

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**«Технологія інтелектуального виявлення загроз хмарним корпоративним
ресурсам на основі Amazon GuardDuty»**

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*

Павло ОРЛИК

(підпис)

Виконав: здобувач(ка) вищої освіти групи БСДМ-62

ОРЛИК Павло

(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

	Стор.
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	9
ВСТУП	10
1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ІНТЕЛЕКТУАЛЬНОГО ВИЯВЛЕННЯ ЗАГРОЗ ХМАРНИМ КОРПОРАТИВНИМ РЕСУРСАМ	13
1.1 Дослідження проблеми інтелектуального виявлення загроз хмарним корпоративним ресурсам	13
1.2 Аналіз підходів до інтелектуального виявлення загроз хмарним корпоративним ресурсам	22
1.3 Аналіз існуючих рішень для інтелектуального виявлення загроз хмарним корпоративним ресурсам	25
2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ІНТЕЛЕКТУАЛЬНОГО ВИЯВЛЕННЯ ЗАГРОЗ ХМАРНИМ КОРПОРАТИВНИМ РЕСУРСАМ НА БАЗІ AMAZON GUARDDUTY	30
2.1 Призначення та основні функції рішення Amazon GuardDuty	30
2.2 Архітектура рішення Amazon GuardDuty	34
2.3 Порядок функціонування рішення Amazon GuardDuty	37
3 ТЕХНОЛОГІЯ ІНТЕЛЕКТУАЛЬНОГО ВИЯВЛЕННЯ ЗАГРОЗ ХМАРНИМ КОРПОРАТИВНИМ РЕСУРСАМ НА БАЗІ AMAZON GUARDDUTY	44
3.1 Порядок застосування рішення Amazon GuardDuty	44
3.2 Технологія інтелектуального виявлення загроз хмарним корпоративним ресурсам	47
3.3 Рекомендації щодо інтелектуального виявлення загроз хмарним корпоративним ресурсам	58
ВИСНОВКИ	63
ПЕРЕЛІК ПОСИЛАНЬ	65
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)	67

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп'ютер

ЦОД – центр обробки даних

API – Application Programming Interface

APT – Advanced Persistent Threat

CDN – Content Delivery Network

CIPS – Cloud Infrastructure and Platform Service

CNAPP – Cloud-Native Application Protection Platform

DAST – Dynamic Application Security Testing

DDoS – Distributed Denial of Service

DNS – Domain Name System

IaaS – Infrastructure as a Service

IAM – Identity and Access Management

MSSP – Managed Security Service Provider

WAAP – Web Application and API protection

SOC – Security Operations Center

OWASP – Open Web Application Security Project

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. Виявлення загроз у реальному часі є критично важливим компонентом сучасної кібербезпеки, що дозволяє організаціям ідентифікувати кіберзагрози та реагувати на них у міру їх виникнення. На відміну від традиційних підходів, які часто виявляють атаки після нанесеної значної шкоди, моніторинг загроз у реальному часі дає миттєве уявлення про підозрілу діяльність. Цей проактивний метод необхідний для захисту від розширених загроз, таких як викрадення хмарних облікових записів, і захисту мережевих середовищ.

Постійно аналізуючи дані, виявлення загроз кібербезпеці в реальному часі допомагає захиститися від кібератак, що розвиваються, забезпечуючи надійну мережеву безпеку для компаній будь-якого розміру. Ця здатність стала незамінною для вирішення зростаючої складності та швидкості сучасного ландшафту кіберзагроз.

Виявлення загроз у реальному часі означає здатність ідентифікувати кіберзагрози та реагувати на них у міру їх виникнення, мінімізуючи потенційну шкоду та збої. Завдяки постійному моніторингу систем, мереж і діяльності користувачів це дозволяє організаціям залишатися попереду загроз у сьогоdnішньому швидкому цифровому середовищі.

Виявлення загроз у реальному часі покладається на постійне спостереження за мережевою активністю, поведінкою користувачів і системними журналами для виявлення аномалій, які можуть вказувати на кіберзагрози. Коли потенційна загроза виявлена, автоматизовані сповіщення гарантують, що групи безпеки можуть вжити негайних заходів, скорочуючи час реагування. Інтеграція з інструментами безпеки такими, як брандмауери, системи виявлення вторгнень та інших інструментів безпеки, покращує загальні можливості виявлення загроз.

Розширені алгоритми машинне навчання аналізують величезні обсяги даних у режимі реального часу, розпізнаючи шаблони та передбачаючи потенційні загрози точніше, ніж традиційні методи. Виявлення загроз у режимі реального часу

дозволяє швидко та скоординовано діяти для зменшення ризиків, забезпечуючи мінімальні збої в роботі.

Використовуючи ці компоненти, виявлення загроз у реальному часі забезпечує проактивний підхід до кібербезпеки. Він не лише визначає поточні загрози, але й готує організації до протидії майбутнім атакам, зміцнюючи їхню загальну стійкість до зростаючої складності ландшафту кіберзагроз.

Вищесказане визначає актуальність теми цієї кваліфікаційної роботи, основний зміст якої становлять дослідження технології інтелектуального виявлення загроз хмарним корпоративним ресурсам на базі Amazon GuardDuty.

Об'єкт дослідження – інтелектуальне виявлення загроз хмарним корпоративним ресурсам.

Предмет дослідження – технологія інтелектуального виявлення загроз хмарним корпоративним ресурсам на базі Amazon GuardDuty.

Мета роботи – розробити порядок застосування технології інтелектуального виявлення загроз хмарним корпоративним ресурсам на базі Amazon GuardDuty та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми інтелектуального виявлення загроз хмарним корпоративним ресурсам;

проаналізувати підходи до інтелектуального виявлення загроз хмарним корпоративним ресурсам;

проаналізувати існуючі рішення для інтелектуального виявлення загроз хмарним корпоративним ресурсам;

проаналізувати методи та засоби інтелектуального виявлення загроз хмарним корпоративним ресурсам на базі Amazon GuardDuty;

розкрити порядок реалізації технології інтелектуального виявлення загроз хмарним корпоративним ресурсам на базі Amazon GuardDuty.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології інтелектуального виявлення загроз хмарним

корпоративним ресурсам на базі Amazon GuardDuty, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 29 жовтня 2025 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ІНТЕЛЕКТУАЛЬНОГО ВИЯВЛЕННЯ ЗАГРОЗ ХМАРНИМ КОРПОРАТИВНИМ РЕСУРСАМ

1.1. Дослідження проблеми інтелектуального виявлення загроз хмарним корпоративним ресурсам

У Звіті Trend Micro [1] зазначається, що безпека хмарних технологій у 2025 році визначається суперечностями: з одного боку, постійні загрози та низький рівень довіри, з іншого – стратегії, що розвиваються, та прискорення автоматизації. Хоча основи хмарних ризиків залишаються вперто знайомими – несанкціонований доступ, витік даних та фішинг – команди безпеки сьогодні стикаються з глибшим, більш структурним викликом: як захистити розлогі, швидкозмінні, багатохмарні середовища за допомогою інструментів та процесів, створених для іншої епохи.

Відмічається, що хмарні загрози розвиваються, але захисні засоби не встигають за ними. Команди безпеки визначають такі складні загрози, як програми-вимагачі (74%) та вразливості нульового дня (63%), як свої найнагальніші проблеми, що підкреслює небезпечну ескалацію витонченості та терміновості зловмисників. Водночас фундаментальні загрози зберігаються, причому несанкціонований доступ (64%), витоки даних (62%) та фішингові атаки (60%) продовжують домінувати серед фактичних інцидентів безпеки. Це поєднання зростаючого числа складних загроз та вперто повторюваних ризиків підкреслює, чому організації повинні терміново посилити свій захист, особливо щодо контролю ідентифікації, безпеки робочих навантажень та видимості в режимі реального часу в хмарних середовищах [1].

Виявлення та реагування фрагментовані, і це уповільнює роботу команд. Лише 21% організацій впевнені у своїй видимості в різних робочих навантаженнях, і лише 25% довіряють своїм інструментам для виявлення складних загроз. Аналіз першопричин зараз є найбільш трудомісткою частиною реагування на інциденти (34%), а 97% повідомляють про труднощі з виконанням єдиної відповіді від усіх

постачальників послуг, що є прямим результатом як фрагментації архітектури, так і операційних витрат [1].

Операційні труднощі обмежують як дотримання вимог, так і автоматизацію. Зусилля щодо дотримання вимог стримуються розповсюдженням інструментів (63%), обмеженою автоматизацією (58%) та труднощами, пов'язаними з інтеграцією з конвеєрами DevOps (37%). Хоча автоматизація вважається найефективнішим покращенням реагування на інциденти (36%), лише 52% організацій наразі надають їй пріоритет, що свідчить про розрив між усвідомленням та діями [1].

Пріоритети безпеки зміщуються в бік єдиного контролю. До головних стратегічних пріоритетів належать безпека даних (83%), управління ідентифікацією та доступом (77%) і виявлення загроз (72%). Разом вони відображають перехід до вбудованого забезпечення виконання політик та видимості в режимі реального часу, переходячи від реактивної позиції до фундаментальної архітектури.

Штучний інтелект більше не є чимось амбітним, а дієвим. Команди безпеки більше не експериментують зі штучним інтелектом, а впроваджують його. Найчастіші варіанти використання включають виявлення загроз (75%), аналіз аномалій (70%) та автоматизоване реагування (62%). Зі зростанням складності хмарних технологій штучний інтелект стає не просто множителем сили, а необхідним рівнем контролю для масштабованого, інтелектуального захисту.

Дані чітко демонструють траєкторію – лідери у сфері безпеки відходять від розрізнених інструментів та ручних робочих процесів до інтегрованих платформ, які об'єднують виявлення, забезпечення дотримання політик та автоматизоване реагування. З'являється не просто розумніший набір інструментів, а стратегія хмарної безпеки, розроблена для швидкості, масштабування та безперервного контролю [1].

Сьогоднішній ландшафт загроз відображає не лише зовнішніх зловмисників – це побічний продукт розширення архітектур, надмірно розкриті ідентифікаційні дані та неправильно узгоджені засоби контролю.

64% фахівців називають несанкціонований доступ своєю головною хмарною загрозою, порівняно з 59% минулого року (рисунок 1.1). Кількість організацій, які вважають фішинг та соціальну інженерію головною загрозою, зросла з 48% до 60%, що свідчить про різке зростання кількості компрометацій, спрямованих на користувачів. Рівень занепокоєння щодо програм-вимагачів зріс до 74%, тоді як атаки нульового дня посідають друге місце з 63%. Вплив API (52%) зараз є головною проблемою, що підкреслює, що інтерфейси, а не інфраструктура, є новою перевагою. Занепокоєння щодо залежності від постачальників (41%) та відновлення після збоїв (37%) свідчать про те, що хоча хмара обіцяє стійкість, багато хто все ще сумнівається у своїй здатності контролювати результати в умовах збоїв [1].

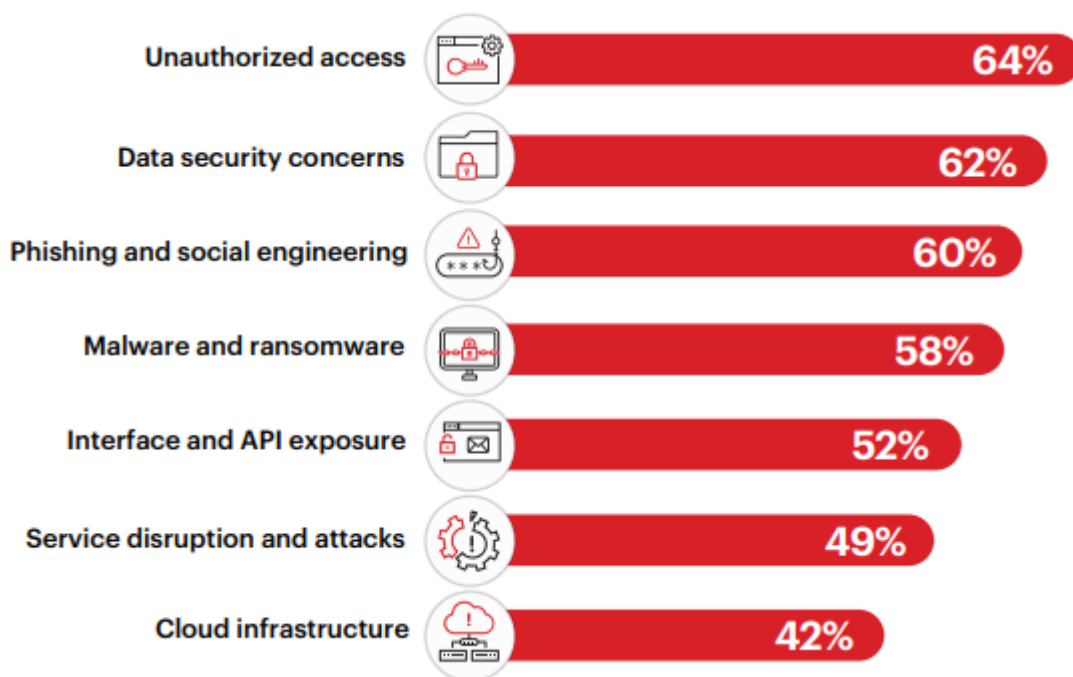


Рис. 1.1. Найбільші загрози безпеці в хмарі [1]

Наступний рівень проблем включає шкідливе програмне забезпечення та програми-вимагачі (58%, порівняно з 38% у 2024 році), а також вплив API (52%, порівняно з 49%), що відображає розширення поверхні атак, властивій багатохмарним та контейнерним середовищам. Збої в обслуговуванні (49%, порівняно з 37%) та ризики, пов'язані з базовою інфраструктурою (42%), йдуть уважно, тоді як внутрішні загрози (39%) та компрометація ланцюга поставок (37%)

завершують багаторівневу модель загроз, яка торкається практично кожної поверхні сучасного хмарного стеку [1].

Захист хмарних середовищ означає захист не лише інфраструктури, а й ідентифікаційних даних, даних та робочих процесів, часто на слабо пов'язаних платформах. За словами респондентів, найнагальніші загрози в хмарі пов'язані з доступом та розкриттям інформації: 64% називають несанкціонований доступ головною проблемою (порівняно з 59% у попередньому році), за ним йдуть безпека даних (62%, порівняно з 61% у 2024 році) та фішингові атаки або атаки соціальної інженерії (60%, порівняно з 48%). Це загрози, які використовують не лише неправильні конфігурації чи недоліки коду, а й прогалини в ідентифікаційних даних, поведінку користувачів та слабку автентифікацію, що робить їх особливо важко стримувати в безпериметральній, постійно активній архітектурі.

Спираючись на найвищі ризики, пов'язані з доступом та розкриттям інформації, дані показують, як ці широкі проблеми переростають у конкретні загрози з високим рівнем впливу, особливо в контексті дедалі складніших багатохмарних середовищ.

Згідно з дослідженням [1], атаки програм-вимагачів та шкідливих програм значно очолюють список проблем, причому 74% респондентів відзначають їх як основний вектор загрози (рисунок 1.2). Відразу за ними йдуть вразливості нульового дня (63%) та загрози ескалації привілеїв або внутрішні загрози (57%), кожна з яких підкреслює подвійну проблему захисту як від невідомих зовнішніх експлойтів, так і від зловживань з боку довірених користувачів. Експлойти API також викликають сильне занепокоєння у 53%, що підтверджує, що API, які часто є сполучною тканиною сучасних хмарних архітектур, тепер розглядаються як стратегічні точки впливу [1].

Наприклад, програма для обміну файлами, розгорнута в кількох регіонах, може інтегруватися з різними хмарними сервісами та інструментами виявлення загроз. Якщо вразливість нульового дня експлуатується в сторонньому компоненті, непослідовність ведення журналу та базових ліній реагування може затримати стримування, що призведе до переростання незначної експлойту у серйозну втрату

даних.

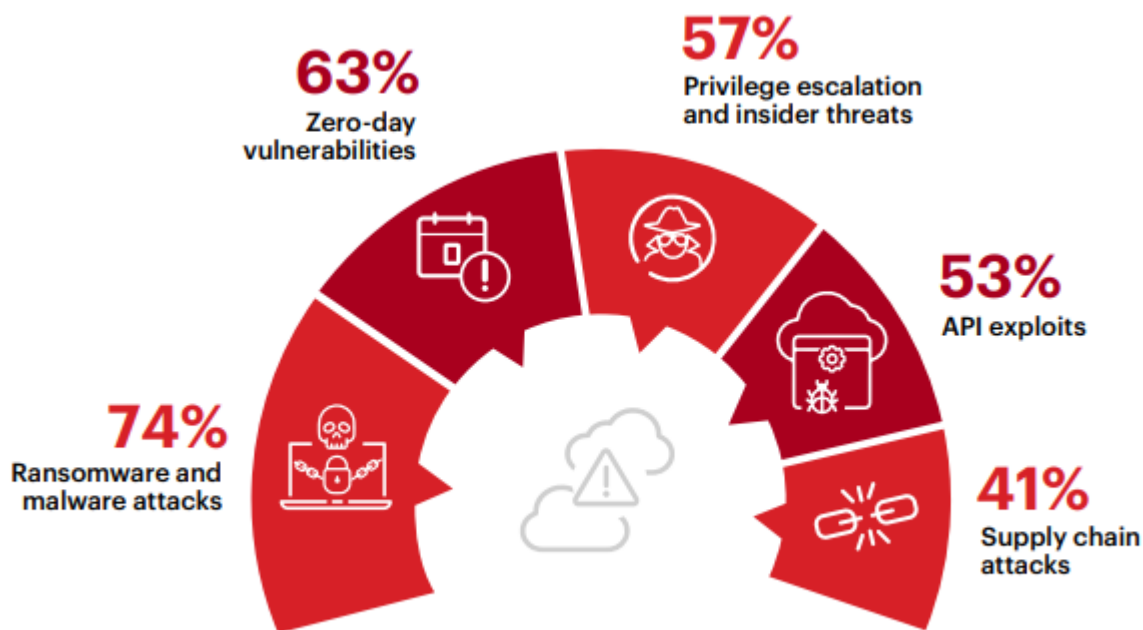


Рис. 1.2. Тип складних загроз у багатохмарному середовищі, який найбільше непокоїть фахівців [1]

Щоб реагувати на це, лідери у сфері безпеки повинні розвивати рішення за межами точкових платформ та інвестувати в хмарні платформи, які забезпечують постійну видимість поведінки робочого навантаження, використання ідентифікаційних даних та взаємодії API. Одного лише розширеного виявлення загроз недостатньо без інтегрованого забезпечення виконання політик та автоматизованих стратегій стримування, адаптованих для хмарних архітектур.

Хоча передові загрози домінують у увазі, лідери у сфері безпеки залишаються однаково стурбованими системними слабкостями, які охоплюють архітектуру, управління та безперервність операцій (рисунок 1.3). 73% респондентів очолюють список, називаючи безпеку даних та конфіденційність як основну проблему, що охоплює все: від втрати даних до випадкового розкриття облікових даних. Далі йдуть питання дотримання вимог та правові питання (66%), що вказує на те, що складність нормативних актів та суверенітет даних продовжують суттєво впливати на рішення щодо хмарної стратегії. Операційна та інфраструктурна безпека (60%) також залишається центральною проблемою, що свідчить про постійне незручність

щодо прогалин у видимості, надійності послуг та прозорості постачальників. Управління інцидентами (53%) та тіньові ІТ (45%) підкреслюють, що простота використання хмари залишається палицею з двома кінцями, що забезпечує гнучкість, але часто обходить нагляд. Занепокоєння щодо залежності від постачальників (41%) та аварійного відновлення (37%) свідчать про те, що хоча хмара обіцяє стійкість, багато хто все ще сумнівається у своїй здатності контролювати результати в умовах збоїв [1].



Рис. 1.3. Основні занепокоєння щодо безпеки хмарних технологій [1]

Команда може виявити, що критично важливе сховище було відкритим протягом тижнів через непослідовний моніторинг у різних постачальників. Ця єдина прогалина у видимості охоплює одночасно захист даних, ризик відповідності та операційний нагляд. Щоб вирішити ці дублюючі пріоритети, стратегії хмарної безпеки повинні бути закріплені на єдиному контролі даних, моніторингу в режимі реального часу та забезпеченні дотримання політик, які працюють у всіх хмарних середовищах, а не лише в окремих. Стійкість починається з контролю, а контроль починається з чіткої, безперервної та дієвої видимості [1].

Навіть попри зростання обізнаності про загрози, більшість організацій все ще мають труднощі з реагуванням чітко та швидко. Лише 21% фахівців повідомляють

про чітку прозорість робочих навантажень, конфігурацій та потоків даних. 34% кажуть, що аналіз першопричини є найбільш трудомісткою частиною реагування на інцидент. 97% повідомляють про труднощі з виконанням єдиного плану реагування для кількох постачальників хмарних послуг. 75% висловлюють лише помірну або низьку впевненість у виявленні та запобіганні складним загрозам. Автоматизація є найбажанішим покращенням, яке називають 36%, проте лише 52% надають їй пріоритет.

Сукупна вага прогалин у видимості, збоїв координації та затримок виявлення вказує на явне вузьке місце, яке автоматизація має всі можливості вирішити. 36% керівників служб безпеки кажуть, що автоматизоване виявлення та реагування найбільше покращили б їхню роботу з інцидентами, далі йдуть централізовані платформи реагування (27%) та інтеграція інформації про загрози (20%). Посил зрозумілий: реагування має бути швидшим, а робочі процеси, що виконуються лише за участю людини, не масштабуватимуться (рисунок 1.4) [1].



Рис. 1.4. Шляхи покращення реагування на інциденти безпеки в багатохмарному середовищі [1]

Отже, організаціям слід зосередитися на автоматизації на основі подій, яка працює в хмарних середовищах – запускаючи дії стримування, забезпечуючи дотримання політик та ескалюючи аномалії високого ризику без затримки.

Вбудовування цих можливостей безпосередньо в рівні виконання, особливо для контролю ідентифікації та API, перетворює виявлення на негайний захист.

Щоб ефективно протидіяти складним сучасним загрозам, команди безпеки швидко звертаються до штучного інтелекту. Однак ефективність рішень на основі штучного інтелекту залежить від їх чіткого узгодження з практичними пріоритетами безпеки. Наведені нижче методи штучного інтелекту та машинного навчання виявилися найперспективнішими для вирішення конкретних реальних проблем хмарної безпеки.

На вершині списку 66% респондентів бачать перспективу в поясненому штучному інтелекті (XAI), що відображає зростаючий попит не лише на розумніше виявлення, але й на моделі, які можна зрозуміти, перевірити та довіряти, особливо враховуючи, що штучний інтелект починає впливати на автоматизоване реагування.

Глибоке навчання для виявлення аномалій (63%) відображає зростаючу потребу у виявленні загроз, прихованих у шумних, зашифрованих середовищах, де традиційні правила не справляються з роботою. Обробка природної мови (57%) та федеративне навчання (52%) відображають більш спеціалізовані пріоритети, такі як виявлення фішингу шляхом розуміння мовних шаблонів зловмисника або забезпечення безпечної та конфіденційної співпраці в роботі з даними на різних платформах. Нижче у списку, але все ж варто зазначити, знаходяться навчання з підкріпленням (42%) та глобальні мережі (GAN) для симуляції загроз (36%), що сигналізує про інтерес до більш адаптивного, проактивного захисту.

Привабливість штучного інтелекту стає зрозумілішою, якщо розглядати її крізь призму сучасних вимог до хмарної безпеки: швидкості, масштабованості та втоми. Команди безпеки не женуться за штучним інтелектом заради новизни – вони звертаються до нього, щоб розширити свою охоплення, зменшити шум та швидше діяти під тиском. Серед основних переваг, що згадуються, покращене виявлення загроз (79%), швидше реагування на інциденти (75%) та зменшення кількості хибнопозитивних результатів (73%), що підтверджує цінність штучного інтелекту в перетворенні обсягу на ясність та дії [1].

Оскільки стратегічна перспектива ІІІ чітко визначена, увага тепер зосереджується на тому, де він забезпечує операційні результати. Очолюють список виявлення та аналіз загроз (75%, порівняно з 71% у 2024 році), за ними йдуть виявлення аномалій та аналіз поведінки (70%, порівняно з 54%). Ці пріоритети відображають зростаючу залежність від ІІІ не лише для виявлення загроз, але й для їх розуміння в режимі реального часу.

Автоматизоване реагування та виправлення (62%, порівняно з 61%) також займає високе місце, що свідчить про перехід до ІІІ не лише як механізму виявлення, а й як рівня реагування. Тим часом, аналітика поведінки користувачів та об'єктів (52%) та управління станом безпеки (47%) завершують список, що відображає ширший інтерес до систем ІІІ, які покращують контекст та зменшують вплив з часом.

Хмарні інфраструктури стали основою незліченної кількості підприємств та послуг. Очікується, що ринок хмарних обчислень досягне 2 291,59 мільярда доларів США до 2032 року. Однак, побоювання щодо безпеки хмарних технологій часто є основною перешкодою для їх впровадження. Без належного захисту хмарні корпоративні ресурси стають вразливими. Захист хмарних ресурсів та ідентифікаційних даних зараз важливіший, ніж будь-коли [7].

Загрози безпеці хмарних середовищ включають витіки даних, внутрішні загрози, викрадення облікових записів, незахищені API та атаки шкідливого програмного забезпечення. Ці загрози спрямовані на хмарні середовища, використовуючи неправильні конфігурації, слабкі засоби контролю доступу або людські помилки. Виявлення в хмарній безпеці передбачає використання передових інструментів, таких як штучний інтелект та машинне навчання, для моніторингу, ідентифікації та реагування в режимі реального часу на незвичайну поведінку або потенційні порушення безпеки.

Проблеми безпеки хмарних технологій включають:

- інтеграція застарілих систем;

- управління мультихмарними та гібридними середовищами;

- забезпечення конфіденційності даних та дотримання нормативних вимог;

підтримка видимості та контролю над складними хмарними інфраструктурами.

1.2. Аналіз підходів до інтелектуального виявлення загроз хмарним корпоративним ресурсам

Розглянемо підходи до виявлення загроз безпеки в режимі реального часу.

Виявлення загроз безпеці в режимі реального часу передбачає використання передових технологій та інструментів для моніторингу систем, аналізу даних і реагування на потенційні загрози в міру їх виникнення. Цей проактивний підхід спирається на [2]:

поведінковий аналіз. Системи реального часу встановлюють базову лінію нормальної активності для користувачів і пристроїв, виявляючи аномалії, які можуть сигналізувати про такі загрози викрадення хмарного облікового запису або спроби несанкціонованого доступу;

штучний інтелект і машинне навчання. Ці технології дозволяють розпізнавати образи та прогнозувати аналітику, дозволяючи швидше ідентифікувати незвичайну поведінку, яка може вказувати на кібератаку в режимі реального часу;

інструменти моніторингу в реальному часі. Такі рішення, як системи інформації про безпеку та управління подіями (SIEM), мережеве виявлення та реагування (NDR) і системи виявлення вторгнень (IDS), постійно відстежують мережеву активність і генерують інформацію. Хоча деякі рішення завжди є системами моніторингу, не можна сказати напевно, що ці інструменти виявлятимуть усі загрози для корпоративних систем. Багато рішень покладаються на історичні дані атак для виявлення загроз, незважаючи на моніторинг корпоративних систем у реальному часі;

інтеграція з існуючою інфраструктурою безпеки. Інструменти виявлення в реальному часі інтегруються з брандмауерами, елементами керування доступом та іншими технологіями безпеки, щоб забезпечити цілісну стратегію захисту.

Прикладами виявлення загроз кібербезпеці в реальному часі корпоративним ресурсам є [2]:

запобігання викраденню хмарних облікових записів. Коли зловмисник намагається отримати доступ до хмарного облікового запису за допомогою викрадених облікових даних, системи виявлення в реальному часі позначають незвичайні місця входу або кілька невдалих спроб. Система негайно сповіщає команди безпеки або блокує обліковий запис, щоб запобігти доступу;

моніторинг внутрішньої мережі. У сценарії, коли зловмисник обходить початкові рівні безпеки, такі як брандмауери, і проникає у внутрішню мережу, інструменти моніторингу в реальному часі можуть виявляти нові загрози, виявляючи тонкі аномалії. Наприклад, скомпрометована кінцева точка може почати спілкуватися з незвичайними зовнішніми IP-адресами або демонструвати бічний рух у мережі. Ця поведінка, яку традиційні методи можуть не помічати, позначається системами реального часу для негайного дослідження;

виявлення інсайдерської загрози. Користувач раптово починає завантажувати великі обсяги конфіденційних файлів. Інструменти реального часу розпізнають поведінку як несумісну з минулою діяльністю, запускаючи сповіщення та призупиняючи сеанс, щоб запобігти подальшій ексфільтрації даних.

Для виявлення загроз кібербезпеки в реальному часі, організаціям потрібні [2]:

рішення на основі штучного інтелекту для аналізу прогнозованих загроз;

інструменти NDR для моніторингу мережевої активності;

інструменти хмарного моніторингу для захисту віртуальних середовищ.

Ці можливості дозволяють організаціям швидко виявляти загрози та реагувати на них, забезпечуючи безпеку мереж, даних і користувачів від передових кіберзагроз.

Необхідно відмітити, що інтеграція штучного інтелекту у виявлення загроз у реальному часі дозволила організаціям вирішувати ці проблеми кібербезпеки. Оскільки кіберзагрози стають все більш складними, рішення, керовані штучним інтелектом, стають незамінними для виявлення та нейтралізації цих ризиків у

режимі реального часу.

Застосування ШІ може значно підвищити швидкість, точність і адаптивність моніторингу загроз у реальному часі. Традиційні системи значною мірою покладалися на заздалегідь визначені правила або статистичні моделі, яким було важко встигати за динамічною природою сучасних кібератак. Інструменти штучного інтелекту, що працюють на основі машинного навчання, постійно навчаються на нових даних, що дозволяє їм виявляти закономірності та аномалії, які можуть вказувати на загрозу. Ця можливість особливо ефективна для ідентифікації нових векторів атак, таких як експлойти нульового дня або інсайдерські загрози, які традиційні системи часто пропускають.

Зростаючий обсяг і складність кібератак зробили необхідним виявлення в реальному часі за допомогою штучного інтелекту. Оскільки підприємства використовують хмарні технології, мобільні пристрої та віддалені робочі середовища, поверхня атаки розширилася, що збільшило потребу в розумніших і швидших рішеннях безпеки. Інструменти на основі штучного інтелекту можуть вирішити ці проблеми, легко масштабуючи та забезпечуючи постійний захист у різноманітних середовищах.

Інструменти штучного інтелекту перевершують статистичні моделі, пропонуючи більшу адаптивність і точність. У той час як статистичні моделі спираються на статичні правила, ШІ динамічно оновлюється на основі нових загроз. Наприклад, штучний інтелект може точніше розрізняти доброякісні аномалії та шкідливу активність, зменшуючи помилкові спрацьовування та забезпечуючи швидші та цілеспрямованіші відповіді. Це робить ШІ безцінним активом у протидії передовим кіберзагрозам, що розвиваються.

Виявлення загроз у реальному часі стало наріжним каменем ефективної кібербезпеки, оскільки підприємства мають більше комплексна цифрова інфраструктура. Отже, вони також стикаються з дедалі складнішими атаками, які вимагають негайного виявлення та реагування. Моніторинг загроз у реальному часі має забезпечувати гнучкість, необхідну для захисту критично важливих активів, гарантуючи, що організації можуть працювати безпечно без шкоди для

продуктивності чи репутації.

1.3. Аналіз існуючих рішень для інтелектуального виявлення загроз хмарним корпоративним ресурсам

Інструменти моніторингу безпеки хмари можуть допомогти організаціям збирати розширену інформацію про загрози та проводити аналіз для ефективного зниження ризиків та управління вразливостями. Рішення для хмарної безпеки може суттєво покращити безпеку організації та запропонувати єдине вікно огляду для моніторингу програм. Постачальники хмарних послуг за замовчуванням нехтують безпекою під час розробки цих платформ, тому організації повинні звертати пильну увагу на деталі [3].

Міграція до хмари зменшує загальну видимість компонентів інфраструктури, тому необхідні інструменти хмарної безпеки для виявлення та проактивного виявлення нових загроз у розподілених місцях.

Моніторинг безпеки хмари охоплює безперервну ідентифікацію, виявлення та усунення внутрішніх та зовнішніх загроз, що стосуються компонентів, платформ та сервісів хмарної інфраструктури. Безпека хмари забезпечує покращену прозорість для підприємств, підвищує гнучкість та зменшує ризики безпеки. Організації стикаються з постійною проблемою неможливості моніторингу хмарних ресурсів та контролю даних під час масштабування або міграції до хмари, і інструменти моніторингу безпеки хмари допомагають у цьому аспекті [3].

Інструменти моніторингу безпеки хмари – це рішення для моніторингу та аналітики загроз, які покращують видимість хмарних програм, мереж, компонентів інфраструктури та середовищ. Вони виявляють та усувають потенційні ризики й допомагають підприємствам забезпечити безперервність та відповідність вимогам. Моніторинг безпеки хмари також допомагає організаціям визначати пріоритети та пом'якшувати критичні проблеми, забезпечувати дотримання політик безпеки та сприяти виявленню конфіденційних даних [3, 9-11].

До цих рішень додаються різні функції, але кожне рішення для моніторингу

хмарної безпеки унікальне, а варіанти використання залежать, перш за все, від вимог бізнесу або підприємства.

Моніторинг безпеки хмарних технологій застосовує проактивний підхід до безпеки, і не існує універсального рішення. Кожна організація матиме різні вимоги до безпеки, і з огляду на швидку міграцію до хмари з традиційних інфраструктур у наші дні, важливо забезпечити безпеку та захист активів, одночасно зменшуючи різні вразливості [3, 9-11].

SentinelOne пропонує платформу захисту хмарних додатків (CNAPP) світового класу, яка забезпечує неперевершений захист для розробки та розгортання багатохмарної інфраструктури. *SentinelOne* підходить для запобігання витоку хмарних облікових даних і постачається з механізмом наступальної безпеки, який розшифровує методи дій зловмисників і зупиняє їх на місці. Він пропонує багато інших переваг безпеки та є одним з провідних інструментів моніторингу хмарної безпеки в галузі [3].

SentinelOne Singularity застосовує комплексний та проактивний підхід до моніторингу безпеки хмари. Він розроблений для вирішення складних задач у багатохмарних та гібридних середовищах. *SentinelOne* забезпечує виявлення загроз та реагування на них за допомогою штучного інтелекту за допомогою безагентного сканування та розширеної аналітики. Уніфікована консоль та панель інструментів відповідності платформи забезпечують глибокий огляд робочих навантажень, контейнерів та безсерверних функцій, що дозволяє швидко виявляти та усувати загрози. Надійний моніторинг та управління відповідністю *SentinelOne* підтримує понад 20 нормативних баз. Він бездоганно інтегрується з робочими процесами CI/CD, Snyk та DevSecOps, забезпечуючи безперервне забезпечення безпеки без переривання розробки додатків [3].

Особливості *SentinelOne* [3]:

система керування безпекою хмари (CSPM) виявляє та усуває помилки в конфігураціях хмари перед розгортанням;

Purple AI, Binary Vault, Singularity Data Lake Integration та інтеграція Snyk;
виправлення в один клік, управління безпекою SaaS (SSPM), сканування

інфраструктури як коду (IaC) та хмарна криміналістика;

безагентне управління вразливостями за допомогою панелі відповідності, діаграми Explorer Graph та унікального механізму Offensive Security Engine на базі штучного інтелекту;

платформа захисту хмарних робочих навантажень (CWPP) застосовує комплексний підхід до хмарної безпеки для хмарних віртуальних машин, контейнерів та безсерверних функцій;

Kubernetes Security Posture Management (KSPM) усуває вразливості контейнерів та вирішує проблеми з неправильною конфігурацією кластера;

виявлення та реагування на хмарні загрози (CDR) дозволяє виявляти, розслідувати та усувати загрози в хмарі в режимі реального часу;

сканування секретів у режимі реального часу для понад 750 типів секретів на BitBucket, GitHub та GitLab;

безперервний моніторинг відповідності хмарним вимогам для понад 20 галузевих стандартів, таких як ISO 27001, PCI-DSS, NIST та управління вразливостями без використання агентів.

Основні проблеми, які усуває SentinelOne [3]:

відсутність єдиної видимості в багатохмарних середовищах;

затримка у виявленні загроз та реагуванні на них за допомогою фрагментованих систем моніторингу;

неправильні конфігурації безпеки хмарних робочих навантажень, контейнерів та конвеєрів CI/CD;

складнощі, пов'язані з дотриманням вимог у кількох рамках;

неефективність управління хмарними обліковими даними та витоками даних;

ручне втручання в процеси виявлення та усунення загроз;

збір даних хмарної телеметрії з різних джерел та її аналіз;

виявлення прихованих шляхів атак, прогнозування нових загроз та виявлення горизонтальних переміщень по мережах.

AWS CloudWatch – це сервіс моніторингу та управління, який пропонує дані та практичну аналітику для AWS, локальних, гібридних та інших хмарних додатків

і ресурсів інфраструктури. Він дозволяє користувачам збирати та отримувати доступ до даних про продуктивність та роботу у вигляді журналів і метрик з однієї єдиної платформи, а не переглядати їх ізольовано [3].

Консолідація даних моніторингу за допомогою CloudWatch призводить до оптимізації використання ресурсів, виявлення аномалій та підтримки безперебійної роботи в середовищах AWS.

Особливості AWS CloudWatch [3]:

збір показників: ця функція збирає та відстежує показники з ресурсів, програм і сервісів AWS, забезпечуючи видимість до однієї секунди;

керування журналами: збирає та агрегує дані журналів з численних джерел для полегшення моніторингу та усунення несправностей у режимі реального часу;

сигнали тривоги: дозволяє користувачам визначати сигнали тривоги, які можуть спрацьовувати на основі певних порогових значень і які сповіщатимуть або ініціюватимуть автоматичні дії;

панелі інструментів: надає налаштовувані панелі інструментів для візуалізації показників та журналів, що допомагає в операційному контролі;

керування подіями: відстежує та реагує на зміни ресурсів AWS, забезпечуючи доступність автоматизованих робочих процесів;

аналітика додатків: спостереження за роботою додатків для виявлення та виправлення проблем.

Microsoft Defender for Cloud захищає організації від кіберзагроз та об'єднує управління безпекою в багатохмарних та багатоконвеєрних середовищах. Він поєднує можливості Development Security Operations (DevSecOps), Cloud Security Posture Management (CSPM) та Cloud Workload Protection Platform (CWPP). Він пропонує хмарно-орієнтовану платформу захисту програм (CNAPP), яка постійно впроваджує належні практики безпеки та розробки програмного забезпечення [3].

Особливості Microsoft Defender for Cloud [3]:

аналітика контекстного кодового конвеєра;

централізоване управління політиками та багатохмарне покриття;

оцінка безпеки, виявлення стану безпеки на основі даних та аналіз шляхів

атаки;

керування дозволами Microsoft Entra;

оглядач безпеки хмари.

Вищезазначені інструменти моніторингу хмарної безпеки є найкращими в галузі та захищають усе: від активів, ресурсів та доступу до різних хмарних облікових записів і сервісів. Організації, які хочуть швидко масштабуватися та покращити управління хмарною безпекою, вважатимуть ці рішення ефективними. Треба зазначити, що хмарна безпека дотримується ітеративного підходу до безпеки, і більшість організацій отримують найкращі результати, поєднуючи ці інструменти для швидшого розслідування та активного усунення загроз [3].

Постачальники хмарних послуг за замовчуванням нехтують безпекою під час розробки цих платформ, тому організації повинні звертати пильну увагу на деталі. Інструменти моніторингу хмарної безпеки можуть допомогти організаціям збирати розширену інформацію про загрози та проводити аналіз для ефективного зниження ризиків та управління вразливостями. Вони можуть суттєво покращити стан безпеки організації та запропонувати єдине «скляне вікно» для моніторингу додатків.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ІНТЕЛЕКТУАЛЬНОГО ВІЯВЛЕННЯ ЗАГРОЗ ХМАРНИМ КОРПОРАТИВНИМ РЕСУРСАМ НА БАЗІ AMAZON GUARDDUTY

2.1. Призначення та основні функції рішення Amazon GuardDuty

Amazon GuardDuty – це служба виявлення загроз, яка постійно відстежує, аналізує та обробляє джерела даних і журнали AWS у корпоративному середовищі AWS. GuardDuty використовує канали інформації про загрози, такі як списки шкідливих IP-адрес і доменів, хеші файлів і моделі машинного навчання (ML), для виявлення підозрілої та потенційно шкідливої активності у корпоративному середовищі AWS. У наступному списку наведено огляд потенційних сценаріїв загроз, які GuardDuty може допомогти виявити [5]:

- скомпрометовані та викрадені облікові дані AWS;

- викрадання та знищення даних, що може призвести до події, спричиненої програмою-вимагачем. Незвичайні закономірності подій входу в підтримувані версії двигунів баз даних Amazon Aurora та Amazon RDS, що свідчать про аномальну поведінку;

- несанкціонована діяльність з криптомайнінгу у корпоративних екземплярах Amazon Elastic Compute Cloud (Amazon EC2) та робочих навантаженнях контейнерів;

- наявність шкідливого програмного забезпечення у корпоративних екземплярах Amazon EC2 та робочих навантаженнях контейнерів, а також нещодавно завантажені файли у корпоративних корзинах Amazon Simple Storage Service (Amazon S3);

- події на рівні операційної системи, мережі та файлів, що вказують на несанкціоновану поведінку у корпоративних кластерах Amazon Elastic Kubernetes Service (Amazon EKS), завданнях Amazon Elastic Container Service (Amazon ECS) – AWS Fargate, а також екземплярах Amazon EC2 та робочих навантаженнях

контейнерів.

Розглянемо основні функції, за допомогою яких рішення Amazon GuardDuty допомагає контролювати, виявляти та керувати потенційними загрозами у корпоративному середовищі AWS [5]:

Постійно контролює певні джерела даних та журнали подій:

виявлення базових загроз. Коли вмикається Amazon GuardDuty в обліковому записі AWS, GuardDuty автоматично починає отримувати базові джерела даних, пов'язані з цим обліковим записом. Ці джерела даних включають події керування AWS CloudTrail, журнали потоків VPC (з екземплярів Amazon EC2) та журнали DNS. Не потрібно вмикати нічого іншого, щоб Amazon GuardDuty почав аналізувати та обробляти ці джерела даних для створення пов'язаних із ними результатів перевірки безпеки;

розширене виявлення загроз. Ця функція виявляє багатоетапні атаки, що охоплюють базові джерела даних, різні типи ресурсів AWS та час в межах облікового запису AWS. В обліковому записі може бути кілька подій, які окремо не є явною загрозою. Однак, коли ці події спостерігаються в послідовності, що свідчить про підозрілу активність, Amazon GuardDuty ідентифікує її як послідовність атак. Amazon GuardDuty повідомляє вас, генеруючи пов'язаний тип пошуку послідовності атак, щоб надати детальну інформацію про спостережувану послідовність атак.

Розширене виявлення загроз автоматично вмикається для кожного облікового запису AWS після ввімкнення Amazon GuardDuty без жодних додаткових витрат. Ця функція не вимагає вмикання будь-якого плану захисту, орієнтованого на конкретний випадок використання. Однак, щоб розширити захист корпоративних ресурсів Amazon S3, Amazon GuardDuty рекомендує ввімкнути захист S3 у корпоративному обліковому записі. Це допоможе розширеному виявленню загроз виявляти багатоетапні атаки, які потенційно впливають на ваші ресурси Amazon S3;

плани захисту Amazon GuardDuty, орієнтовані на випадки використання для покращеної видимості виявлення загроз безпеці корпоративного середовища AWS,

Amazon GuardDuty пропонує спеціальні плани захисту, які ми можемо активувати. Плани захисту допомагають контролювати журнали та події з інших сервісів AWS. Ці джерела включають журнали аудиту EKS, активність входу RDS, події даних Amazon S3 у CloudTrail, томи EBS, моніторинг виконання в Amazon EKS, Amazon EC2 та Amazon ECS-Fargate, а також журнали активності мережі Lambda. GuardDuty об'єднує ці джерела журналів та подій під терміном Функції. Ми можемо будь-коли активувати один або кілька спеціалізованих планів захисту в підтримуваному регіоні AWS. Amazon GuardDuty почне моніторинг, обробку та аналіз активності на основі того, який план захисту ми активуємо (таблиця 2.1).

Таблиця 2.1

Перелік планів захисту Amazon GuardDuty [5]

План захисту	Опис
<u>Захист S3</u>	Виявляє потенційні ризики безпеки, такі як спроби витоку даних та знищення у корпоративних контейнерах Amazon S3.
<u>Захист EKS</u>	Моніторинг журналів аудиту EKS аналізує журнали аудиту Kubernetes з корпоративних кластерів Amazon EKS на наявність потенційно підозрілої та шкідливої діяльності.
<u>Моніторинг виконання</u>	Відстежує та аналізує події на рівні операційної системи на корпоративних Amazon EKS, Amazon EC2 та Amazon ECS (включно з AWS Fargate) для виявлення потенційних загроз під час виконання.
<u>Захист від шкідливого програмного забезпечення для EC2</u>	Виявляє потенційну наявність шкідливого програмного забезпечення шляхом сканування томів Amazon EBS, пов'язаних з корпоративними екземплярами Amazon EC2. Існує можливість використовувати цю функцію за запитом.
<u>Захист від шкідливого програмного забезпечення для S3</u>	Виявляє потенційну наявність шкідливого програмного забезпечення у щойно завантажених об'єктах у корпоративних корзинах Amazon S3.
<u>Захист RDS</u>	Аналізує та профілює вашу активність входу до RDS на наявність потенційних загроз доступу до підтримуваних баз даних Amazon Aurora та Amazon RDS.
<u>Захист Lambda</u>	Відстежує журнали активності мережі Lambda, починаючи з журналів потоку VPC, для виявлення загроз корпоративним функціям AWS Lambda. Прикладами цих потенційних загроз є криптомайнінг та зв'язок зі шкідливими серверами.

Керування середовищем з кількома обліковими записами.

Ми можемо керувати середовищем AWS з кількома обліковими записами, використовуючи або організації AWS (рекомендовано), або застарілий метод запрошення.

Генерування висновків безпеки для виявлених загроз.

Коли GuardDuty виявляє потенційні загрози безпеці, пов'язані з корпоративними ресурсами AWS, він починає генерувати результати пошуку даних безпеки, які надають інформацію про потенційно скомпрометований ресурс. Після ввімкнення GuardDuty у нашому обліковому записі генеруються зразки результатів пошуку, щоб переглянути пов'язані деталі результатів пошуку.

За допомогою GuardDuty ми також можемо використовувати скрипт тестування, який генерує певні результати безпеки GuardDuty, щоб зрозуміти, як переглядати результати GuardDuty та реагувати на них.

Оцінка та управління результатами виявлення проблем безпеки.

GuardDuty об'єднує дані щодо безпеки в усіх облікових записах і відображає результати на панелі інструментів «Зведення» в консолі GuardDuty. Ми також можемо отримати результати через API AWS Security Hub, інтерфейс командного рядка AWS або AWS SDK. Маючи цілісне уявлення про поточний стан безпеки, ми можемо виявити тенденції та потенційні проблеми, а також вжити необхідних заходів для їх усунення.

Інтеграція з пов'язаними службами безпеки AWS.

Щоб додатково проаналізувати та дослідити тенденції безпеки у корпоративному середовищі AWS, є можливість використання наступних сервісів безпеки AWS у поєднанні з GuardDuty [5]:

центр безпеки AWS – ця послуга надає повне уявлення про стан безпеки корпоративних ресурсів AWS і допомагає перевірити середовище AWS на відповідність стандартам галузі безпеки та передовим практикам. Це частково робиться шляхом використання, агрегації, упорядкування та визначення пріоритетів корпоративних даних щодо безпеки з кількох сервісів AWS (включно з Amazon Macie) та підтримуваних продуктів партнерської мережі AWS (APN).

Центр безпеки допомагає аналізувати тенденції безпеки та виявляти проблеми безпеки з найвищим пріоритетом у корпоративному середовищі AWS.

Amazon Detective – цей сервіс допомагає аналізувати, досліджувати та швидко виявляти першопричину виявлених проблем безпеки або підозрілої активності. Detective автоматично збирає дані журналів з корпоративних ресурсів AWS. Потім він використовує машинне навчання, статистичний аналіз та теорію графів для створення візуалізацій, які допомагають проводити швидше та ефективніше розслідування безпеки. Попередньо створені Detective агрегації даних, зведення та контекст допомагають аналізувати та визначати характер і масштаб потенційних проблем безпеки.

Amazon EventBridge – цей сервіс допомагає отримувати сповіщення та реагувати на результати перевірки безпеки GuardDuty майже в режимі реального часу. GuardDuty створює подію, коли результати перевірки змінюються. Ми можемо вибрати, як часто ми хочемо отримувати сповіщення від EventBridge.

2.2. Базові джерела даних для Amazon GuardDuty

GuardDuty використовує базові джерела даних для виявлення зв'язку з відомими шкідливими доменами та IP-адресами, а також для виявлення потенційно аномальної поведінки та несанкціонованої активності. Під час передачі від цих джерел до GuardDuty всі дані журналів шифруються. GuardDuty витягує різні поля з цих джерел журналів для профілювання та виявлення аномалій, а потім видаляє ці журнали [5].

Події керування AWS CloudTrail

AWS CloudTrail надає історію викликів AWS API для відповідного облікового запису, включаючи виклики API, здійснені за допомогою консолі керування AWS, AWS SDK, інструментів командного рядка та певних сервісів AWS. CloudTrail також допомагає нам визначити, які користувачі та облікові записи викликали AWS API для сервісів, що підтримують CloudTrail, вихідну IP-адресу, з якої були викликані виклики, та час, коли були викликані виклики [5].

GuardDuty відстежує події керування CloudTrail, також відомі як події площини керування. Ці події надають уявлення про операції керування, що виконуються над ресурсами у корпоративному обліковому записі AWS.

Нижче наведено приклади подій керування CloudTrail, які відстежує GuardDuty [5]:

- налаштування безпеки (AttachRolePolicyоперації IAM API);

- налаштування правил маршрутизації даних (операції CreateSubnet Amazon EC2 API);

- налаштування ведення журналу (операції CreateTrail API AWS CloudTrail).

Коли вмикається GuardDuty, він починає споживати події керування CloudTrail безпосередньо з CloudTrail через незалежний та дубльований потік подій та аналізує журнали подій CloudTrail.

GuardDuty не керує подіями CloudTrail і не впливає на існуючі конфігурації CloudTrail. Аналогічно, конфігурації CloudTrail не впливають на те, як GuardDuty використовує та обробляє журнали подій. Щоб керувати доступом до подій CloudTrail та їх збереженням, використовуйте консоль служби CloudTrail або API.

Розглянемо обробку GuardDuty глобальних подій AWS CloudTrail. Для більшості сервісів AWS події CloudTrail записуються в регіоні AWS, де вони створюються. Для глобальних сервісів, таких як AWS Identity and Access Management (IAM), AWS Security Token Service (AWS STS), Amazon Simple Storage Service (Amazon S3), Amazon CloudFront та Amazon Route 53 (Route 53), події генеруються лише в регіоні, де вони відбуваються, але мають глобальне значення.

Коли GuardDuty використовує події глобальної служби (GSE) CloudTrail із значеннями безпеки, такими як конфігурації мережі або дозволи користувачів, він реплікує ці події та обробляє їх у кожному регіоні, де ввімкнули GuardDuty. Така поведінка допомагає GuardDuty підтримувати профілі користувачів і ролей у кожному регіоні, що життєво важливо для виявлення аномальних подій [5].

Рекомендується увімкнути GuardDuty у всіх регіонах AWS, доступних у корпоративному обліковому записі AWS. Навіть якщо немає розгорнутих ресурсів у певних регіонах, увімкнення GuardDuty допоможе захистити обліковий запис від

потенційних загроз. Зловмисники можуть потенційно запускати атаки через глобальні сервіси (такі як IAM, AWS STS або Amazon CloudFront). Вони можуть спробувати створити несанкціоновані ресурси для використання в регіонах, де присутність обмежена. GuardDuty обробляє події глобальних сервісів у всіх регіонах, де ввімкнули сервіс, включаючи як регіони за замовчуванням, так і регіони, в яких ми ввімкнули сервіс за згодою. Це допомагає GuardDuty виявляти потенційно підозрілу активність у корпоративному обліковому записі AWS, включаючи регіони, де ми активно не використовуємо ресурси.

Журнали потоку VPC

Функція журналів потоку VPC в Amazon VPC фіксує інформацію про IP-трафік, що надходить до та з мережевих інтерфейсів, підключених до екземплярів Amazon Elastic Compute Cloud (Amazon EC2) у корпоративному середовищі AWS.

Коли ми вмикаємо GuardDuty, він негайно починає аналізувати журнали потоків VPC з екземплярів Amazon EC2 у корпоративному обліковому записі. Він використовує події журналу потоків VPC безпосередньо з функції журналів потоків VPC через незалежний та дубльований потік журналів потоків. Цей процес не впливає на жодну з корпоративних існуючих конфігурацій журналів потоків.

Захист Lambda

Lambda Protection – це додаткове доповнення Amazon GuardDuty. Наразі моніторинг активності мережі Lambda включає журнали потоку Amazon VPC з усіх функцій Lambda для корпоративного облікового запису, навіть тих, які не використовують мережу VPC. Щоб захистити функцію Lambda від потенційних загроз безпеці, потрібно налаштувати Lambda Protection у корпоративному обліковому записі GuardDuty.

Моніторинг виконання GuardDuty

Коли ми керуємо агентом безпеки (вручну або через GuardDuty) в EKS Runtime Monitoring або Runtime Monitoring for EC2 instances, і GuardDuty наразі розгорнуто на екземплярі Amazon EC2 та отримує типи подій середовища виконання Collected від цього екземпляра, GuardDuty не стягуватиме плату з корпоративного облікового запису AWS за аналіз журналів потоку VPC від цього

екземпляра Amazon EC2. Це допомагає GuardDuty уникнути подвійних витрат на використання в обліковому записі.

GuardDuty не керує корпоративними журналами потоків і не робить їх доступними у корпоративному обліковому записі. Щоб керувати доступом до журналів потоків та їх збереженням, необхідно налаштувати функцію журналів потоків VPC.

Журнали DNS-запитів Route53 Resolver

Якщо ми використовуємо DNS-резолвери AWS для своїх екземплярів Amazon EC2 (налаштування за замовчуванням), GuardDuty може отримувати доступ до журналів запитів DNS Route53 Resolver та обробляти їх через внутрішні DNS-резолвери AWS. Якщо ми використовуємо інший DNS-резолвер, такий як OpenDNS або GoogleDNS, або якщо ми налаштували власні DNS-резолвери, GuardDuty не може отримувати доступ до даних з цього джерела даних та обробляти їх.

Коли ми вмикаємо GuardDuty, він негайно починає аналізувати журнали DNS-запитів Route53 Resolver з незалежного потоку даних. Цей потік даних окремий від даних, що надаються через функцію журналювання запитів Route 53 Resolver . Налаштування цієї функції не впливає на аналіз GuardDuty.

2.3. Порядок функціонування рішення Amazon GuardDuty

Amazon GuardDuty – це служба виявлення загроз, яка постійно відстежує шкідливу активність та несанкціоновану поведінку для захисту корпоративних облікових записів AWS, робочих навантажень та даних, що зберігаються в хмарі. Вона використовує машинне навчання, виявлення аномалій та інтегровану аналітику загроз для виявлення та визначення пріоритетів потенційних загроз. GuardDuty аналізує різні джерела даних, такі як журнали потоків VPC, журнали подій CloudTrail та журнали DNS, що дозволяє їй виявляти такі дії, як незвичайні виклики API, потенційно несанкціоновані розгортання та зв'язок зі шкідливими IP-адресами [4].

GuardDuty можна інтегрувати з іншими сервісами AWS, такими як AWS Security Hub, Amazon CloudWatch та сторонніми інструментами SIEM, для автоматизації реагування та покращення загальної безпеки.

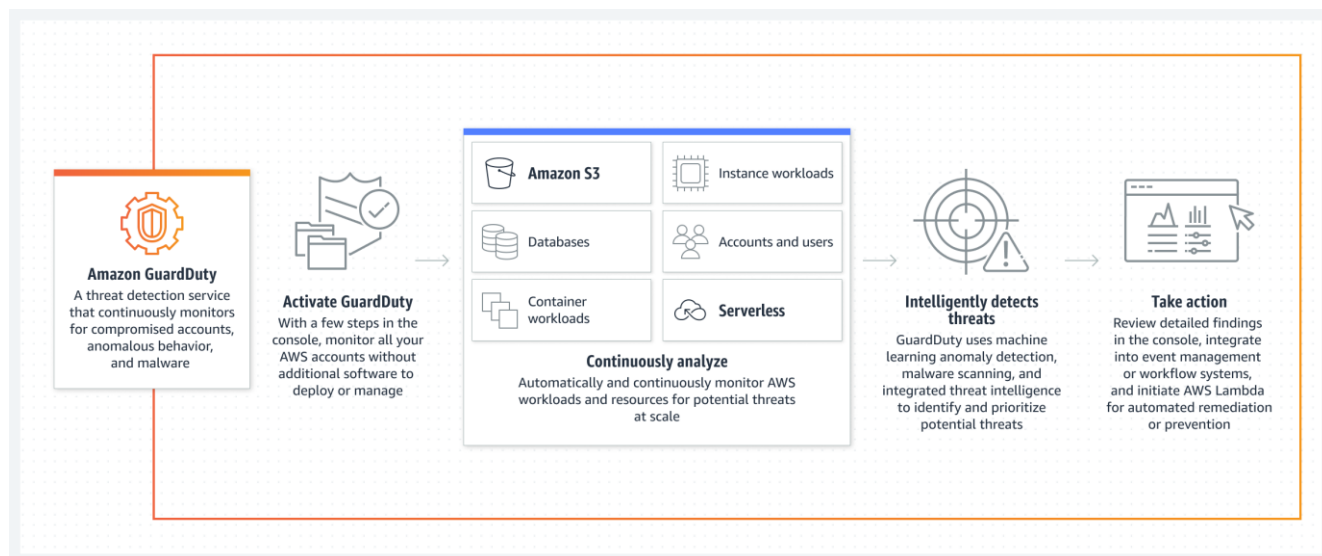


Рис. 2.1. Основні функції Amazon GuardDuty [4]

GuardDuty автоматично агрегує та співвідносить ці дані з усіх пов'язаних облікових записів AWS, консолідуючи та визначаючи пріоритет потенційних загроз як низький, середній або високий пріоритет.

Первинні категорії виявлення включають [4]:

розвідка: виявляє таку діяльність, як незвичайна активність API, підозрілі входи в базу даних, сканування портів всередині VPC, невдалі шаблони входу та зондування портів з відомих шкідливих IP-адрес;

компрометація екземпляра: виявляє такі ознаки, як майнінг криптовалют, дії командування та контролю, шкідливе програмне забезпечення, вихідні атаки типу «відмова в обслуговуванні», високий мережевий трафік, незвичайні мережеві протоколи та зв'язок зі шкідливими IP-адресами за допомогою облікових даних Amazon Elastic Compute Cloud (EC2);

компрометація облікового запису: відстежує виклики API з нетипових геолокацій або проксі-серверів, спроби вимкнення журналювання CloudTrail, зміни політики слабких паролів, незвичайні запуски та виклики зі шкідливих IP-адрес;

компрометація Bucket: спостерігає за Amazon S3 на наявність незвичайного доступу до даних, несанкціонованого доступу та викликів API, що свідчить про потенційне неправомірне використання облікових даних;

шкідливе програмне забезпечення: виявляє шкідливе програмне забезпечення на екземплярах EC2 або робочих навантаженнях контейнерів, включаючи троянів, черв'яків та криптомайнери;

компрометація контейнера: аналізує Amazon EKS та ECS, відстежуючи журнали аудиту EKS та дії під час виконання контейнера, щоб виявити підозрілу поведінку в робочих навантаженнях контейнера.

Основні переваги Amazon GuardDuty включають [4]:

безперервне виявлення загроз на базі машинного навчання: використовує машинне навчання, виявлення аномалій, моделювання поведінки та сторонні аналітичні дані про загрози для швидкого виявлення загроз у корпоративних облікових записах AWS. Це дозволяє швидше реагувати та мінімізувати вплив інцидентів безпеки до їх ескалації;

виявлення підозрілої активності робочого навантаження ІІІ: виявляє аномальну поведінку, таку як видалення захисних бар'єрів ІІІ, незвичне використання моделі або неправильне використання облікових даних EC2 в Amazon Bedrock, Amazon SageMaker або інших платформах ІІІ;

покращений захист від шкідливого програмного забезпечення: автоматично сканує томи Amazon EBS та відстежує завантаження даних у корзини Amazon S3 для виявлення шкідливого програмного забезпечення, включаючи програми-вимагачі, вторгнення через бекдор та дії, пов'язані з криптовалютою;

централізоване виявлення загроз для контейнерів: забезпечує єдине рішення для управління загрозами в контейнерному середовищі AWS, включаючи Amazon Elastic Kubernetes Service (EKS) та Elastic Container Service (ECS), як для екземплярів, так і для безсерверних контейнерних робочих навантажень;

підтримка відповідності: допомагає у виконанні вимог відповідності, таких як PCI DSS, демонструючи надійні можливості виявлення вторгнень;

інтеграції AWS для розслідування та усунення недоліків: надає детальні

результати з контекстом та метаданими. Інтегрується з Amazon Detective для аналізу першопричин та направляє сповіщення до AWS Security Hub та Amazon EventBridge для оптимізованого усунення недоліків.

Місце рішення Amazon GuardDuty в загальній архітектурі AWS показано на рисунку 2.2.



Рис. 2.2. Місце рішення Amazon GuardDuty в загальній архітектурі AWS [8]

Вхідні дані Amazon GuardDuty включають [8]:

журнали подій CloudTrail – незвичайні виклики API, несанкціоновані розгортання;

журнали подій керування CloudTrail – створення VPC, підмережі, створення сліду;

події даних Cloud Trail S3 – отримання об’єкта, перелік об’єктів, видалення об’єктів;

журнали потоку VPC – незвичайний внутрішній трафік, незвичайна IP-адреса;

журнали DNS – скомпрометовані екземпляри EC2, що надсилають закодовані дані за допомогою DNS;

журнали аудиту Kubernetes – підозріла активність та компрометація кластера EKS.

Розглянемо зміст технології інтелектуального виявлення загроз хмарним корпоративним ресурсам на основі Amazon GuardDuty на прикладі виявлення

аномалій у поведінці користувачів та ресурсів. Процес можна розділити на три ключові етапи:

Етап 1. Збір та аналіз даних. Amazon GuardDuty не втручається у роботу корпоративних ресурсів і не впливає на їхню продуктивність. Замість цього він "тихо" аналізує величезні потоки даних з трьох основних джерел:

журнали AWS CloudTrail: фіксується кожен виклик API: хто, що, коли і звідки зробив. Це основне джерело для аналізу поведінки користувачів та ролей;

журнали VPC Flow Logs: це інформація про весь мережевий трафік, що входить і виходить з корпоративних віртуальних мереж (VPC). GuardDuty аналізує, хто з ким спілкується, які порти та протоколи використовуються. Це ключові дані для аналізу поведінки ресурсів, таких як EC2-інстанси;

DNS-логи: це записи про те, до яких доменних імен звертаються корпоративні ресурси. Аналіз цих журналів допомагає виявити комунікацію зі шкідливими серверами (наприклад, командними центрами ботнетів).

Етап 2. Створення базової лінії поведінки. Після активації GuardDuty починає процес навчання, формуючи модель нормальної, очікуваної активності для корпоративного середовища. Ця базова лінія є унікальною для кожного акаунту і включає в себе патерни поведінки як для користувачів, так і для ресурсів.

Щодо поведінки користувачів (IAM Users/Roles) моделі машинного навчання аналізують такі аспекти:

типові API-виклики: які сервіси та дії зазвичай виконує певний користувач чи роль? (Наприклад, розробник часто працює з Lambda та API Gateway, а роль для EC2 – з S3);

геолокація та IP-адреси: з яких країн, міст чи мереж зазвичай надходять запити;

час активності: в які дні тижня та години користувач зазвичай активний;

використовувані інструменти: чи використовує користувач AWS CLI, консоль, чи певний SDK?

Щодо поведінки ресурсів (EC2, контейнери тощо) моделі машинного навчання аналізують такі аспекти:

мережеві з'єднання: з якими IP-адресами та по яких портах зазвичай комунікує EC2-інстанс? Чи є стабільні патерни трафіку?

обсяг трафіку: скільки даних зазвичай відправляється чи отримується?

DNS-запити: до яких доменів ресурс звертається для оновлень, отримання даних тощо?

Етап 3. Виявлення аномалій та відхилень. Це найважливіший етап, де GuardDuty порівнює поточну активність із вивченою базовою лінією. Якщо фіксується значне відхилення, сервіс генерує знахідку (finding).

Ось конкретні приклади аномалій, які Amazon GuardDuty може виявити:

Приклади аномалій у поведінці користувачів:

незвичні API-виклики – IAM-користувач, який зазвичай працює лише з базами даних (RDS), раптом починає робити виклики для вимкнення логування в CloudTrail (StopLogging) або створення знімків баз даних. Це класична ознака скомпрометованого акаунту;

вхід з нетипової локації: адміністратор, який завжди підключається з України, раптом робить запит з IP-адреси, що належить до іншої країни, та ще й у неробочий час;

«неможлива подорож» (Impossible Travel): API-ключ був використаний спочатку в Києві, а через 5 хвилин – у Сінгапурі. Фізично це неможливо, що свідчить про викрадення облікових даних;

спроби приховати сліди: користувач намагається видалити логи або вимкнути механізми безпеки.

Приклади аномалій у поведінці ресурсів:

незвичний мережевий трафік: веб сервер, який зазвичай спілкується лише з користувачами по портах 80/443, раптом починає відправляти великі обсяги даних на невідому IP-адресу по нестандартному порту. Це може свідчити про витік даних;

комунікація з відомими шкідливими IP: EC2-інстанс встановлює з'єднання з IP-адресою, яка відома як командний центр (C&C) для майнінгу криптовалют;

сканування портів: один з корпоративних EC2-інстансів починає масово сканувати порти інших ресурсів у корпоративній VPC. Це може означати, що інстанс скомпрометовано і зловмисник проводить розвідку всередині мережі.

Таким чином, машинне навчання в GuardDuty – це не просто набір статичних правил, а динамічна система, що постійно адаптується. Вона вчиться, що є нормальним саме для конкретних ресурсів, і завдяки цьому може ефективно виявляти складні та раніше невідомі загрози, які неможливо знайти за допомогою традиційного сигнатурного аналізу.

3 ТЕХНОЛОГІЯ ІНТЕЛЕКТУАЛЬНОГО ВИЯВЛЕННЯ ЗАГРОЗ ХМАРНИМ КОРПОРАТИВНИМ РЕСУРСАМ НА БАЗІ AMAZON GUARDDUTY

3.1. Порядок застосування рішення Amazon GuardDuty

Необхідно відмітити, що рішення AWS GuardDuty – це керована служба безпеки, яка постійно моніторить корпоративне середовище AWS на наявність потенційних загроз, аналізуючи дані з таких джерел, як CloudTrail, журнали потоків VPC та журнали DNS. Вона використовує машинне навчання та розвідку загроз для виявлення аномалій та підозрілої активності, такої як спроби несанкціонованого доступу, незвичайні передачі даних або випадки компрометації [6].

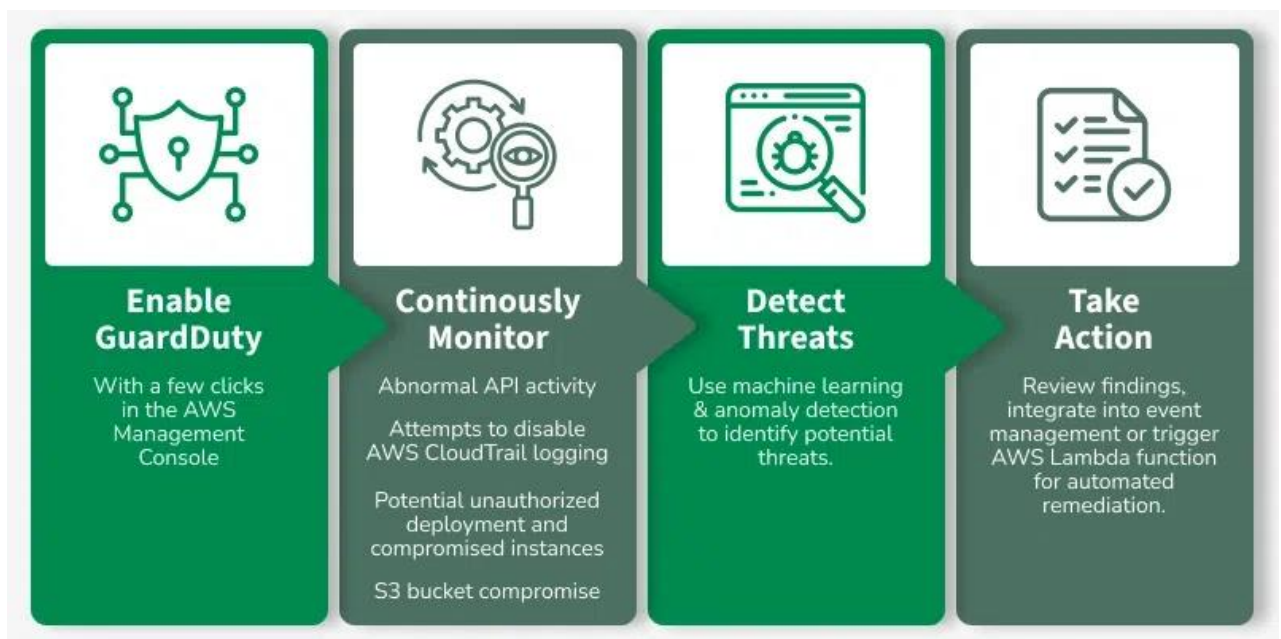


Рис. 3.1. Реалізація інтелектуального виявлення загроз хмарним корпоративним ресурсам на базі Amazon GuardDuty [6]

Безпека стає головним фактором, коли користувачі зберігають свої дані в хмарі. Усі хочуть, щоб їхні дані були в безпеці. Тому вони шукають платформу, яка також є економічно ефективною, а послуги, що надаються ними, можуть захистити

їхні дані.

Amazon GuardDuty може безперервно контролювати кілька облікових записів одночасно без додаткових витрат та складності. Він може автоматично реагувати та усувати загрозу. Amazon GuardDuty може всебічно виявляти загрози. Він постійно відстежує вхідні дані та мережеву активність для досягнення кращих результатів, використовуючи інші сервіси AWS.

Amazon GuardDuty посилює безпеку за рахунок автоматизації. Оскільки здатний автоматично реагувати на виявлення загроз, він може вживати коригувальних заходів, використовуючи події Amazon Cloudwatch та інші сервіси. Він може централізовано керувати всіма новими обліковими записами користувачів та існуючими обліковими записами.

Amazon GuardDuty постійно аналізує хмарні події, використовуючи численні інші сервіси AWS, такі як журнали подій AWS CloudTrail, журнали потоків Amazon Virtual Private Cloud (VPC) та журнали системи доменних імен (DNS) для аналізу шкідливої діяльності.

Amazon GuardDuty може виявити три типи об'єктів [6]:

скомпрометовані облікові записи. Це загроза, за якої особа не має доступу до облікового запису, але використовує його несанкціонованими засобами. У хмарі ці загрози включають виклики API з дивного місця та спроби внести зміни в інфраструктуру або вимкнути CloudTrail, щоб створити перешкоду для аналізу журналу даних;

розвідка зловмисника. Вона включає загрозу, за якої атаки починаються зі сканування мережі з зараженої кінцевої точки, щоб знайти актив і служби, на які зловмисник хоче націлитися, що в основному називається скануванням портів.

скомпрометовані ресурси. Це, по суті, загроза, при якій ресурси, такі як екземпляри EC2, викрадаються зовнішньою IP-адресою, і спостерігаються незвичайні сплески мережевого трафіку.

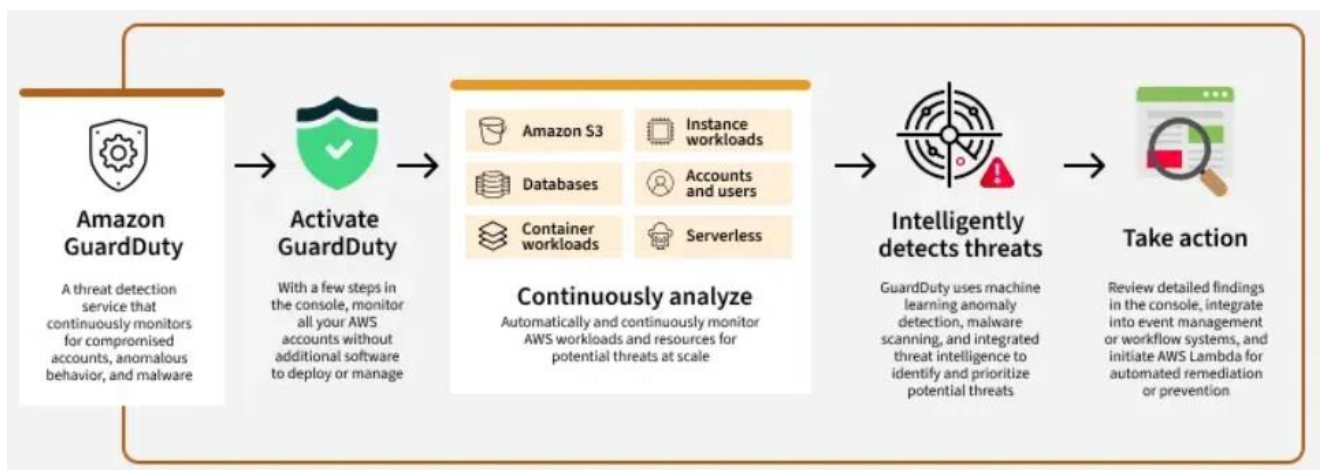


Рис. 3.2. Процеси функціонування Amazon GuardDuty [6]

Адміністратор Amazon GuardDuty повинен надати свої IP-адреси для виявлення загрози, оскільки GuardDuty не має функції налаштованих правил виявлення підтримки. Для ефективнішої роботи користувачі можуть реагувати на оцінки «вгору» або «вниз», надані GuardDuty, щоб покращити роботу. У консолі керування це у форматі JSON, що дозволяє користувачеві вживати заходів, ідентифікуючи загрозу, виявлену GuardDuty.

Централізоване керування Amazon GuardDuty дозволяє контролювати кілька облікових записів за допомогою Amazon GuardDuty. Ми можемо об'єднати всі свої облікові записи в один обліковий запис адміністратора Amazon GuardDuty для зручності та цілей управління. Це корисно, коли йдеться про велике підприємство з окремою командою безпеки, щоб вони могли безпосередньо зосередитися на цьому для всього бізнесу.

Повна автоматизація процесів функціонування – нам потрібно лише вказати свої IP-адреси і всього за кілька кліків ми можемо активувати цю функцію, не турбуючись про обладнання, конфігурацію, налаштування чи управління.

Реалізується комплексна ідентифікація загроз. Amazon GuardDuty постачається з сучасними інтегрованими методами та інструментами розвідки загроз для моніторингу корпоративних даних. Це допомагає відстежувати неочікуваний, незвичайний доступ до корпоративних даних, криптовалют та інші зловмисні дії.

Amazon GuardDuty – це цінний інструмент для підвищення безпеки середовищ AWS шляхом постійного моніторингу потенційних загроз, несанкціонованого доступу та незвичайної активності. Його інтеграція з машинним навчанням та розвідкою загроз дозволяє виявляти широкий спектр проблем безпеки, від скомпрометованих екземплярів до ризиків витоку даних.

3.2. Технологія інтелектуального виявлення загроз хмарним корпоративним ресурсам на базі Amazon GuardDuty

Розширене виявлення загроз Amazon GuardDuty автоматично виявляє багатоетапні атаки, що охоплюють джерела даних, різні типи ресурсів AWS та час в межах облікового запису AWS. Завдяки цій можливості Amazon GuardDuty зосереджується на послідовності кількох подій, які він спостерігає, моніторячи різні типи джерел даних. Розширене виявлення загроз співвідносить ці події, щоб визначити сценарії, які представляють собою потенційну загрозу для корпоративного середовища AWS, а потім генерує результати пошуку послідовності атак [5].

Розширене виявлення загроз охоплює сценарії загроз, що включають компрометацію, пов'язану з неправильним використанням облікових даних AWS, спробами компрометації даних у корзинах Amazon S3, а також компрометацією контейнерів і ресурсів Kubernetes у кластерах Amazon EKS. Одна знахідка може охоплювати цілу послідовність атак. Наприклад, у наступному списку описано сценарії, які може виявити GuardDuty [5]:

приклад 1: компрометація облікових даних AWS та даних корзини Amazon S3. Зловмисник отримує несанкціонований доступ до обчислювального навантаження. Потім актор виконує серію дій, таких як ескалація привілеїв та встановлення стійкості. Зрештою, актор витягує дані з ресурсу Amazon S3;

приклад 2: компрометація кластера Amazon EKS. Зловмисник намагається використати контейнерний застосунок у кластері Amazon EKS. Актор використовує цей скомпрометований контейнер для отримання токенів

привілейованого облікового запису служби. Потім актор використовує ці підвищені привілеї для доступу до конфіденційних секретів Kubernetes або ресурсів AWS через ідентифікатори подів.

Через характер пов'язаних сценаріїв загроз, Amazon Guard Duty вважає всі типи пошуку послідовностей атак критичними.

Коли ми вмикаємо Amazon GuardDuty у своєму обліковому записі в певному регіоні AWS, розширене виявлення загроз також вмикається за замовчуванням. Використання розширеного виявлення загроз не передбачає додаткових витрат. За замовчуванням воно співвідносить події з усіма джерелами даних Foundational. Однак, якщо ми вмикаємо більше планів захисту Amazon GuardDuty, таких як S3 Protection, EKS Protection та Runtime Monitoring, це відкриє додаткові типи виявлення послідовностей атак, розширивши діапазон джерел подій. Це потенційно може допомогти з більш повним аналізом загроз та кращим виявленням послідовностей атак.

Amazon GuardDuty співвідносить кілька подій, включаючи дії API та результати Amazon GuardDuty. Ці події називаються *сигналами*. Іноді у корпоративному середовищі можуть бути події, які самі по собі не є явною потенційною загрозою. Amazon GuardDuty називає їх слабкими сигналами. Завдяки розширеному виявленню загроз Amazon GuardDuty визначає, коли послідовність кількох дій збігається з потенційно підозрілою активністю, і генерує послідовність виявлених атак у нашому обліковому записі. Ці кілька дій можуть включати слабкі сигнали та вже виявлені результати Amazon GuardDuty у нашому обліковому записі.

Під час співвіднесення подій для послідовностей атак розширене виявлення загроз не враховує архівовані результати, зокрема ті, що автоматично архівуються через правила придушення. Така поведінка гарантує, що лише активні, релевантні сигнали сприяють виявленню послідовності атак.

Amazon GuardDuty також розроблений для виявлення потенційних поточних або нещодавніх атак (протягом 24-годинного періоду) у нашому обліковому записі. Наприклад, атака може розпочатися з отримання суб'єктом ненавмисного доступу

до обчислювального навантаження. Потім суб'єкт виконує низку кроків, включаючи перерахування, ескалацію привілеїв та викрадання облікових даних AWS. Ці облікові дані потенційно можуть бути використані для подальшої компрометації або зловмисного доступу до даних.

Розглянемо порядок забезпечення планів захисту для максимізації виявлення загроз.

Для будь-якого облікового запису Amazon GuardDuty у регіоні функція розширеного виявлення загроз вмикається автоматично. За замовчуванням ця функція враховує численні події у всіх базових джерелах даних. Щоб скористатися цією можливістю, нам не потрібно вмикати всі плани захисту Amazon GuardDuty, орієнтовані на конкретний випадок використання. Наприклад, за допомогою базового виявлення загроз GuardDuty може ідентифікувати потенційну послідовність атак, починаючи з активності виявлення привілеїв IAM на API Amazon S3, і виявляти подальші зміни площини керування S3, такі як зміни, що роблять політику ресурсів корзини більш дозвоільною.

Розширене виявлення загроз розроблено таким чином, що якщо ми вмикаємо більше планів захисту, це допоможе Amazon GuardDuty співвідносити більш різноманітні сигнали з кількох джерел даних. Це потенційно розширить спектр сигналів безпеки для комплексного аналізу загроз та охоплення послідовностей атак. Щоб виявляти результати, які потенційно можуть бути одним із кількох етапів послідовності атак в Amazon GuardDuty рекомендується ввімкнути спеціальні плани захисту – захист S3, захист EKS та моніторинг виконання (з доповненням EKS).

Розглянемо виявлення послідовностей атак у кластерах Amazon EKS.

Amazon GuardDuty співвідносить кілька сигналів безпеки з журналів аудиту EKS, поведінки процесів під час виконання та активності API AWS для виявлення складних шаблонів атак. Щоб скористатися перевагами розширеного виявлення загроз для EKS, необхідно ввімкнути принаймні одну з цих функцій – захист EKS або моніторинг середовища виконання (з доповненням EKS). Захист EKS відстежує діяльність площини керування за допомогою журналів аудиту, тоді як моніторинг

середовища виконання спостерігає за поведінкою в контейнерах.

Для максимального покриття та комплексного виявлення загроз GuardDuty рекомендує увімкнути обидва плани захисту. Разом вони створюють повне уявлення про корпоративні кластери EKS, що дозволяє GuardDuty виявляти складні схеми атак. Наприклад, він може виявити аномальне розгортання привілейованого контейнера (виявлене за допомогою EKS Protection), а потім спроби збереження, криптомайнінг та створення зворотної оболонки в цьому контейнері (виявлене за допомогою Runtime Monitoring). GuardDuty представляє ці пов'язані події як єдину знахідку критичного рівня під назвою *AttackSequence:EKS/CompromisedCluster*. Коли ми вмикаємо обидва плани захисту, пошук послідовності атак охоплює такі сценарії загроз:

- компрометація контейнерів, на яких працюють вразливі веб-застосунки;
- несанкціонований доступ через неправильно налаштовані облікові дані;
- спроби посилення привілеїв;
- підозрілі запити API;
- спроби зловмисного доступу до даних.

Розглянемо захист EKS. Увімкнення захисту EKS надає Amazon GuardDuty можливість виявляти послідовності атак, що стосуються діяльності площини керування кластером Amazon EKS. Це дозволяє Amazon GuardDuty співвідносити журнали аудиту EKS та активність API AWS. Наприклад, Amazon GuardDuty може виявляти послідовність атак, коли актор намагається отримати несанкціонований доступ до секретів кластера, змінює дозволи керування доступом на основі ролей (RBAC) Kubernetes та створює привілейовані pod-системи.

Увімкнення моніторингу середовища виконання для кластерів Amazon EKS надає Amazon GuardDuty можливість покращити виявлення послідовностей атак EKS завдяки видимості на рівні контейнера. Це допомагає Amazon GuardDuty виявляти потенційно шкідливі процеси, підозрілу поведінку під час виконання та потенційне виконання шкідливого програмного забезпечення. Наприклад, GuardDuty може виявляти послідовність атак, коли контейнер починає демонструвати підозрілу поведінку, таку як процеси криптомайнінгу або

встановлення з'єднань із відомими шкідливими кінцевими точками.

Якщо ми не вмикаємо захист EKS або моніторинг середовища виконання, GuardDuty не зможе генерувати окремі типи результатів захисту EKS або моніторингу середовища виконання. Таким чином, GuardDuty не зможе виявляти багатостадійні послідовності атак, що включають пов'язані результати.

Розглянемо порядок виявлення послідовностей атак у корзинах Amazon S3.

Увімкнення захисту S3 надає GuardDuty можливість виявляти послідовності атак, що включають спроби компрометації даних у корпоративних корзинах Amazon S3. Без захисту S3 GuardDuty може виявляти, коли політика ресурсів корпоративної корзини S3 стає надмірно дозвоільною. Коли ми вмикаємо захист S3, GuardDuty отримує можливість виявляти потенційні дії з витоку даних, які можуть відбуватися після того, як корзина S3 стає надмірно дозвоільною.

Якщо захист S3 не увімкнено, GuardDuty не зможе генерувати окремі типи результатів S3 Protection. Таким чином, GuardDuty не зможе виявляти багатостадійні послідовності атак, що включають пов'язані результати.

Розглянемо розширене виявлення загроз у консолі GuardDuty. За замовчуванням на сторінці розширеного виявлення загроз у консолі GuardDuty відображається статус «Увімкнено». При виявленні базових загроз цей статус означає, що GuardDuty може виявити потенційну послідовність атак, що включає активність виявлення привілеїв IAM на API Amazon S3 та подальші зміни площини керування S3.

Результати послідовності атак такі ж, як і інші результати GuardDuty у нашому обліковому записі. Ми можемо переглянути їх на сторінці «Результати» в консолі GuardDuty.

Подібно до інших результатів GuardDuty, результати послідовностей атак також автоматично надсилаються до Amazon EventBridge. Залежно від наших налаштувань, результати послідовностей атак також експортуються до місця призначення публікації (кошик Amazon S3).

Розглянемо більш детально функцію в Amazon Guard Duty під назвою «розширене виявлення загроз». Ця функція використовує штучний інтелект та

машинне навчання, щоб допомогти нам зрозуміти послідовності атак, що охоплюють різні джерела даних, періоди часу та допомагає нам ідентифікувати загрози з найвищим пріоритетом у корпоративному хмарному середовищі.

Розширена функція виявлення загроз працює, навіть якщо ми ввімкнули базове виявлення загроз Amazon Guard Duty без додаткових планів захисту. Однак ми отримаємо вищий рівень безпеки, коли ввімкнемо спеціалізовані плани захисту Guard Duty. Це допоможе Guard Duty співвідносити більш різноманітні сигнали з різних джерел даних.

Amazon Guard Duty є службою моніторингу безпеки, яка аналізує та обробляє базові джерела даних, такі як події управління хмарними трасами AWS, журнали потоку VPC з екземплярів Amazon EC2 та журнали DNS. Вона також обробляє журнали аудиту Kubernetes, активність входу RDS, події даних S3, томи EBS, моніторинг часу виконання та журнали активності мережі Lambda. Вона використовує інформацію про загрози, таку як список IP-адрес, шкідливих IP-доменів та машинне навчання для виявлення неочікуваної потенційно несанкціонованої та шкідливої активності у корпоративному середовищі AWS.

Потім Guard Duty надає нам фактичні результати, щоб ми могли виправити цю активність. Розширене виявлення загроз співвідносить кілька сигналів з часом, щоб представити цілісне уявлення про потенційні загрози безпеці. Ця функція вводить два нових типи виявлення: один для компрометації даних, а інший для компрометації облікових даних.

Що відрізняє розширене виявлення загроз, так це його здатність, по-перше, швидко ідентифікувати складні послідовності атак, що охоплюють кілька ресурсів, джерел даних та періодів часу. По-друге, воно автоматично співвідносить різні сигнали, щоб забезпечити високонадійну аналітику та потенційно поставити під загрозу ресурси. По-третє, щоб скоротити час і зусилля, необхідні командам безпеки для сортування подій.

Важливо, що виявлені послідовності атак класифікуються як критично серйозні, що вказує на високу ймовірність загроз, які потребують негайної уваги. Ця пріоритезація допомагає командам безпеки зосередитися на найнагальніших

питаннях. Крім того, розширене виявлення загроз забезпечує зіставлення незначних атак для кожного виявлення. Ці зіставлення забезпечують стандартизовану основу для розуміння тактик і методів, що використовуються в послідовності атак, що дозволяє проводити більш комплексний аналіз загроз для подальшої допомоги командам безпеки.

Ця функція також надає рекомендації щодо усунення наслідків на основі найкращих практик AWS. Це керівництво допомагає оптимізувати процес реагування та гарантує, що команди дотримуються провідних протоколів безпеки.

На рисунку 3.3. показано консоль Amazon Guard Duty. За типом загрози, послідовністю атак, результатами ми можемо переглянути всі результати або вказати, що ми хочемо переглянути лише результати послідовності атак.

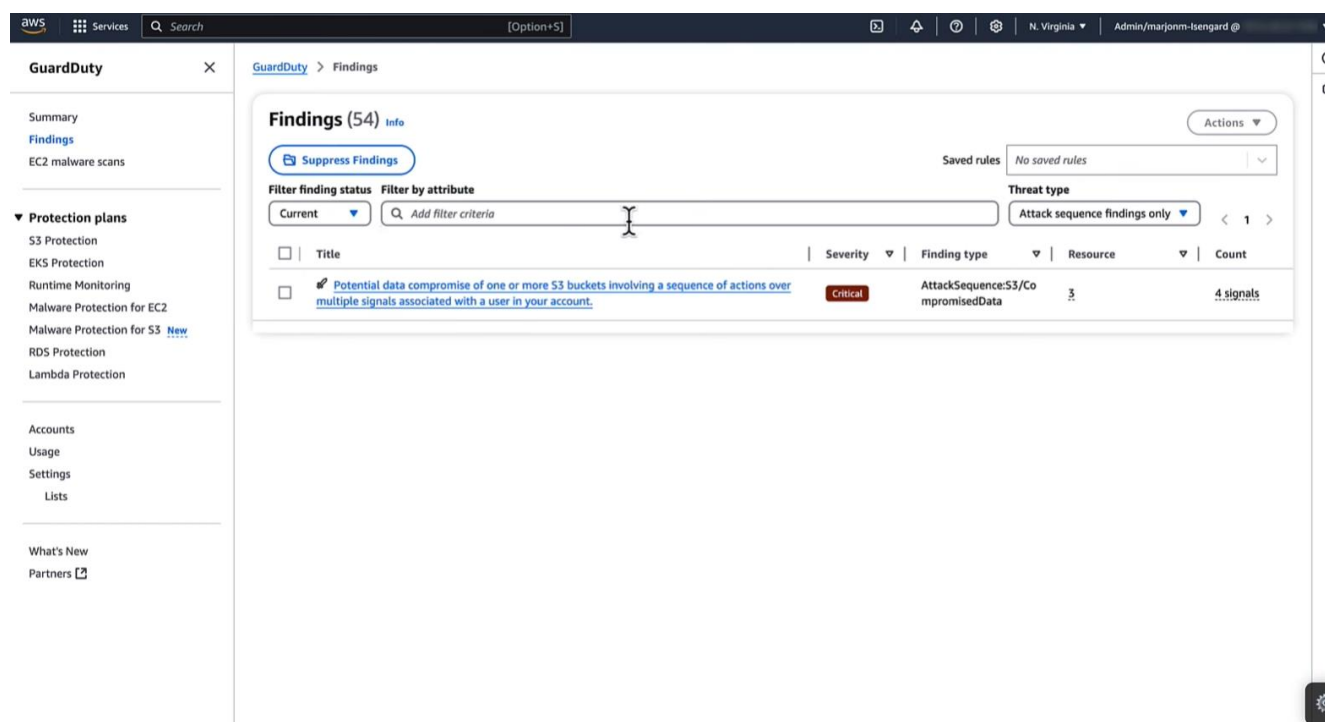


Рис. 3.3. Консоль Amazon Guard Duty

Ми можемо бачити, що у нас є результат *потенційної компрометації даних одного або кількох кошиків S3*, що включає послідовність дій за кількома сигналами, пов'язаними з користувачем у корпоративному обліковому записі. Серйозність є критичною, як ми вже казали, ці ступені серйозності послідовності атак є критичними. Є три задіяні ресурси та чотири сигнали.

Ми можемо отримати оглядову інформацію в правій частині екрана (рисунок 3.4), таку як деталі, пов'язані зі знахідкою або цією послідовністю атаки, знаходячи учасників, причетних до деяких інших деталей, пов'язаних зі знахідкою. Для цього, ми натискаємо «Переглянути деталі» та заглиблюємося в деталі.

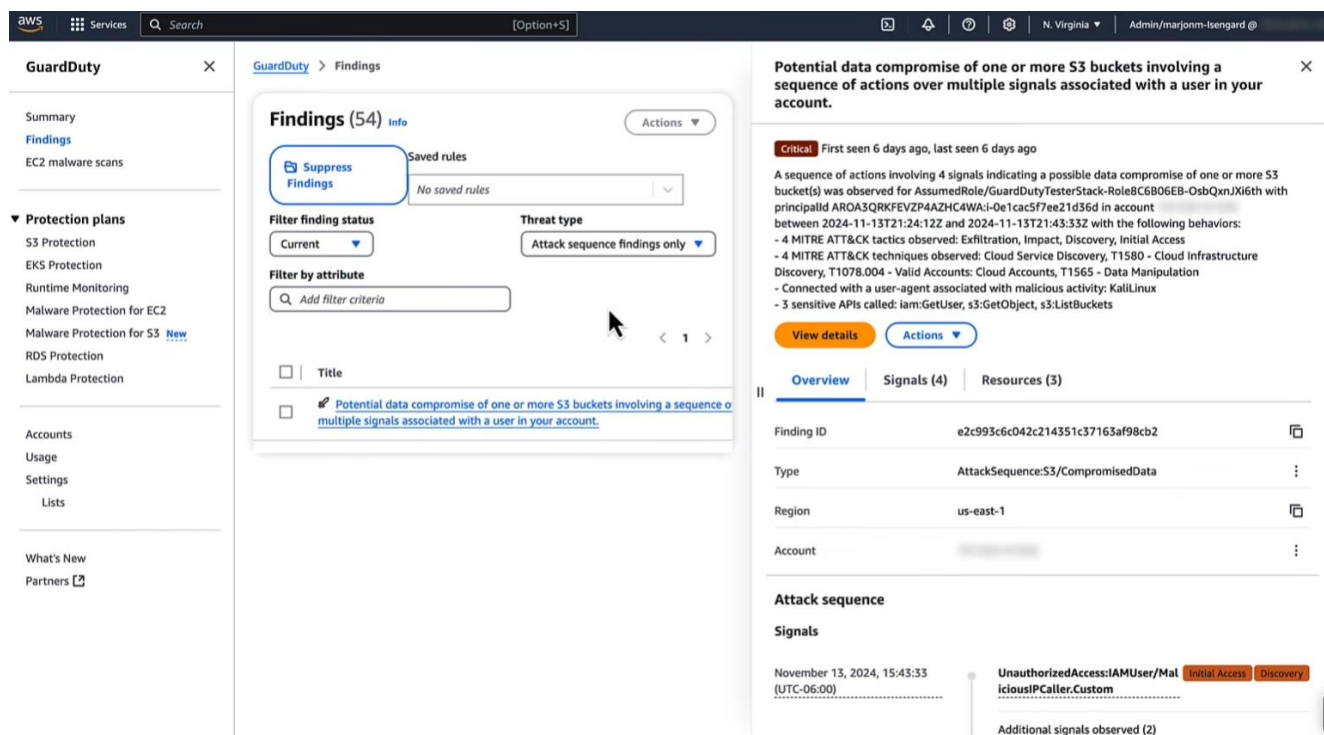


Рис. 3.4. Оглядова інформація про подію безпеки

Ми можемо побачити, що оглядова інформація має набагато більше деталей, і що вона говорить нам, що є чотири сигнали (рисунок 3.5), які вказують на можливу компрометацію даних одного або кількох кошиків S3. Ми можемо побачити передбачувану роль, частиною якої це було, в ідентифікаторі учасника. Ми можемо бачити часові рамки, протягом яких ця активність відбулася. Ми знаємо, що це повідомляє нам, що спостерігалися чотири незначні тактики атаки: викриття, вплив, виявлення та початковий доступ.

GuardDuty ×

Summary
Findings
EC2 malware scans

▼ **Protection plans**
S3 Protection
EKS Protection
Runtime Monitoring
Malware Protection for EC2
Malware Protection for S3 **New**
RDS Protection
Lambda Protection

Accounts
Usage
Settings
Lists

What's New
Partners

GuardDuty > Findings > Finding details

Potential data compromise of one or more S3 buckets involving a sequence of actions over multiple signals associated with a user in your account.

Critical First seen 6 days ago, last seen 6 days ago

Actions

A sequence of actions involving 4 signals indicating a possible data compromise of one or more S3 bucket(s) was observed for AssumedRole/GuardDutyTesterStack-Role8C6B06EB-05bQxnJXi6th with principalId AROA3QRKFEVZP4AZHC4WA-i-0e1cac5f7ee21d36d in account

between 2024-11-13T21:24:12Z and 2024-11-13T21:43:33Z with the following behaviors:

- 4 MITRE ATT&CK tactics observed: Exfiltration, Impact, Discovery, Initial Access
- 4 MITRE ATT&CK techniques observed: Cloud Service Discovery, T1580 - Cloud Infrastructure Discovery, T1078.004 - Valid Accounts: Cloud Accounts, T1565 - Data Manipulation
- Connected with a user-agent associated with malicious activity: KaliLinux
- 3 sensitive APIs called: iam:GetUser, s3:GetObject, s3:ListBuckets

Finding ID	e2c993c6c042c214351c37163af98cb2
Type	AttackSequence:S3/CompromisedData
Region	us-east-1
Account	

Attack sequence

MITRE tactics

Discovery Initial Access Execution Persistence Privilege Escalation
Defense Evasion Lateral Movement Credential Access Collection
Exfiltration Impact

Signals (4) **Resources (3)**

Sort by
Newest first

November 13, 2024

15:43:33 (UTC-06:00)

UnauthorizedAccess:IAMUser/MaliciousIPCaller:Custom Initial Access Discovery

Resources involved
Access Key: AROA3QRKFEVZP4AZHC4WA-i-0e1cac5f7ee21d36d
EC2 Instance: i-0e1cac5f7ee21d36d

► Indicators (2)

► Actors (1)

► Endpoints (1)

15:40:37 (UTC-06:00)

The API GetObject was invoked from an IP address on a custom threat list. Impact Exfiltration

Resources involved
Access Key: AROA3QRKFEVZP4AZHC4WA-i-0e1cac5f7ee21d36d

Рис. 3.5. Зміст сигналів інциденту безпеки

Ми бачимо, що існували такі методи, як хмарний сервіс, виявлення та маніпулювання даними. Ми також бачимо, що ця активність відбулася з користувацького агента, пов'язаного з користувацьким агентом Linux CI, і було кілька викликів API. Ми можемо побачити тут деяку інформацію про ресурс, таку як пошук ID в області типу облікового запису, що це сталося. Ми можемо побачити інформацію про послідовність атак відповідно до незначних тактик загалом для всієї послідовності атак, таких як виявлення, початковий доступ, викриття та вплив.

Якщо ми перейдемо до правої частини екрана, ми побачимо, що тут перелічені чотири сигнали, ми можемо побачити часові рамки, в які вони відбулися, типи сигналів, тому у нас є користувачі IP-абоненти. Об'єкт API було викликано з IP-адреси у користувацькому списку загроз Intel і ми бачимо, що є ще один для S3 Linux, тому частина цієї інформації надходить або частина цієї активності надходить з Linux для кожного з них.

Ми можемо бачити пов'язані з ними тактики, такі як початковий доступ та виявлення, ми можемо бачити інформацію про індикатори, таку як початковий доступ до виявлення,

Ми можемо бачити деталі учасника атаки та інформацію про кінцеву точку, таку як IP-адреса, пов'язана з цією активністю. Якщо ми прокрутимо вгору та натиснемо на цю іншу вкладку, ми можемо бачити ресурси, пов'язані з цією послідовністю атаки, такі як ключ доступу, корзина S3 та екземпляр EC2, пов'язаний з цією проблемою безпеки. Зрештою, ця послідовність атаки збирає певну інформацію з сигналів та ресурсів та зіставляє її з тактиками та методами MITRE (рисунок 3.6), щоб служби реагування на інциденти могли зрозуміти весь спектр проблеми безпеки та зрештою реагувати ефективніше та результативніше на загальну проблему безпеки, а не на основі пошуку за пошуком.

The screenshot displays the Amazon GuardDuty console interface. On the left, a sidebar contains navigation links for 'GuardDuty', 'Protection plans', 'Accounts', 'Usage', 'Settings', and 'Lists'. The main content area shows an 'Attack sequence' for a specific finding. It details the observed MITRE ATT&CK tactics: Discovery, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Lateral Movement, Credential Access, and Collection. A diagram illustrates the flow of these tactics. Below the tactics, the interface lists indicators, actors, and endpoints. The right sidebar provides details for three resources associated with the attack: an Access Key, an S3 Bucket, and an EC2 Instance. Each resource is tagged with 'Exfiltration', 'Impact', 'Discovery', and 'Initial Access'.

Рис. 3.6. Зіставлення інформації щодо сигналів з тактиками та методами MITRE

Отже, було розглянуто функцію в Guard Duty, яка допомагає нам зрозуміти початкову послідовність, що охоплює кілька ресурсів, джерела даних, періоди часу, допомагає нам ідентифікувати загрози з найвищим пріоритетом у корпоративних хмарних середовищах.

Також треба відмітити, що Amazon GuardDuty застосовує штучний інтелект (AI) та машинне навчання (ML) разом із вбудованою аналітикою загроз для

інтелектуального виявлення потенційних загроз у корпоративному середовищі AWS.

Хоча AWS не публікує повний список усіх пропрієтарних алгоритмів ML, які використовуються, ключові підходи, які застосовує GuardDuty, включають:

моделі виявлення аномалій (Anomaly Detection):

GuardDuty встановлює базові лінії нормальної поведінки для ваших облікових записів, користувачів (IAM), робочих навантажень (наприклад, інстансів Amazon EC2, контейнерів Amazon EKS/ECS) та мережевого трафіку.

Моделі ML, такі як Variational Autoencoders (VAEs) (особливо для аналізу викликів AWS API через AWS CloudTrail), використовуються для оцінки ймовірнісного розподілу дій. Вони допомагають виявити незвичайну активність, яка відхиляється від встановленого профілю, навіть якщо вона не є відомою загрозою.

Приклади виявлених аномалій:

доступ до ресурсів AWS з нетипової геолокації або у незвичний час доби;
незвичайні виклики API (наприклад, спроби вимкнути логування CloudTrail або створити знімки бази даних із підозрілої IP-адреси);

нетипова поведінка функцій AWS Lambda або входів до бази даних Amazon RDS.

моделі поведінкового аналізу (Behavioral Modeling):

ці моделі безперервно аналізують потоки даних, таких як VPC Flow Logs, DNS Logs та AWS CloudTrail Management Events, щоб створювати профілі поведінки та виявляти підозрілі шаблони, що вказують на компрометацію облікових записів або ресурсів.

Нові можливості, як-от GuardDuty Extended Threat Detection, використовують AI/ML для кореляції безпекових сигналів протягом тривалого часу та через різні ресурси, щоб ідентифікувати складні, багатоетапні послідовності атак (наприклад, викрадення облікових даних, за яким слідує витік даних), і представляти їх як єдине, критичне виявлення.

аналіз загроз (Threat Intelligence Integration):

моделі ML інтегруються з власними та сторонніми потоками даних про загрози (Threat Intelligence Feeds), що містять списки відомих шкідливих IP-адрес, доменів, хешів файлів тощо.

ML допомагає підвищити точність, поєднуючи поведінкові аномалії з відомими індикаторами компрометації.

3.3. Рекомендації щодо інтелектуального виявлення загроз хмарним корпоративним ресурсам

Необхідно постійно забезпечувати ідентифікацію. Контроль доступу не повинен зупинятися на вході в систему. У хмарних середовищах, де ідентифікаційні дані та дозволи постійно змінюються, забезпечення дотримання правил у режимі реального часу є надзвичайно важливим. Необхідно проваджувати політики контекстного доступу та автоматично скасовувати невикористані привілеї.

Необхідно автоматизовувати шляхи реагування на високоризикові ситуації. Ручне реагування не може встигати за такими загрозами, як горизонтальне переміщення або зловживання API. Необхідно автоматизовувати робочі процеси від виявлення до стримування там, де швидкість має найбільше значення, особливо для загроз ідентифікації та виконання. Автоматизація має найбільший вплив на реагування на інциденти.

Необхідно уніфікувати видимість у всій корпоративній хмарній системі. Фрагментована телеметрія уповільнює та робить аналіз першопричини неповним. Централізуйте спостереження в хмарах за допомогою інструментів на основі API, які відстежують поведінку робочого навантаження, потоки даних та конфігурації.

Необхідно забезпечувати безперервне дотримання вимог. Періодичні перевірки більше не є достатніми. Вбудуйте забезпечення дотримання політик у робочі процеси DevOps та запускайте сповіщення в режимі реального часу про неправильні конфігурації та відхилення. Використовуйте автоматизований моніторинг відповідності. Необхідно розглядати відповідність як активну систему,

а не як заплановане завдання.

Необхідно об'єднувати можливості різних інструментів. Непов'язані інструменти створюють прогалини та затримують реагування. Консолідуйтеся навколо платформ, які інтегрують виявлення, забезпечення дотримання політик та виправлення помилок у корпоративному хмарному стеку.

Необхідно використовувати ШІ там, де він спонукає до дії. Штучний інтелект має уточнювати, а не ускладнювати. Зосередьтеся на цінних випадках використання, таких як виявлення аномалій, збагачення сигналів та автоматизоване виправлення.

Безпека хмарних технологій більше не визначається тим, як швидко команди виявляють загрози, а тим, як швидко вони можуть діяти. Існує тенденція чіткого переходу від реактивних архітектур з великою кількістю інструментів до інтегрованих, адаптивних систем, що працюють зі швидкістю хмари.

Розглянемо основні рекомендації щодо впровадження та ефективного використання Amazon GuardDuty для інтелектуального виявлення загроз хмарним корпоративним ресурсам.

GuardDuty – це сервіс виявлення загроз, який використовує машинне навчання, виявлення аномалій та інтегровані джерела даних про загрози (threat intelligence) для ідентифікації та пріоритизації потенційних атак.

Нижче наведено рекомендації, від базового налаштування до просунутих технік автоматизації.

1. Фундаментальне налаштування та архітектура (Foundation Phase)

Найважливіший крок – забезпечити максимальне покриття моніторингом.

Щодо централізованого управління через AWS Organizations. Якщо у вас кілька AWS-акаунтів, обов'язково використовуйте інтеграцію GuardDuty з AWS Organizations. Для цього необхідно призначити один акаунт (зазвичай Security Audit акаунт) як делегованого адміністратора GuardDuty. Це дозволить автоматично вмикати GuardDuty для всіх існуючих та нових акаунтів в організації, а також централізовано переглядати всі знахідки (findings).

Це призведе до уникнення «сліпих зон» при створенні нових ресурсів або

акаунтів.

Щодо забезпечення глобального покриття (Всі регіони). GuardDuty – це регіональний сервіс. Увімкніть його в усіх регіонах AWS, навіть у тих, які ви активно не використовуєте.

Для цього використовуйте скрипти (CloudFormation StackSets або Terraform) для активації сервісу в усіх доступних регіонах. Це враховує те, що зломисники часто використовують невикористовувані регіони для приховування своєї діяльності (наприклад, майнінгу криптовалюти).

Щодо активації всіх джерел даних (Data Sources) GuardDuty за замовчуванням аналізує CloudTrail Management Events, VPC Flow Logs та DNS Logs. Однак для повного захисту критично важливо увімкнути додаткові модулі:

S3 Protection, який відстежує підозрілий доступ до даних у кошиках S3 (наприклад, незвичні патерни вивантаження даних);

Kubernetes Protection (EKS), який аналізує аудит-логи Kubernetes для виявлення загроз у контейнеризованих середовищах;

Malware Protection який автоматично сканує EBS-томи, пов'язані з EC2 інстансами або контейнерами, які GuardDuty ідентифікував як підозрілі;

RDS Protection, який виявляє підозрілі спроби входу в бази даних Aurora;

Lambda Protection, який виявляє зловмисне використання Lambda функцій.

2. Налаштування точності та зменшення шуму (Tuning Phase)

Інтелектуальне виявлення загроз потребує контексту корпоративного середовища, щоб відрізнити нормальну активність від аномальної.

Щодо використання списків довірених IP (Trusted IP Lists). Визначте IP-адреси, які точно є безпечними (наприклад, публічні IP ваших офісних VPN-шлюзів, IP-адреси довірених партнерів або зовнішніх інструментів моніторингу).

Для цього завантажте ці списки в GuardDuty. Це призведе до того, що GuardDuty не генеруватиме знахідки для активності з цих IP-адрес, що суттєво зменшує кількість хибних спрацьовувань (false positives).

Щодо використання списків загроз (Threat Lists). Якщо у вас є власна розвідка загроз (Cyber Threat Intelligence) або ви купуєте специфічні для галузі фіди

зловмисних IP-адрес, необхідно завантажувати власні списки шкідливих IP в GuardDuty. Це доповнює стандартні фіди AWS та дозволяє виявляти специфічні загрози, актуальні для вашого бізнесу.

Щодо розуміння «періоду навчання» (Baselining). Важливо знати та враховувати, що моделям машинного навчання GuardDuty потрібно від 7 до 14 днів для побудови базового профілю (baseline) нормальної поведінки у вашому акаунті. Протягом цього періоду можлива підвищена кількість аномальних знахідок, які з часом стабілізуються.

3. Налаштування операцій та реагування (Response Phase)

Виявлення загрози не має сенсу без швидкого реагування.

Необхідно здійснювати централізацію через AWS Security Hub. Для цього інтегруйте GuardDuty з AWS Security Hub. Увімкніть Security Hub у тому ж адміністративному акаунті. Знахідки GuardDuty автоматично надходитимуть туди у стандартизованому форматі (ASFF). Це забезпечить «єдине вікно» для перегляду загроз разом із результатами перевірок конфігурації (CSPM) та даними з інших інструментів безпеки.

Щодо налаштування сповіщень у реальному часі Не покладайтесь на ручний перегляд консолі. Налаштуйте сповіщення для знахідок із високим (High) та середнім (Medium) пріоритетом.

Для цього використовуйте Amazon EventBridge (раніше CloudWatch Events) для перехоплення знахідок GuardDuty. Створіть правило, яке надсилає повідомлення через Amazon SNS (наприклад, на Email, в Slack-канал команди безпеки, або в систему PagerDuty/OpsGenie).

Щодо впровадження автоматизованого реагування (SOAR) – для критичних загроз швидкість реакції має вирішальне значення. Використовуйте наступну автоматизацію:

Сценарій 1 (Ізоляція EC2). Якщо GuardDuty виявляє, що EC2 інстанс комунікує з C&C (Command & Control) сервером -> EventBridge тригерить AWS Lambda функцію -> Lambda змінює Security Group інстансу, блокуючи весь трафік, і додає IAM роль, що забороняє дії.

Сценарій 2 (Блокування користувача). Якщо виявлено компрометацію IAM-креденціалів -> EventBridge тригерить Lambda -> Lambda деактивує ключі доступу (Access Keys) та примусово завершує сесії користувача.

Для проведення глибокого розслідування з Amazon Detective необхідно увімкнути Amazon Detective. Коли GuardDuty знаходить щось підозріле, Detective допомагає відповісти на запитання чому і як це сталося, будуючи візуальний граф взаємозв'язків між ресурсами, IP-адресами та API-викликами за певний час до і після інциденту.

4. Найкращі практики та постійне вдосконалення

Не ігноруйте знахідки низького пріоритету (Low Severity). Вони можуть бути індикаторами ранніх стадій розвідки зловмисника або проблем із гігієною безпеки (наприклад, використання незахищених протоколів).

Використовуйте фільтри та збережені пошуки. В консолі GuardDuty налаштуйте фільтри, щоб фокусуватися на конкретних типах загроз (наприклад, Cryptocurrency:EC2/BitcoinTool.B!DNS).

Регулярне тестування (Purple Teaming). Перевіряйте, чи працюють ваші налаштування та сповіщення. Ви можете згенерувати тестові знахідки GuardDuty (Sample Findings) через консоль або API, щоб переконатися, що весь ланцюжок реагування працює коректно.

Аналіз вартості. Хоча Amazon GuardDuty є високоефективним, вартість залежить від обсягу логів. Регулярно перевіряйте вкладку «Usage» в консолі GuardDuty, щоб розуміти, які джерела даних генерують найбільші витрати, та оптимізувати їх за потреби (наприклад, оптимізація VPC Flow Logs).

Отже, інтелектуальне виявлення загроз на базі GuardDuty – це не разова дія «увімкнув і забув», а процес. Ключ до успіху полягає в повному покритті всіх акаунтів та регіонів, активації додаткових джерел даних (S3, EKS, Malware Protection), тюнінгу системи за допомогою Trusted IP, а також в автоматизації сповіщень та реагування на інциденти.

ВИСНОВКИ

В роботі досліджено проблему інтелектуального виявлення загроз хмарним корпоративним ресурсам, визначено його мету та завдання. Виявлення загроз безпеці в режимі реального часу передбачає використання передових технологій та інструментів для моніторингу систем, аналізу даних і реагування на потенційні загрози в міру їх виникнення.

Визначено існуючі підходи до інтелектуального виявлення загроз хмарним корпоративним ресурсам. Проактивний підхід до інтелектуального виявлення загроз хмарним корпоративним ресурсам спирається на поведінковий аналіз, штучний інтелект і машинне навчання, інструменти моніторингу в реальному часі та інтеграцію з існуючою інфраструктурою безпеки.

Проаналізовано провідні інструменти моніторингу хмарної безпеки, які є найкращими в галузі та захищають активи, ресурси та доступ до різних хмарних облікових записів і сервісів. Організації, які хочуть швидко масштабуватися та покращити управління хмарною безпекою, вважатимуть ці рішення ефективними. Треба зазначити, що хмарна безпека дотримується ітеративного підходу до безпеки, і більшість організацій отримують найкращі результати, поєднуючи ці інструменти для швидшого розслідування та активного усунення загроз.

Проаналізовано методи та засоби інтелектуального виявлення загроз хмарним корпоративним ресурсам на базі Amazon GuardDuty. Amazon GuardDuty – це служба виявлення загроз, яка постійно відстежує, аналізує та обробляє джерела даних і журнали AWS у корпоративному середовищі AWS. GuardDuty використовує канали інформації про загрози, такі як списки шкідливих IP-адрес і доменів, хеші файлів і моделі машинного навчання, для виявлення підозрілої та потенційно шкідливої активності у корпоративному середовищі AWS.

Визначено призначення, основні функції та склад рішення Amazon GuardDuty. Особливістю рішення Amazon GuardDuty є застосування машинного навчання. Рішення Amazon GuardDuty постійно адаптується, навчається, що є

нормальним саме для конкретних ресурсів, і завдяки цьому може ефективно виявляти складні та раніше невідомі загрози, які неможливо знайти за допомогою традиційного сигнатурного аналізу.

На основі досліджень проведених в роботі запропоновано порядок застосування технології інтелектуального виявлення загроз хмарним корпоративним ресурсам. Розширене виявлення загроз Amazon GuardDuty автоматично виявляє багатоетапні атаки, що охоплюють джерела даних, різні типи ресурсів AWS та час в межах облікового запису AWS. Завдяки цій можливості Amazon GuardDuty зосереджується на послідовності кількох подій, які він спостерігає, моніторячи різні типи джерел даних. Розширене виявлення загроз співвідносить ці події, щоб визначити сценарії, які представляють собою потенційну загрозу для корпоративного середовища AWS, а потім генерує результати пошуку послідовності атак.

Розроблено рекомендації фахівцям з кібербезпеки щодо інтелектуального виявлення загроз хмарним корпоративним ресурсам.

Таким чином, правильна реалізація технології інтелектуального виявлення загроз хмарним корпоративним ресурсам має забезпечити ефективний захист корпоративних даних та своєчасне реагування на виникаючі загрози.

ПЕРЕЛІК ПОСИЛАНЬ

1. 2025 Cloud Security Report. Trend Micro. By Cybersecurity Insiders. URL: <https://whitepaper.silicon.co.uk/wp-content/uploads/2025/08/2025-TrendMicro-Cloud-Report-by-CSI.pdf>
2. What is Real-time Threat Detection? Darktrace. URL: <https://www.darktrace.com/cyber-ai-glossary/real-time-threat-detection>
3. 11 Best Cloud Security Monitoring Tools. SentinelOne. Updated: September 9, 2025. URL: <https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-monitoring-tools/>
4. What is AWS Guard Duty? URL: <https://www.nops.io/glossary/what-is-aws-guard-duty/>
5. Amazon GuardDuty. User Guide. URL: <https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html>
6. Amazon GuardDuty – Intelligent Threat Detection. Last Updated: 15 Jul, 2025. URL: <https://www.geeksforgeeks.org/blogs/what-is-amazon-guardduty>
7. Niels Kroeze. 14 Cloud Security Risks, Threats and Challenges in 2025. URL: <https://intercept.cloud/en-gb/blogs/14-cloud-security-risks-threats-challenges-2025>
8. Ranjinnijoshe. AWS GuardDuty Architecture. Medium, Sep 12, 2023. URL: <https://medium.com/@ranjinnijoshe/%EF%B8%8Faws-guardduty-architecture-e01067d83fb2>
9. Die 10 besten Cloud-Sicherheitstools: Leitfaden (2025 aktualisiert). Cyera Research, Oct 2, 2025. URL: <https://www.cyera.com/de/blog/top-10-cloud-security-tools-guide>
10. Top 12 Cloud Security Monitoring Tools. Last updated on January 28, 2025. URL: <https://www.scrut.io/post/best-cloud-security-monitoring-tools>
11. Cloud Security Posture Management Tools Reviews and Ratings. Gartner Research. URL: <https://www.gartner.com/reviews/market/cloud-security-posture-management-tools>

12. Орлик Павло Анатолійович. Технологія інтелектуального виявлення загроз хмарним корпоративним ресурсам на основі Amazon GuardDuty. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». 29 жовтня 2025 року. Державний університет інформаційно-комунікаційних технологій, м. Київ. Тези доповідей. С. 113-115. URL: https://duikt.edu.ua/uploads/p_2779_58326207.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(Презентація)