкала та панель подій користувача

Такий підхід забезпечує зручний та інформативний інструмент для відстеження аномальної активності в реальному часі, сприяє оперативному виявленню потенційних загроз і допомагає приймати своєчасні заходи для їх нейтралізації.

Завдяки функціональності панелі подій, спеціаліст з інформаційної безпеки має можливість детально переглянути інформацію про кожну зафіксовану активність, пов’язану з користувачем. Це дозволяє не лише відстежувати загальний контекст подій, а й отримувати поглиблені дані про їхній характер і потенційний вплив на безпеку системи.

Як показано на рисунку 3.18, система User Behavior Analytics коректно

відреагувала на підозрілу активність, ідентифікувавши сайт, пов'язаний із завантаженням браузера Tor, як потенційно небезпечний. Ця подія була класифікована як перехід до підозрілого веб-ресурсу, що відображається у відповідному розділі панелі подій.

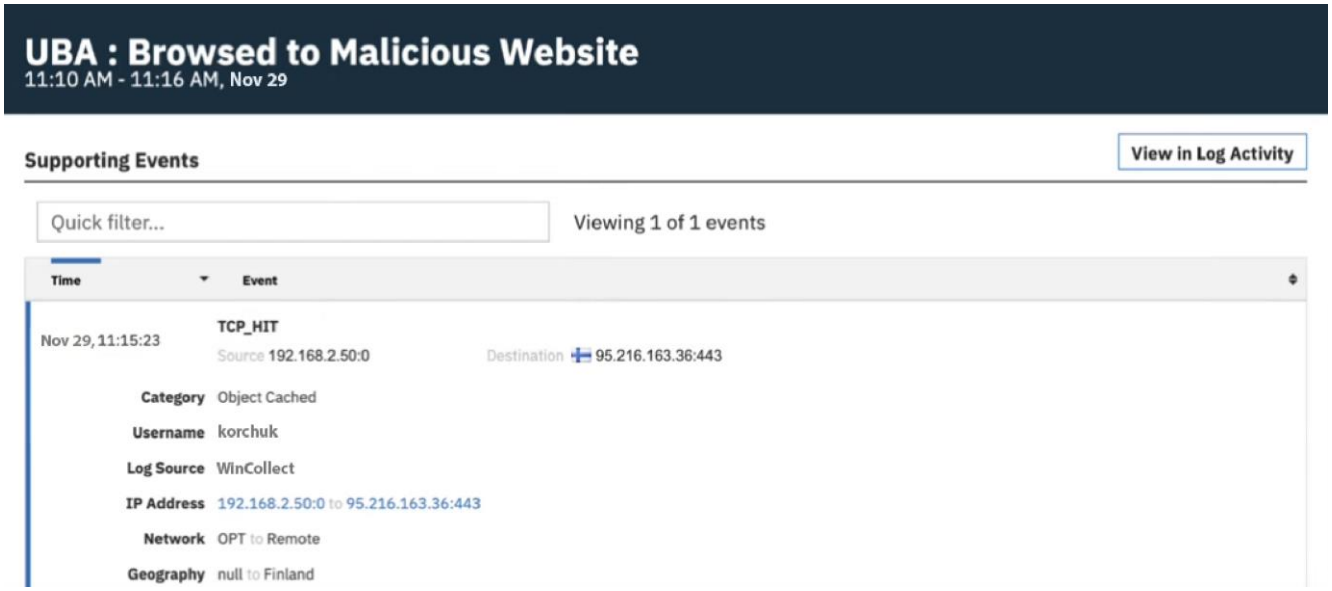

Рис. 3.18. UBA в дії

Подібна деталізація дозволяє аналітикам оцінювати природу інциденту, проводити розслідування причин його виникнення та розробляти заходи для запобігання подібній активності в майбутньому. Це значно підвищує ефективність системи моніторингу та сприяє підтриманню високого рівня інформаційної безпеки організації.

3.3. Рекомендації щодо виявлення внутрішньої загрози в інформаційних системах організацій

Для підвищення ефективності виявлення внутрішніх загроз необхідно використовувати комплексний підхід, інтегрувати сучасні технології та розробити та притримуватися чіткої стратегії кібербезпеки.

Рекомендації можна поділити на кілька ключових напрямків: технологічна інфрастуктура, організаційні заходи, використання аналітики та автоматизації, навчання та підвищення обізнаності працівників, постійне вдосконалення процесів.

Розглянемо кожний з цих пунктів більш детально.

Технологічна інфраструктура включає в себе:

інтеграція SIEM-систем: Рекомендується використовувати сучасні платформи, такі як IBM QRadar, для централізованого збору, аналізу та кореляції даних з різних джерел, таких як журнали подій, мережеві потоки та системи управління доступом;

впровадження UBA: UBA дозволяє створювати поведінкові профілі користувачів та виявляти аномальні дії, що можуть свідчити про внутрішню загрозу;

застосування DLP-систем: Для контролю доступу до конфіденційних даних та запобігання їх витоку;

підтримка PAM-рішень: Використання систем управління привілейованим доступом для мінімізації ризиків, пов'язаних із компрометацією облікових записів із підвищеними правами.

Організаційні заходи включають в себе:

регулярні аудити безпеки: Проведення внутрішніх перевірок для оцінки захищеності інформаційної інфраструктури та ідентифікації потенційних вразливостей;

розробка політик безпеки: Встановлення чітких правил і процедур використання інформаційних систем, включаючи контроль доступу, оновлення паролів та сегментацію мережі;

моніторинг привілейованих облікових записів: Спеціальний контроль за активністю користувачів із розширеними правами.

Використання аналітики та автоматизації включає в себе:

впровадження машинного навчання: Для автоматизації виявлення загроз і зниження кількості помилкових спрацьовувань;

інтеграція великих даних: Аналіз масштабних обсягів інформації для створення кореляцій і виявлення складних схем атак;

пріоритезація подій: Фокус на інцидентах із найбільшим ризиком для забезпечення ефективного реагування.

Навчання та підвищення обізнаності працівників включає в себе:

регулярні тренінги для співробітників: Для підвищення їх обізнаності щодо методів виявлення фішингових атак, безпечного використання ресурсів компанії та реагування на підозрілу активність;

розробка навчальних сценаріїв внутрішніх атак: Моделювання можливих інцидентів для навчання команд реагування.

Постійне вдосконалення процесів включає в себе:

інцидент-менеджмент: Забезпечення ефективної стратегії реагування на інциденти, включаючи відновлення систем та аналіз причин;

впровадження систем зворотного зв’язку: Постійна оцінка ефективності впроваджених рішень і модифікація політик безпеки на основі змін у ландшафті загроз.

Дотримання зазначених рекомендацій дозволяє організаціям значно знизити ризики, пов’язані з внутрішніми загрозами, а також мінімізувати їх потенційні негативні наслідки. Такий підхід сприяє створенню більш безпечного інформаційного середовища, де вчасне виявлення та нейтралізація аномальної активності стають ключовими елементами системи кіберзахисту.

Імплементація відповідних заходів дозволяє не лише підвищити рівень захищеності, але й зміцнити довіру до організації з боку співробітників, партнерів і клієнтів, що є важливим чинником для її стабільного функціонування та розвитку.

ВИСНОВКИ

У роботі проведено дослідження проблеми виявлення внутрішніх загроз в інформаційних системах організацій, проаналізовано сучасні підходи та існуючі рішення, а також розглянуто особливості застосування технологій на базі QRadar UBA.

Під час проведення аналізу проблем було виявлено, що внутрішні загрози становлять значний виклик для інформаційної безпеки організацій, оскільки такі загрози важко виявити за допомогою традиційних методів через їх специфіку: використання легітимного доступу, низьку видимість у стандартних системах моніторингу та поведінкові аномалії, які можуть залишатися непоміченими.

Проведено аналіз методів виявлення внутрішніх загроз, зокрема поведінковий аналіз, кореляцію подій, машинне навчання та аналіз аномалій. Також проаналізовано функціональні можливості сучасних платформ, що використовуються для моніторингу та аналізу внутрішніх загроз, включаючи SIEM-системи та спеціалізовані UBA-рішення.

Особливу увагу приділено аналізу QRadar UBA, яка забезпечує можливість ідентифікації аномальної поведінки користувачів через машинне навчання та кореляцію подій. QRadar UBA дозволяє створювати профілі користувачів, виявляти відхилення від типових моделей поведінки та автоматично визначати інциденти, які можуть свідчити про внутрішні загрози.

Розроблено порядок впровадження технології на базі QRadar UBA, який включає налаштування системи для збору даних, інтеграцію з іншими компонентами безпеки, створення політик та правил для виявлення аномалій, а також регулярний моніторинг і вдосконалення алгоритмів аналізу. Даний підхід дозволяє значно підвищити ефективність виявлення внутрішніх загроз та мінімізувати ризики для інформаційних активів організації.

Таким чином, робота робить внесок у вирішення проблеми виявлення внутрішніх загроз шляхом впровадження інноваційних технологій аналізу

поведінки, підвищення адаптивності систем захисту та забезпечення комплексного підходу до моніторингу інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Звіт IBM 2024 про вартість витоку даних - CoreWin. *CoreWin*. URL: https://corewin.ua/news/ibm-report-2024/ (дата звернення: 04.12.2024).

2. 2023 Insider Threat Report [Gurucul] - Cybersecurity Insiders. *Cybersecurity Insiders*. URL: https://www.cybersecurity-insiders.com/portfolio/2023-insider-threat-report-gurucul/ (дата звернення: 04.12.2024).

3. 2022 Cost of the insider threats global report – Ponemon Institute. URL: https://static.poder360.com.br/2022/01/pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf (дата звернення 04.12.2024)

4. Insider Threat Statistics for 2024: Facts, Reports & Costs | Syteca. *Syteca*. URL: https://www.syteca.com/en/blog/insider-threat-statistics-facts-and-figures (дата звернення: 04.12.2024).

5. Defining Insider Threats | CISA. *Cybersecurity and Infrastructure Security Agency CISA*. URL: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats (дата звернення: 04.12.2024).

6. Лог – що це таке і як з ними працювати | Wiki HOSTiQ. *HOSTiQ Wiki*. URL: https://hostiq.ua/wiki/ukr/log/ (дата звернення: 04.12.2024).

7. Trellix. *Trellix Doc Portal*. URL: https://docs.trellix.com/ru-RU/bundle/network-security-platform-10.1.x-product-guide/page/GUID-6046ADFB-FAF7-4C91-9CCE-8A77486D2C80.html (дата звернення: 04.12.2024).

8. IBM. What is User Behavior Analytics (UBA) | IBM?. *IBM - United States*. URL: https://www.ibm.com/topics/user-behavior-analytics (дата звернення: 04.12.2024).

9. Zero Trust: відповідь на сучасні виклики у сфері кібербезпек. *Міжнародна аудиторська компанія BDO - BDO*. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/zero-trust-a-revolutionary-approach-in-modern-cybersecurity (дата звернення: 04.12.2024).

10. IBM Registration form. *IBM*. URL: https://www.ibm.com/account/reg/us-

en/signup?formid=urx-52823 (дата звернення: 04.12.2024).

11. IBM QRadar SIEM. *IBM - United States*. URL: https://www.ibm.com/products/qradar-siem#Why+QRadar+SIEM (дата звернення: 04.12.2024).

12. IBM QRadar Security Intelligence Platform 7.5. *IBM - United States*. URL: https://www.ibm.com/docs/en/qsip/7.5?topic=deployment-qradar-architecture-overview (дата звернення: 04.12.2024).

13. QRadar common. *IBM - United States*. URL: https://www.ibm.com/docs/en/qradar-common?topic=app-qradar-user-behavior-analytics (дата звернення: 04.12.2024).

14. QRadar User Behavior Analytics Ratings Overview. *Gartner Peer Insight*. URL: https://www.gartner.com/reviews/market/insider-risk-management-solutions/vendor/ibm/product/qradar-user-behavior-analytics#reviews (дата звернення: 04.12.2024)

15. QRadar Machine Learning. *IBM - United States*. URL: https://www.ibm.com/docs/en/qradar-common?topic=app-machine-learning-user-models (дата звернення: 04.12.2024).

16. Detect Insider Threats with User Behavior Analytics - IBM Digital Transformation Blog. *IBM Digital Transformation Blog*. URL: https://www.ibm.com/blogs/digital-transformation/in-en/blog/detect-insider-threats-with-user-behavior-analytics/ (дата звернення: 04.12.2024).

17. Корчук Дмитрій Вікторович. Важливість використання аналізу поведінки користувачів та сутностей в сучасних корпоративних мережах. Всеукраїнська Науково-Практична «Актуальні проблеми кібербезпеки» Державний Університет Телекомунікацій. 25 жовтня 2024. Тези доповідей. С. 100-103. URL: https://duikt.edu.ua/uploads/p_2661_48963150.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)