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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія виявлення вторгнень до хмарних корпоративних ресурсів на базі Amazon Detective»

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

_____ Олексій БОГДАНОВИЧ
(підпис)

Виконав: здобувач(ка) вищої освіти групи БСДМ-63
БОГДАНОВИЧ Олексій
(прізвище, ім'я)

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

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

Київ 2025

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

API – Application Programming Interface

APT – Advanced Persistent Threat

CDN – Content Delivery Network

CIEM – Cloud Infrastructure Entitlement Management

CIPS – Cloud Infrastructure and Platform Service

CNAPP – Cloud-Native Application Protection Platform

CSPM – Cloud Security Posture Management

CWPP – Cloud Workload 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

OWASP – Open Web Application Security Project

SOC – Security Operations Center

WAAP – Web Application and API protection

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. Одним із найцінніших аспектів хмарних систем виявлення вторгнень є те, що сповіщення є цілеспрямованими. Виявляючи ймовірні порушення, адміністратори можуть бути попереджені про критичні та своєчасні інциденти, а не мати справу з втомою від сповіщень через неспецифічні сповіщення. Використовуючи такі методи, як машинне навчання, для аналізу системної активності та виявлення закономірностей, багато систем виявлення вторгнень здатні краще виявляти та попереджати адміністраторів про зловмисну активність, не генеруючи хибно позитивних результатів. Це дозволяє адміністраторам зосередити свою увагу на найважливіших сповіщеннях та швидко реагувати на те, що має значення.

Виявлення вторгнень в хмарних обчисленнях здійснюється шляхом моніторингу активності системи та аналізу закономірностей для виявлення шкідливої активності. Добре спроектована система виявлення вторгнень може виявляти аномальну поведінку та сповіщати адміністраторів про виявлення підозрілої активності.

Найбільш очевидною перевагою хмарних систем виявлення вторгнень є те, як вони можуть покращити безпеку організації, своєчасно виявляючи та стримуючи потенційну шкідливу активність. Хоча цінність хмарних систем виявлення вторгнень полягає в тому, що вони можуть швидко попереджати адміністраторів про підозрілу активність, ці сповіщення зрештою базуються на даних спостереження про всю базову систему. Від моніторингу мережевого трафіку до активності системи та користувачів або навіть журналів доступу та аналізу поведінки, ці дані надають повнішу картину того, що відбувається в хмарній інфраструктурі, на яку покладається організація. Завдяки кращій видимості всієї цієї системної активності, організації краще оснащені для швидкого та ефективного виявлення та усунення проявів шкідливої поведінки.

Вищесказане визначає актуальність теми цієї кваліфікаційної роботи,

основний зміст якої становлять дослідження технології виявлення вторгнень до хмарних корпоративних ресурсів на базі Amazon Detective.

Об'єкт дослідження – виявлення вторгнень до хмарних корпоративних ресурсів.

Предмет дослідження – технологія виявлення вторгнень до хмарних корпоративних ресурсів на базі Amazon Detective.

Мета роботи – розробити порядок застосування технології виявлення вторгнень до хмарних корпоративних ресурсів на базі Amazon Detective та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми виявлення вторгнень до хмарних корпоративних ресурсів;

проаналізувати підходи до виявлення вторгнень до хмарних корпоративних ресурсів;

проаналізувати існуючі рішення для виявлення вторгнень до хмарних корпоративних ресурсів;

проаналізувати методи та засоби виявлення вторгнень до хмарних корпоративних ресурсів на базі Amazon Detective;

розкрити порядок реалізації технології виявлення вторгнень до хмарних корпоративних ресурсів на базі Amazon Detective.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології виявлення вторгнень до хмарних корпоративних ресурсів на базі Amazon Detective, 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 ВИЯВЛЕННЯ ВТОРГНЕНЬ ДО ХМАРНИХ КОРПОРАТИВНИХ РЕСУРСІВ

1.1. Дослідження проблеми виявлення вторгнень до хмарних корпоративних ресурсів

Вразливості хмари – це слабкі місця, недогляди або прогалини в хмарній інфраструктурі, які зловмисники або неавторизовані користувачі можуть використовувати для отримання доступу до середовища організації та потенційного заподіяння шкоди [1].

Оскільки компанії збільшують використання хмарного хостингу для зберігання даних та обчислень, ризик атаки на їхні хмарні сервіси зростає, оскільки хмара являє собою дуже динамічний та розподілений ландшафт. Як зазначається у звіті CrowdStrike 2024 Global Threat Report, у 2023 році спостерігалося 75% зростання кількості вторгнень у хмарне середовище. У звіті також було виявлено 110% зростання випадків, пов’язаних з хмарно-орієнтованими зловмисниками, тобто зловмисниками, які знають про здатність компрометувати хмарні робочі навантаження та використовують ці знання для зловживання функціями, унікальними для хмари. Часто зловмисники отримують дійсні облікові дані для доступу до хмарного середовища жертви, щоб потім продовжити свою атаку, зазвичай використовуючи інструменти, схвалені організацією [1].

Згідно з опитуванням CrowdStrike кількість вторгнень у хмару зросла на 136 відс. у першій половині 2025 року. Найпримітніше, що 81 відс. цих вторгнень не були пов’язані з використанням шкідливого програмного забезпечення. Замість розгортання шкідливого програмного забезпечення, зловмисники все частіше покладаються на викрадені облікові дані для отримання доступу та роботи в легітимних системах. Цей зсув означає, що багато традиційних методів виявлення, створених для позначення шкідливого коду, повністю ігноруються [11].

Оскільки більшість вторгнень зараз повністю уникають шкідливого

програмного забезпечення, акцент у безпеці має зміститися. Коли зловмисники діють з дійсними обліковими даними, ключовою точкою контролю стає ідентифікація, а не периметр мережі. Сьогодні існує очевидна потреба в безпеці, орієнтованій на дані, яка захищає самі дані та виявляє зловживання, а не покладається виключно на запобігання проникненню [11].

Неефективне управління вразливостями хмарних технологій може завдати шкоди репутації, якщо дані клієнтів будуть скомпрометовані, що призведе до втрати бізнесу. Основними вразливостями хмарних технологій є [1]:

Неправильні конфігурації хмарних ресурсів є однією з найпоширеніших вразливостей, з якими стикаються організації. Неправильні конфігурації можуть варіюватися від надмірних дозволів облікового запису до незахищених резервних копій, і вони часто спричинені швидкістю розгортання, обмеженими знаннями належних практик або відсутністю повного розуміння хмарної інфраструктури.

Незахищені API. API широко поширені в сучасній розробці програмного забезпечення, оскільки вони використовуються в мікросервісах, додатках та серверах веб-сайтів. Вони повинні обробляти запити, отримані від мобільних пристроїв, додатків, веб-сторінок та третіх сторін, а також запити від ботів, спамерів та хакерів. Саме тому наявність безпечного API є критично важливою для зменшення поверхні атаки.

Зловмисні запити API можуть мати різні форми. Деякі з найпоширеніших включають:

ін’єкція коду та запитів (SQL-ін’єкція, ін’єкція команд);

зміна параметрів;

необмежене завантаження файлів.

Відсутність видимості. Зі збільшенням використання хмарних сервісів зростає і масштаб корпоративної інфраструктури. Коли компанії використовують тисячі екземплярів хмарних сервісів, може бути важко відстежувати, як вони всі підключені, або бачити, які з них працюють у робочому середовищі в будь-який момент часу. Відстеження стану всієї корпоративної інфраструктури має бути простим і зручним.

Відсутність видимості хмарної інфраструктури є серйозною проблемою, яка ускладнює вжиття заходів щодо загрози, оскільки пошук джерела вразливості складною справою. Як команди безпеки, так і команди DevOps повинні постійно контролювати свій стан хмарної безпеки в режимі реального часу, оскільки команди безпеки мають уявлення про ризики, а команди DevOps володіють хмарними ресурсами та додатками.

Тіньові IT-системи. Однією з головних причин, чому організаціям бракує прозорості щодо своєї хмарної інфраструктури, є використання тіньових IT, що стосується практики створення хмарних ресурсів або будь-яких інших цифрових активів без належного схвалення IT-відділу. Тіньові IT поширені, коли компанії швидко зростають, оскільки співробітники можуть обійти процес схвалення, щоб мінімізувати перебої у своїй щоденній діяльності.

Тіньові IT-системи створюють ризики для безпеки, оскільки несанкціоновані активи часто не захищені належним чином через недбалість. Наприклад, співробітники можуть зберігати паролі за замовчуванням або неправильні конфігурації, оскільки ці активи були створені поза затвердженим процесом.

Незахищене керування ідентифікацією та доступом (IAM) є поширеним ризиком у хмарних системах. На високому рівні це виникає, коли користувачі або служби мають доступ до ресурсів, до яких вони не повинні мати доступу та/або які їм не потрібні. Неналежне управління доступом може призвести до зловмисних дій, таких як викрадення облікового запису.

Викрадення облікового запису – це тип атаки, під час якої зловмисники намагаються викрасти конфіденційні облікові дані за допомогою таких методів, як фішинг, кейлоггер, атаки методом перебору та міжсайтовий скриптинг (XSS). Зловмисники також можуть впроваджувати шкідливе програмне забезпечення в хмарні сервіси, щоб поставити під загрозу дані та операції.

Зловмисні інсайдери, також відомі як внутрішні загрози, – це ризики кібербезпеки, що виникають всередині організації, зазвичай у вигляді невдоволеного або недбайливого співробітника. Існує кілька способів, за допомогою яких ці зловмисники можуть отримати доступ до корпоративних

хмарних облікових записів – наприклад, якщо колишній співробітник все ще має дійсні облікові дані для облікових записів, він зможе отримати доступ.

Зловмисники також можуть отримати доступ до корпоративних хмарних ресурсів через викрадення облікового запису внаслідок успішної фішингової атаки та/або слабкого захисту облікових даних (наприклад, якщо у співробітника занадто простий пароль або пароль використовується спільно між обліковими записами). Такий тип вразливості може бути особливо небезпечним, оскільки дані – це не єдине, що може бути викрадено або змінено, – під загрозою також перебуває інтелектуальна власність.

Вразливість нульового дня – це недолік безпеки або програмного забезпечення, для якого немає виправлень чи виправлень. Тому ці типи вразливостей не виявляються багатьма антивірусними програмними рішеннями або іншими технологіями виявлення загроз на основі сигнатур. Після використання вразливості зловмисники можуть спробувати викрасти конфіденційні дані, виконати віддалене виконання коду або заблокувати доступ законних користувачів до своїх хмарних сервісів.

Людська помилка. Згідно з дослідженням Thales Global Cloud Security, людські дії були відповідальні за 44% зареєстрованих випадків порушення безпеки хмарних даних. Ці помилки можуть мати різні форми, включаючи неправильні конфігурації та проблеми з керуванням доступом. Багато з цих вразливостей спричинені обмеженими знаннями про найкращі практики безпеки або поганим стратегічним плануванням.

Вразливості хмарних середовищ стають дедалі поширенішими, і організаціям надзвичайно важко керувати високо розподіленими та динамічними хмарними середовищами.

Необхідно відмітити, що у першій половині 2025 року спостерігалося зростання кількості хмарних вторгнень на 136% порівняно з усім 2024 роком [2]. У Звіті [2] зазначено, що за останні 12 місяців CrowdStrike OverWatch спостерігав 40% зростання кількості вторгнень у хмару, пов’язаних зі зловмисниками, що працюють з China-nexus. Це зростання свідчить про те, що експлуатація хмарних

ресурсів продовжує бути ключовим напрямком для цих зловмисників. Величезні обсяги даних, масштабованість та некоректні конфігурації хмари дозволяють зловмисникам досягати стійкості, рухатися в нерівномірному напрямку та викрадати дані.

Згідно з аналізом набору даних, тактика соціальної інженерії залишається основною точкою входу для зловмисників, причому фішинг (включаючи вішинг, шкідливий спам та шкідливу рекламу) становить близько 60% спостережуваних випадків. Експлуатація вразливостей (21,3%) залишається поширеним вектором вторгнення, за ним йдуть ботнети (9,9%). Шкідливі програми становлять 8%, що свідчить про те, що скомпрометоване або троянське програмне забезпечення та програми продовжують відігравати певну роль у вторгненнях у систему, тоді як несанкціонований доступ з боку внутрішніх загроз (0,8%) становить меншу, але все ще значну частку. Загалом, розподіл підкреслює, що хоча фішинг домінує в ландшафті загроз, технічні експлойти, механізми доставки шкідливого програмного забезпечення та внутрішні ризики залишаються значними проблемами. Дані демонструють чіткий контраст між фішингом та експлуатацією вразливостей як векторами вторгнення. Хоча фішинг є найпоширенішим шляхом, його вплив різноманітний. Приблизно 73% випадків фішингу класифікуються як невідомі, що відображає нечіткі або різноманітні подальші дії шкідливої діяльності, а 27% призвели до вторгнень [4].

Що стосується корисного навантаження, фішинг призводить до розгортання шкідливого коду у 23% випадків, що свідчить про те, що він може використовуватися переважно для цілей, пов'язаних із шкідливим програмним забезпеченням. З іншого боку, вразливості демонструють більш цілеспрямований профіль ризику. Майже 70% випадків вразливостей завершуються вторгненнями, причому 30% класифікуються як невідомі, а 68% цих інцидентів, пов'язаних з вразливостями, призводять до розгортання шкідливого коду, що вказує на те, що експлуатація вразливостей часто є прямим попередником встановлення шкідливого програмного забезпечення [4].

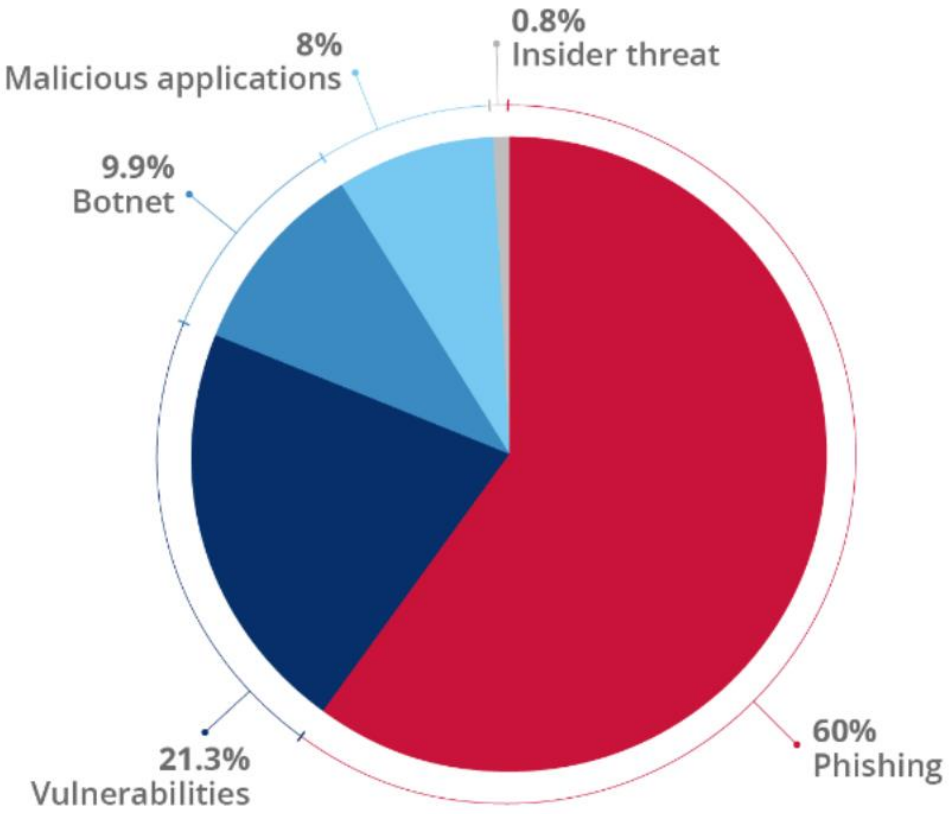

Рис. 1.1. Основні вектори ініціації атак [4]

Розподіл типів інцидентів домінує серед DDoS-атак, які складають близько 76,7% зареєстрованих випадків. Ця категорія переважно керується групами хактивістів, на які припадає більшість зібраних DDoS-інцидентів, при цьому кіберзлочинні групи складають незначну частку, часто пов’язану з вимаганням (наприклад, DDoS з метою вимагання викупу). Далі йдуть вторгнення з 17,8%, переважно кіберзлочинною діяльністю, за якими йдуть узгоджені з державою набори вторгнень, які зазвичай прагнуть збереження. Хактивісти з’являються лише незначно у випадках вторгнень. Дефейси майже виключно асоціювалися з хактивістами, що підкреслювало їхню роль як символічної тактики для підвищення видимості та протесту, а не як методу постійного вторгнення [4].

Оскільки компанії переносять все більше робочих навантажень і даних у хмару, проблеми безпеки продовжують загострюватися. Поверхня атак розширюється, і зловмисники використовують штучний інтелект для автоматизації атак, використання неправильних конфігурацій та обходу традиційних засобів контролю безпеки [3].

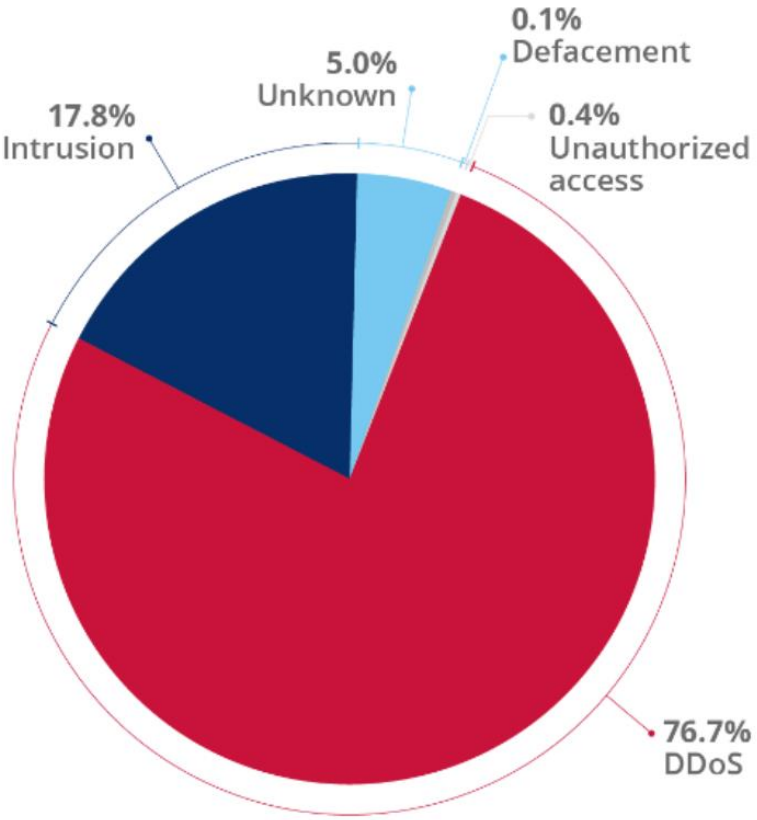

Рис. 1.2. Розподіл типів інцидентів [4]

У 2025 році рівень готовності до хмарних технологій залишається на місці, організації намагаються досягти повної зрілості, оскільки переважають часткові розгортання. Зростаюче впровадження хмарних технологій та штучного інтелекту на сучасному ринку прямо суперечить загальній відсутності прогресу в готовності до хмарної безпеки, що свідчить про те, що компанії залишають значні прогалини, якими можуть скористатися зловмисники. Без більш рішучих дій підприємства ризикують зіткнутися з постійно зростаючою прогалиною в безпеці своїх хмарних середовищ [3].

Опитування Cisco [3] підкреслює зростаючу залежність від заходів хмарної безпеки на основі штучного інтелекту. Серед компаній, які впровадили хмарні рішення для безпеки, 46% значне включення ШІ в ці захисні механізми. Однак, незважаючи на широке впровадження вдосконалень ШІ, рівень впровадження базових функцій залишається низьким.

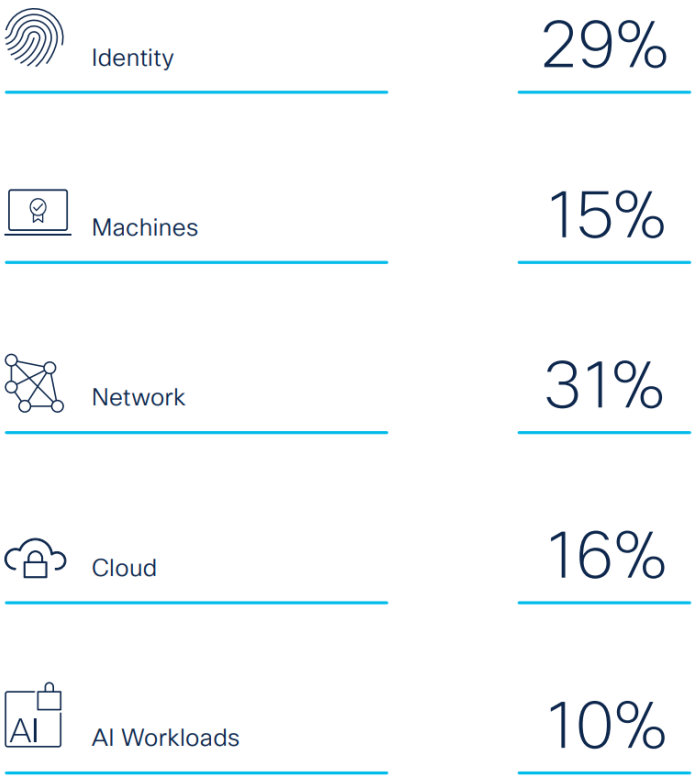

Рис. 1.3. Сфери, які компаніям найскладніше захистити від кібератак [3]

Досі існує низка компаній, які ще не почали впроваджувати хмарні рішення безпеки. З тих, хто це зробив, лідирують у впровадженні брандмауери хостів (53%) та інструменти аналітики видимості (47%), ймовірно, завдяки їхнім безпосереднім перевагам для безпеки та простоті розгортання. Натомість спостерігається відставання у розгортанні більш просунутих можливостей, таких як гібридні архітектури нульової довіри (40%) та забезпечення дотримання політик у кількох хмарних середовищах (36%) [3].

Ці прогалини відображають ширшу тенденцію: хоча компанії визнають важливість хмарної безпеки, виконання залишається проблемою. Вартість, складність та перешкоди в інтеграції уповільнюють прогрес, особливо для рішень, що потребують централізованої координації та міжхмарної сумісності [3].

Cisco [3] рекомендує, що компанії повинні вийти за межі фрагментованих стратегій безпеки та інвестувати в єдину, проактивну модель, покращену штучним інтелектом. Оскільки впровадження хмарних технологій прискорюється, компанії повинні вийти за рамки фрагментованих стратегій безпеки та інвестувати в

уніфіковані засоби захисту, покращені штучним інтелектом. Компанії ризикують залишити критично важливі робочі навантаження під впливом постійно зростаючого ландшафту загроз, який стає все більш автоматизованим, адаптивним та невблаганним, що підкреслює необхідність проактивного підсилення.

1.2. Аналіз підходів до виявлення вторгнень до хмарних корпоративних ресурсів

Виявлення вторгнень – це практика моніторингу корпоративної мережі, серверів, робочих станцій та інших IT-активів на предмет будь-якої підозрілої активності, зловмисних дій або порушень певних політик. Ця практика є невід'ємною складовою безпеки інфраструктури компанії.

Прикладами виявлення вторгнень є [5]:

політика регулювання трафіку: відстежує підозрілий трафік у мережі, наприклад, надзвичайно високу частоту TCP-з'єднань;

політика обмежених IP-адрес: приклад політики атаки IDS, яка спрямована на обмежені IP-адреси для однієї локальної IPv6-адреси, діапазону віддалених IPv6-адрес та всіх портів;

політика постійного відлуння: приклад політики атаки IDS, яка спрямована на постійне відлуння на локальному та віддаленому портах 7;

сповіщення електронною поштою: виявлення вторгнення в локальну систему та надсилання сповіщення електронною поштою системному адміністратору.

Система виявлення вторгнень – це пристрій або програмний застосунок, який контролює мережу на наявність шкідливої активності або порушень політик [5].

Типи систем виявлення вторгнень [5]:

система виявлення вторгнень у мережу;

система виявлення вторгнень на базі хоста;

система виявлення вторгнень периметра;

система виявлення вторгнень на базі віртуальної машини.

Традиційно, в середовищах центрів обробки даних, виявлення вторгнень

здійснюється на мережевому рівні за допомогою таких інструментів, як Zeek та Snort. Ці інструменти обробляють необроблені дані мережевого трафіку, а потім зіставляють їх зі шаблонами для виявлення певних сигнатур, моделей поведінки або аномалій. Наприклад, якщо вперше фіксується вхід з іншої країни або помічається, що десять людей одночасно ввійшли в систему на одному сервері, то можна розпізнати це як підозрілу спробу та запустити сповіщення. Аналогічно, відомі сигнатури експлойтів можна зіставити з мережевим трафіком.

Однак у хмарі отримати копію необробленого мережевого трафіку не так просто через обмеження середовища. Хмарний постачальник зазвичай розміщує кількох клієнтів і відповідає за фізичну мережу, а це означає, що клієнти не мають прямого доступу до неї. Тому в хмарі для виявлення вторгнень необхідно перемикатися на різні рівні.

Розглянемо виявлення вторгнень на трьох різних рівнях [5]:

рівень хмари;

мережевий рівень;

рівень обчислення (віртуальні машини, контейнери тощо).

Хоча хмарний рівень знаходиться на вершині, мережевий рівень та віртуальні машини залежать від нього. Той, хто контролює доступ до рівня керування хмарою, може впливати на мережевий та обчислювальний рівні. Розглянемо деякі ефективні методи виявлення вторгнень, які можна використовувати на кожному рівні.

Хмарний рівень: огляд журналів API. У хмарі вкрай важливо забезпечити безпеку автентифікації, оскільки, наприклад, будь-хто може спробувати увійти до облікового запису AWS з будь-якого місця. Однак, навіть після того, як ми максимально захистили його, люди все одно можуть зламати рівень керування хмарою, включаючи API. Ключі або облікові записи можуть бути випадково витекти, робоча станція спеціаліста DevOps з відкритими сеансами може бути атакована, і, по суті, хоча профілактика є чудовою, нам потрібно припускати, що засоби контролю в певний момент вийдуть з ладу, і бути готовими виявити це. Тому важливо проводити виявлення вторгнень на хмарному рівні – на один рівень вище за обчислення.

Все, що відбувається в хмарі, контролюється постачальником хмарних послуг, тому ми не маємо доступу до необробленого мережевого трафіку. Ми отримуємо лише журнали з детальним описом використання самих API, які надають інформацію про людей, що входять на рівень керування хмарою, створюють нові віртуальні машини, бази даних, облікові записи та багато іншого на рівні хмари.

Хмарні API не є традиційною функцією, яку можна знайти у стандартній системі виявлення вразливостей (IDS). Насправді, «хмарні IDS» рідко називають «IDS», оскільки цей термін тісно пов’язаний з методами виявлення на основі мережі та хоста. Хмарна IDS, для порівняння, має функції, які полегшують цю сферу застосування, дозволяючи командам безпеки аналізувати журнали та налаштовувати сповіщення в централізованому середовищі реєстрації, щоб повідомляти їх про щось підозріле, а іноді підтримує кількох постачальників хмарних послуг.

Обчислювальний рівень: використання виявлення вторгнень на основі хоста.

Виявлення вторгнень на основі хоста (HIDS) – це система, яка здатна моніторити та аналізувати внутрішні дані обчислювальної системи. Зростання популярності шифрованих мережевих протоколів також означає, що виявлення вторгнень на мережевому рівні стає все складнішим, хмарним чи ні. Виявлення вторгнень на основі хоста дуже добре працює в традиційних середовищах, як окремий варіант або навіть як доповнення до мережевої системи виявлення вторгнень.

У хмарі, через загальну відсутність доступу до необроблених мережевих даних, це часто єдиний варіант для виявлення вторгнень на обчислювальному рівні. Як приклад, *osquery* надає доступ до даних, що дозволяє виявляти підозрілу активність і вразливості, а також проводити глибокі розслідування.

Мережевий рівень: використання журналів потоку VPC для отримання метаданих мережевого трафіку. У локальному середовищі, такому як центр обробки даних, ми можемо запустити Zeek і налаштувати комутатори для копіювання всього трафіку на нього. Зазвичай ми не можемо зробити це в хмарному

середовищі, а коли можете, це дорога ініціатива.

Якщо ми користуємося Amazon Web Services (AWS) та віртуальною приватною хмарою (VPC), в журналах потоку VPC ми можемо побачити, які машини підключені та де вони підключені. Ми можемо поєднати ці дані зі службою виявлення загроз Amazon GuardDuty для виявлення вторгнень у мережу. Цей метод використовує метадані мережевого трафіку замість повного захоплення пакетів.

Мережевий трафік на віртуальних машинах та контейнерах надає змогу впровадити систему виявлення вторгнень на основі хоста за допомогою *osquery* для доповнення даних мережевого рівня. Іноді метаданих достатньо, щоб розпізнати підозрілу активність, але бувають і інші випадки, коли потрібно отримати набагато більше деталей.

Запуск *osquer*y на всіх корпоративних серверах Linux може надати дані, подібні до журналів потоку VPC від хмарного провайдера, що дозволить приймати глибші аналітичні дані, на яких базуватимуться рішення щодо безпеки. Оскільки *osquery* бачить всю мережеву активність, але з точки зору хоста, ми можемо легко визначити, який процес підключається до якого пункту призначення, і співвіднести це з даними аналітики загроз. Якщо ми використовуємо віртуальні машини, виявлення вторгнень на основі хоста може доповнити наші зусилля, якщо у нас немає всіх даних мережевого рівня.

1.3. Аналіз існуючих рішень для виявлення вторгнень до хмарних корпоративних ресурсів

Аналіз існуючих рішень для виявлення вторгнень до хмарних корпоративних ресурсів охоплює широкий спектр технологій, які розвинулися від традиційних систем виявлення вторгнень (IDS) до комплексних платформ безпеки хмарних застосунків (CNAPP).

Можна виділити наступні основні категорії рішень для виявлення вторгнень до хмарних корпоративних ресурсів:

традиційні системи виявлення вторгнень (IDS/IPS). Хоча спочатку вони були

розроблені для локальних мереж, багато з них мають хмарні імплементації. Прикладами мережевих IDS/IPS (NIDS/NIPS) є Suricata, Snort, Zeek.

Принцип роботи даних систем – аналізують мережевий трафік на наявність відомих сигнатур атак або аномальної поведінки. У хмарі їх розгортають як віртуальні пристрої (Virtual Appliances) або вбудовують у мережеві шлюзи хмарного провайдера.

Переваги: висока швидкість виявлення відомих загроз, гнучкість налаштувань.

Недоліки: Складність моніторингу «East-West2 трафіку (між хмарними ресурсами в межах однієї мережі) через особливості архітектури хмар, вимагають ручного керування та оновлення сигнатур.

Прикладами хостових IDS/IPS (HIDS/HIPS) є OSSEC, Wazuh.

Принцип роботи даних систем – встановлюються безпосередньо на віртуальні машини або контейнери, моніторять системні журнали, зміни файлів, процеси.

Переваги: детальний моніторинг внутрішньої активності хоста.

Недоліки: потребують встановлення агента на кожен ресурс, що ускладнює масштабування, можуть мати проблеми сумісності з різними ОС.

власні (нативні) інструменти хмарних провайдерів. Провідні хмарні провайдери (AWS, Azure, Google Cloud) пропонують власні інтегровані сервіси безпеки. Прикладами таких систем є Amazon GuardDuty, Azure Security Center / Microsoft Defender for Cloud, Google Cloud Security Command Center.

Принцип роботи даних систем – використовують машинне навчання та аналіз логів (CloudTrail, VPC Flow Logs, журналів активності) для виявлення підозрілої активності, такої як несанкціонований доступ, використання скомпрометованих облікових даних, аномалії в конфігурації.

Переваги: глибока інтеграція з екосистемою провайдера, автоматизоване керування, не потребують розгортання додаткової інфраструктури.

Недоліки: прив’язка до конкретного провайдера (vendor lock-in), можуть бути менш гнучкими для гібридних середовищ.

платформи захисту хмарних застосунків (CNAPP). Це сучасний, комплексний підхід, який об’єднує кілька функцій безпеки в єдиній платформі. Прикладами таких систем є Wiz, Lacework, Palo Alto Networks Prisma Cloud, CrowdStrike Falcon Cloud.

Принцип роботи даних систем – охоплюють весь життєвий цикл хмарного застосунку від розробки (DevSecOps) до виконання (Run-time). Вони комбінують функції Cloud Security Posture Management (CSPM), Cloud Workload Protection Platforms (CWPP), Cloud Infrastructure Entitlement Management (CIEM) та виявлення загроз.

Переваги: комплексний захист, централізоване керування, автоматизація виявлення та реагування, підтримка гібридних та мультихмарних середовищ.

Недоліки: висока вартість, складність впровадження та налаштування повного спектра функцій.

інструменти управління інформацією про безпеку та подіями (SIEM). Прикладами таких систем є Splunk, QRadar, Microsoft Sentinel.

Принцип роботи даних систем – збирають та агрегують дані (логи, події) з різних джерел, як хмарних, так і локальних, для централізованого аналізу та виявлення комплексних загроз.

Переваги: централізований моніторинг гібридного середовища, можливість кореляції подій з різних систем.

Недоліки: вимагають значних ресурсів для налаштування правил кореляції, висока вартість ліцензій залежно від обсягу даних.

Порівняльний аналіз власних (нативних) інструментів виявлення вторгнень від провідних хмарних провайдерів показує (таблиця 1.1), що кожен із них має унікальні сильні сторони, інтеграцію та підхід.

AWS (Amazon Web Services)

AWS пропонує зрілу та широку екосистему інструментів безпеки, де Amazon GuardDuty є ключовим сервісом для виявлення вторгнень. Він постійно аналізує мільярди подій і журналів для виявлення таких загроз, як скомпрометовані екземпляри EC2, несанкціонований доступ до даних та аномалії облікових записів.

Сильною стороною є його деталізоване, гранулярне управління і велика кількість сертифікатів відповідності стандартам.

Azure (Microsoft Azure)

Microsoft Defender for Cloud вирізняється своєю інтеграцією в існуючу корпоративну інфраструктуру, особливо для компаній, які вже використовують продукти Microsoft. Він надає уніфіковане управління безпекою та захист від загроз у гібридних хмарах, що є значною перевагою порівняно з конкурентами, які зосереджені лише на своєму середовищі. Можливості SIEM (Security Information and Event Management) через Microsoft Sentinel також дуже потужні для централізованого аналізу та реагування на інциденти.

На рисунку 1.4 показано сценарії використання Microsoft Defender for Cloud, зокрема: комплексне керування безпекою DevSecOps, посилення захищеності хмари за допомогою контекстних аналітичних висновків і захист робочих процесів у хмарі від сучасних кіберзагроз. У нижній частині рисунку 1.4 показано гібридні й багатохмарні платформи, які підтримує Defender for Cloud, зокрема веб-служби Amazon Web Services, Microsoft Azure, Google Cloud Platform і локальні робочі процеси.

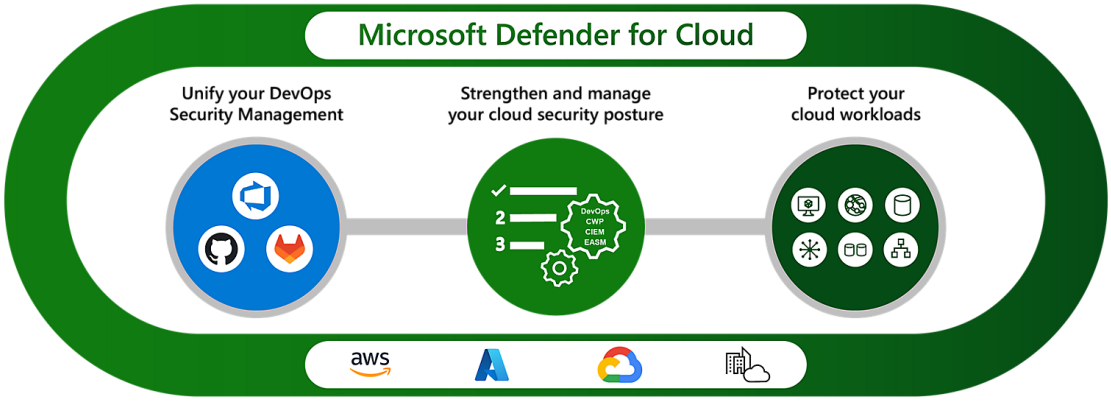

Рис. 1.4. Сценарії використання Microsoft Defender for Cloud

GCP (Google Cloud Platform)

Google Cloud Security Command Center (SCC) – це хмарне рішення для управління ризиками, яке допомагає професіоналам з безпеки для запобігання,

виявлення та реагування на проблеми безпеки. Це допомагає захистити корпоративне хмарне середовище, надаючи інструменти для моніторингу та керування наступні області:

виявлення вразливостей. Виявлення та усунення таких проблем, як неправильні конфігурації, оприлюднені ресурси, витік облікових даних і ресурси з відомими ризиками. Контроль дотримання вимог загальної безпеки такі тести, як NIST, HIPAA, PCI-DSS і CIS;

виявлення та пом’якшення загроз. Виявлення та реагування на активні загрози такі як зловмисне програмне забезпечення, майнери криптовалют, атаки під час виконання контейнерів і розповсюдження атаки типу «відмова в обслуговуванні» (DDoS);

позиції та політики. Визначення та розгортання позицій безпеки для моніторингу статусу корпоративних ресурсів Google Cloud і позицій адреси, які дрейфують, коли вони бувають. Перевірка та виправлення облікових записів з надмірним дозволом;

відповідність і системи безпеки даних. Визначення і розгортання фреймворків та хмарних елементів керування, щоб контролювати стан ресурсів Google Cloud що забезпечують безпеку даних і дрейф адреси, коли вони бувають;

експорт даних. Експорт даних і результатів в BigQuery і Pub/Sub для подальшого аналізу.

Google Cloud Security Command Center (SCC) використовує сильні сторони Google в галузі ШІ, машинного навчання та аналітики великих даних для виявлення загроз. GCP робить акцент на простоті використання, безпечних налаштуваннях за замовчуванням та моделі «нульової довіри» (Zero Trust). Хоча AWS та Azure вважаються більш зрілими на ринку, GCP швидко наздоганяє їх завдяки потужним функціям шифрування та мережевої безпеки.

Вибір між цими інструментами залежить від пріоритетів організації. Якщо корпоративна інфраструктура повністю на AWS і потрібен глибокий, детальний моніторинг, то рішення GuardDuty буде ідеальним вибором. Якщо організація використовує гібридне середовище або вже має великі інвестиції в екосистему

Microsoft, Microsoft Defender for Cloud забезпечить найкращу інтеграцію та комплексний захист. Якщо буде надано пріоритет AI-driven аналітиці загроз, простоті управління та інформаційні ресурси розміщені переважно в середовищі GCP, то Security Command Center буде найкращим рішенням.

Таблиця 1.1

Порівняльна таблиця нативних інструментів для виявлення вторгнень до хмарних корпоративних ресурсів [6-8]

Характеристика	**Amazon Web Services (AWS)**	**Microsoft Azure**	**Google Cloud Platform (GCP)**
Основний інструмент виявлення загроз	Amazon GuardDuty	Microsoft Defender for Cloud (раніше Azure Security Center)	Security Command Center (SCC)
Принцип виявлення	Використовує машинне навчання, аналіз аномалій та інтелект загроз для моніторингу мережевого трафіку (VPC Flow Logs) та журналів подій (CloudTrail, DNS logs).	Комплексна платформа, що використовує ШІ, машинне навчання та розширений інтелект загроз Microsoft (Microsoft Threat Intelligence).	Використовує можливості AI/ML, а також правила виявлення для проактивного моніторингу та оцінки ризиків.
Охоплення платформ	Призначений виключно для середовища AWS.	Мультихмарна підтримка (Azure, AWS, GCP) та гібридні середовища.	Призначений виключно для середовища GCP.
Інтеграція	Глибока інтеграція з іншими сервісами AWS (Security Hub, CloudTrail, Amazon Detective).	Безшовна інтеграція з продуктами Microsoft (Microsoft 365, Active Directory, Azure Sentinel SIEM) та сторонніми рішеннями.	Інтеграція з власними сервісами GCP (BigQuery, Chronicle SIEM), а також з відкритим вихідним кодом.
Ключова перевага	Глибокий та детальний моніторинг активності в межах AWS з високою швидкістю виявлення в реальному часі.	Найкраще підходить для підприємств, які вже використовують екосистему Microsoft, завдяки гібридним та мультихмарним можливостям.	Сильні сторони в аналітиці даних, AI/ML та автоматизації, що підходить для організацій, орієнтованих на інновації та нульову довіру (Zero Trust).

Часто організації застосовують комбінований підхід, використовуючи нативні інструменти як основу, доповнюючи їх сторонніми CNAPP-платформами

для забезпечення мультихмарної видимості.

Оптимальний вибір рішення залежить від конкретних потреб відповідних організацій. Для гібридних середовищ або якщо потрібен високий рівень контролю, підійдуть CNAPP-платформи або комбінація HIDS/SIEM. Якщо організація використовує одного хмарного провайдера і шукає просте, інтегроване рішення, найкращим вибором будуть нативні інструменти провайдера. Для організацій з досвідом та специфічними вимогами до моніторингу трафіку можуть бути корисні NIDS-рішення з відкритим кодом, такі як Suricata.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДО ХМАРНИХ КОРПОРАТИВНИХ РЕСУРСІВ НА БАЗІ AMAZON DETECTIVE

2.1. Призначення та основні функції рішення Amazon Detective

Оскільки інфраструктура додатків та робоче середовище стають складнішими в хмарі, командам безпеки може бути складно виявляти потенційні проблеми та всебічно досліджувати їхню діяльність. Amazon Detective розроблений для того, щоб допомогти пом’якшити ці проблеми за допомогою аналітики та візуалізації на основі машинного навчання [12].

Amazon Detective допомагає вирішувати кілька поширених проблем хмарної безпеки завдяки єдиному огляду активності та підтримці швидкого відстеження з’єднань для виявлення першопричин [12]:

виявлення криптомайнінгу – виявлення незвичайного вихідного трафіку та використання API, що свідчить про встановлення відповідного програмного забезпечення;

захист від DDoS-атак – виявлення джерел перевантаження трафіком та посилань на скомпрометовані ресурси;

відстеження зараження шкідливим програмним забезпеченням – поверхневі ознаки витоку даних та їхнього переміщення тощо.

Amazon Detective – служба безпеки, яка допомагає аналітикам розслідувати потенційні проблеми безпеки. Вона робить це, збираючи дані журналів з AWS CloudTrail, журналів потоків Amazon Virtual Private Cloud (VPC) та інших служб. Amazon Detective використовує машинне навчання, статистичний аналіз та теорію графів для створення пов’язаного набору даних, який називається графіком поведінки безпеки, який можна використовувати для проведення швидших та ефективніших розслідувань безпеки [13].

Amazon Detective допомагає фахівцям аналізувати, досліджувати та швидко

виявляти першопричину виявлених проблем безпеки або підозрілої активності. Amazon 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 Amazon Detective агрегації даних, зведення та контекст допомагають швидко аналізувати та визначати характер і масштаб можливих проблем безпеки [9].

За допомогою рішення Amazon Detective ми можемо отримати доступ до історичних даних про події за період до одного року. Ці дані доступні через набір візуалізацій, які показують зміни в типі та обсязі активності протягом вибраного періоду часу. Amazon Detective пов’язує ці зміни з висновками рішення GuardDuty.

Завдяки автоматичному агрегуванню даних та наданню візуальних інструментів, Amazon Detective дозволяє проводити швидші та ефективніші розслідування безпеки. Ми можемо швидко аналізувати потенційні проблеми та визначати масштаби загроз безпеці.

Розглянемо ключові способи, якими Amazon Detective може допомогти розслідувати підозрілу активність у корпоративному середовищі AWS та аналізувати ресурси для виявлення першопричини проблем безпеки.

Групи пошуку Amazon Detective. Групи пошуку Amazon Detective дозволяють досліджувати кілька дій, пов’язаних з потенційною подією безпеки. Ми можемо проаналізувати першопричину виявлених подій GuardDuty з високим рівнем серйозності за допомогою груп пошуку. Якщо зловмисник намагається скомпрометувати корпоративне середовище AWS, він зазвичай виконує послідовність дій, які генерують численні виявлені події безпеки та незвичайну поведінку [9].

На сторінці груп знахідок у Detective відображаються всі пов’язані групи знахідок, отримані з корпоративного графіка поведінки. Детектив надає інтерактивну візуалізацію кожної групи знахідок, щоб допомогти швидше та ретельніше розслідувати проблеми безпеки. Візуалізація призначена для відображення об’єктів та результатів, пов’язаних з інцидентом безпеки, що

полегшує розуміння зв’язків та першопричин. Це допоможе швидше та ретельніше розслідувати проблеми з меншими зусиллями. Панель візуалізації групи знахідок відображає результати та об’єкти, що стосуються групи знахідок [9].

Розслідування для сортування результатів Amazon Detective. За допомогою розслідувань Amazon Detective ми можемо досліджувати користувачів IAM та ролі IAM, використовуючи індикатори компрометації, які можуть допомогти нам визначити, чи задіяний ресурс в інциденті безпеки. Індикатор компрометації (IoC) – це артефакт, що спостерігається в мережі, системі чи середовищі, який може (з високим рівнем впевненості) ідентифікувати зловмисну активність або інцидент безпеки. За допомогою розслідувань ми можемо максимізувати ефективність, зосередитися на загрозах безпеці та посилити можливості реагування на інциденти.

Detective Investigation використовує моделі машинного навчання та аналітику загроз, щоб виявляти лише найкритичніші та найпідозріліші проблеми, що дозволяє нам зосередитися на розслідуваннях високого рівня. Він автоматично аналізує ресурси у вашому середовищі AWS, щоб виявити потенційні ознаки компрометації або підозрілої активності. Це дозволяє нам виявляти закономірності та розуміти, на які ресурси впливають події безпеки, пропонуючи проактивний підхід до виявлення та пом’якшення загроз [9].

Ми можемо розпочати розслідування з консолі Amazon Detective, виконавши команду «Запуск детективного розслідування». Щоб запустити розслідування програмно, можна скористатися операцією *StartInvestigation* API Amazon Detective. Щоб запустити розслідування за допомогою інтерфейсу командного рядка AWS (AWS CLI), виконайте команду *start-investigation*.

Інтеграція Amazon Detective з Amazon Security Lake. Detective інтегрується з Amazon Security Lake, що означає, що ми можемо запитувати та отримувати необроблені дані журналів, що зберігаються Security Lake. Завдяки цій інтеграції ми можемо збирати журнали та події з наступних джерел, які Security Lake підтримує власно [9]:

події керування AWS CloudTrail версії 1.0 та новіших;

журнали потоків Amazon Virtual Private Cloud (Amazon VPC) версії 1.0 і

новіших;

журнал аудиту служби Amazon Elastic Kubernetes (Amazon EKS) версії 2.0.

Після інтеграції Amazon Detective з Security Lake, Detective починає отримувати необроблені журнали з Security Lake, пов’язані з подіями керування AWS CloudTrail та журналами Amazon VPC Flow. Ми можемо запитувати необроблені журнали, щоб переглядати журнали та події в Detective.

Дослідження об’єму потоку VPC. За допомогою Detective ми можемо інтерактивно перевіряти деталі активності мережевих потоків віртуальної приватної хмари (VPC) корпоративних екземплярів Amazon Elastic Compute Cloud (Amazon EC2) та подів Kubernetes. Detective автоматично збирає журнали потоків VPC з корпоративних контрольованих облікових записів, агрегує їх за екземплярами EC2 та надає візуальні зведення та аналітику щодо цих мережевих потоків.

Для екземпляра EC2 деталі активності для загального обсягу потоку VPC показують взаємодію між екземпляром EC2 та IP-адресами протягом вибраного діапазону часу. Для поду Kubernetes загальний об’єм потоку VPC відображає загальний об’єм байтів, що надходять та надходять з призначеної поду Kubernetes IP-адреси для всіх IP-адрес призначення.

2.2. Архітектура рішення Amazon Detective

Amazon Detective спрощує аналіз, розслідування та швидке виявлення першопричини потенційних проблем безпеки або підозрілої активності. Він автоматично збирає дані журналів з корпоративних ресурсів AWS, а потім використовує машинне навчання, статистичний аналіз та теорію графів для створення пов’язаного набору даних, що дозволяє проводити швидше та ефективніше розслідування безпеки [10].

Для виявлення потенційних проблем безпеки або виявлених недоліків можна використовувати сервіси безпеки AWS, такі як Amazon GuardDuty , Amazon Macie та AWS Security Hub, а також партнерські продукти безпеки. Ці сервіси

надзвичайно корисні для сповіщення про проблеми та направлення до відповідного місця для їх виправлення [10].

Amazon Detective спрощує цей процес, дозволяючи командам безпеки легко розслідувати та швидко знаходити суть виявлених помилок. Він може аналізувати мільйони подій з різних джерел даних, включаючи журнали потоків Amazon Virtual Private Cloud (Amazon VPC), журнали аудиту Amazon Elastic Kubernetes Service (Amazon EKS) та результати Amazon GuardDuty, і автоматично створює єдине інтерактивне представлення корпоративних ресурсів, користувачів та їхньої взаємодії з часом [10].

Основні функції Amazon Detective показано на рисунку 2.1.

На основі подій безпеки Amazon Detective використовує машинне навчання та візуалізацію для створення єдиного, інтерактивного представлення поведінки корпоративних ресурсів та взаємодії між ними з часом. Ми можемо дослідити цей графік поведінки, щоб проаналізувати різні дії, такі як невдалі спроби входу або підозрілі виклики API. Також можна побачити, як ці дії впливають на такі ресурси, як облікові записи AWS та екземпляри Amazon EC2. Ми можемо налаштувати область дії та часову шкалу графіка поведінки для різних завдань [9]:

швидке розслідування будь-якої діяльності, яка виходить за рамки норми;

визначення закономірностей, які можуть свідчити про проблему безпеки;

усвідомлення всіх ресурсів, на які впливає знайдений процес.

Розглянемо взаємодію компонентів Amazon Detective (рисунок 2.1).

Detective витягує з джерел даних події, що залежать від часу, такі як виклики API, спроби входу та мережевий трафік, і застосовує машинне навчання та візуалізацію для створення уявлення про щоденні взаємодії та поведінку ресурсів з плином часу. Guard Duty, Amazon Inspector та Amazon Security Hub – це сервіси, які надають сповіщення та моніторинг безпеки.

Guard Duty керує виявленням загроз, забезпечує постійний моніторинг незвичайної або шкідливої поведінки та захищає облікові записи AWS від сканування портів, тестування на проникнення та навіть майнінгу біткоїнів.

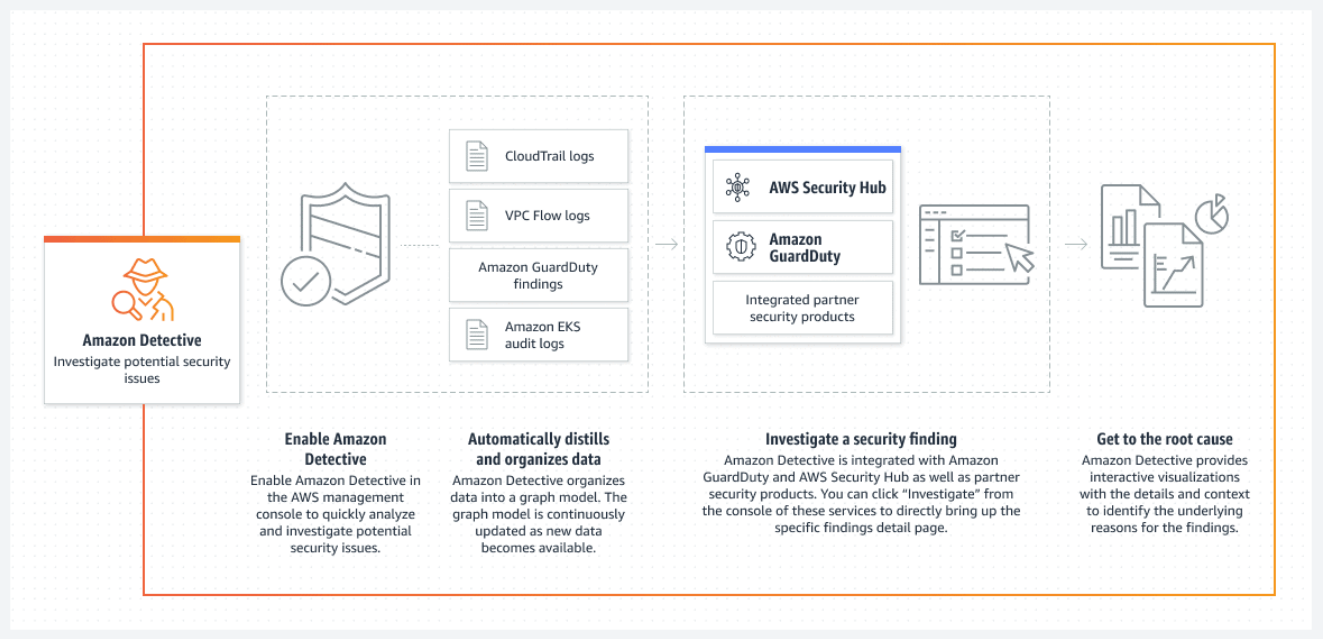

Рис. 2.1. Реалізація функцій та взаємодія Amazon Detective [10]

Amazon Inspector надає оцінки безпеки на рівні додатків та покращує загальну безпеку AWS, автоматизуючи аналіз безпеки мережі та хоста.

Центр безпеки AWS збирає дані безпеки з AWS та інших джерел, щоб допомогти у виявленні тенденцій та встановленні більш просунутої системи безпеки, що дозволяє нам реагувати на ширший спектр загроз безпеці.

Amazon Detective дозволяє розслідувати події безпеки або потенційні загрози з різних джерел. Amazon Detective збирає та інтегрує терабайти даних журналів, перетворює їх для аналізу та надає візуалізації для сприяння виявленню аномалій.

Основні можливості рішення Amazon Detective [10]:

автоматичний збір даних з усіх корпоративних облікових записів AWS. Amazon Detective збирає та аналізує події з таких джерел даних, як журнали AWS CloudTrail, журнали Amazon VPC Flow, журнали аудиту Amazon EKS та результати Amazon GuardDuty, і зберігає агреговані дані до року для аналізу;

об'єднує різнорідні події в графічну модель. Amazon Detective може аналізувати трильйони подій щодо IP-трафіку, операцій управління AWS та зловмисної або несанкціонованої активності з багатьох різних джерел даних, щоб побудувати графічну модель, яка об'єднує дані журналів за допомогою машинного навчання, статистичного аналізу та теорії графів для створення пов'язаного набору

даних для розслідувань безпеки;

інтерактивні візуалізації для ефективного розслідування. Amazon Detective містить інтерактивні візуалізації, які дозволяють досліджувати проблеми швидше та ретельніше, докладаючи менше зусиль. Великі набори даних про події можна легко фільтрувати в певні часові рамки з усіма деталями, контекстом та інструкціями, необхідними для швидкого розслідування;

безперешкодна інтеграція для розслідування виявлених недоліків безпеки. Amazon Detective інтегровано з такими сервісами безпеки AWS, як Amazon GuardDuty та AWS Security Hub, а також з продуктами безпеки партнерів AWS, щоб допомогти у швидкому розслідуванні виявлених недоліків безпеки в цих сервісах;

просте розгортання без попередньої інтеграції джерел даних або складних налаштувань для обслуговування. Немає потреби встановлювати програмне забезпечення, налаштовувати агентів та влаштовувати складні домовленості для обслуговування. Немає потреби вмикати джерела даних, тому нам не доведеться платити за активацію джерел даних, передачу даних або їх зберігання.

Amazon Detective надає єдине уявлення про взаємодію користувачів та ресурсів з плином часу, з усім контекстом та деталями в одному місці, щоб допомогти нам швидко проаналізувати та визначити першопричину виявлення проблеми безпеки.

Amazon Detective автоматично обробляє терабайти IP-трафіку, операцій управління AWS та записів даних про зловмисні або несанкціоновані дії. Він упорядковує дані в графічну модель, яка підсумовує всі зв’язки, пов’язані з безпекою AWS.

Amazon Detective зберігає агреговані дані до року, які відображають зміни в типі та обсязі активності протягом певного періоду часу та пов’язують ці зміни з результатами перевірки безпеки. Amazon Detective генерує візуалізації, що містять дані, необхідні для розслідування та реагування на результати перевірки безпеки.

Основними випадками використання Amazon Detective є [10]:

сортування результатів перевірки безпеки. Сортування часто є першим етапом процесу розслідування. Воно використовується для визначення того, чи є

виявлення справжньою проблемою безпеки чи хибнопозитивним результатом. Використовуючи візуалізації Amazon Detective, ми можемо швидко визначити, чи є виявлення шкідливим чи хибнопозитивним, побачивши, які ресурси, IP-адреси та облікові записи AWS пов'язані з ним, а також пов'язані результати та активність, що відбулися поблизу в певний час або місцезнаходження;

розслідування інцидентів. Коли служби безпеки AWS, такі як Amazon GuardDuty, виявляють знахідку, ми можемо негайно перейти до Amazon Detective та переглянути контекст і дії, пов'язані зі знахідкою, детально переглянути відповідні історичні дії, щоб виявити незвичайні закономірності, а також швидко визначити характер і масштаб першопричини та дії, яка сприяла знахідці;

полювання на загрози. Полювання на загрози – це проактивний аналіз, який виявляє приховані загрози на основі певних підказок або гіпотез. Amazon Detective допомагає у полюванні на загрози, дозволяючи нам зосередитися на певних ресурсах, таких як IP-адреси, облікові записи AWS, VPC та екземпляри EC2, а також надаючи детальну візуалізацію діяльності, пов'язаної з цими ресурсами.

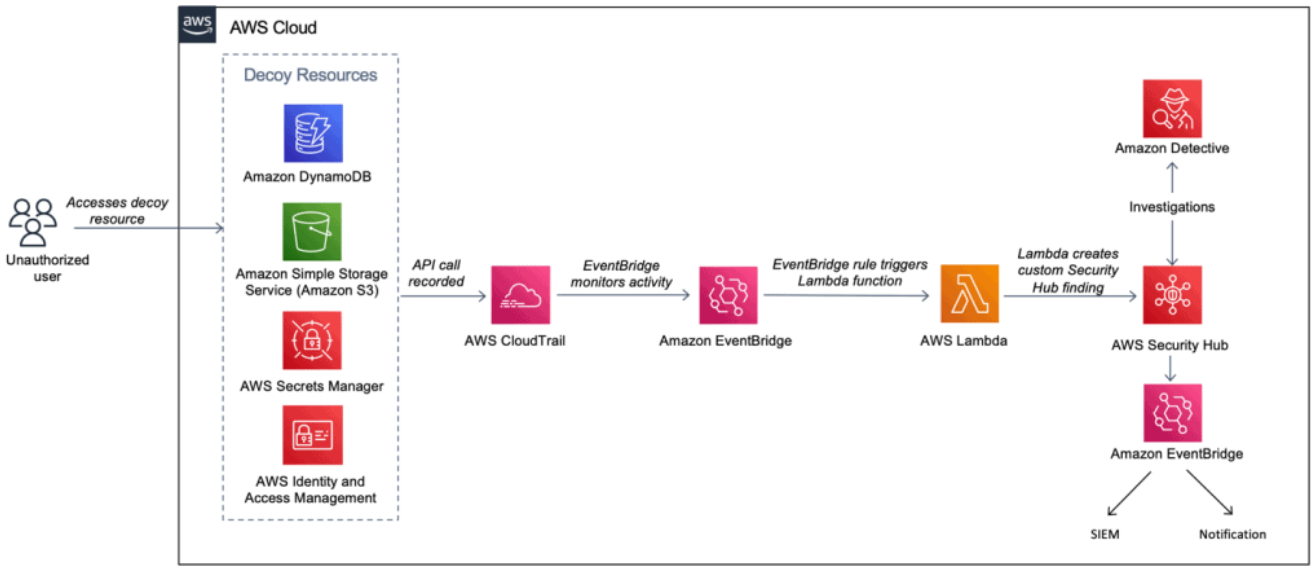

Рис. 2.2. Схема взаємодії компонентів безпеки в AWS Cloud [10]

AWS надає перевагу хмарній безпеці понад усе. Як клієнт AWS, ми маємо доступ до центру обробки даних та мережевої архітектури, розробленої для задоволення потреб організацій, які найбільше дбають про безпеку.

Безпека – це спільна відповідальність між AWS та організацією. Модель спільної відповідальності описує це як безпеку хмари, так і безпеку в хмарі [10]:

безпека хмари – AWS відповідає за захист інфраструктури, яка підтримує сервіси AWS у хмарі AWS. AWS також пропонує сервіси, які можна використовувати безпечно;

безпека в хмарі – сервіс AWS, який ми використовуємо, визначає нашу відповідальність. Інші фактори, такі як конфіденційність корпоративних даних, вимоги організації та чинні закони та правила, також є нашою відповідальністю.

Отже, Amazon Detective автоматично збирає дані журналів з корпоратвиних ресурсів AWS та використовує машинне навчання, статистичний аналіз і теорію графів для створення пов’язаного набору даних, який дозволяє легко проводити швидші та ефективніші розслідування безпеки.

2.3. Порядок функціонування рішення Amazon Detective

Amazon Detective спрощує аналіз, розслідування та швидке визначення першопричини виявлених недоліків безпеки або підозрілої активності. Detective надає інструменти для підтримки всього процесу розслідування. Розслідування в Detective може розпочатися з виявлення, групи виявлених недоліків або об’єкта [9].

Розглянемо фази розслідування в в Amazon Detective. Будь-який процес розслідування в Amazon Detective включає такі етапи [9]:

сортування. Процес розслідування починається, коли нас повідомляють про підозрюваний випадок шкідливої або високоризикової діяльності. Наприклад, нам доручають розглянути результати або сповіщення, виявлені такими сервісами, як Amazon GuardDuty та Amazon Inspector.

На етапі сортування ми визначаємо, чи вважаємо ми, що активність є справді позитивною (справжня зловмисна активність) чи хибнопозитивною (не зловмисна або високоризикова активність). Профілі в Amazon Detective підтримують процес сортування, надаючи уявлення про активність залученої особи. Для справді позитивних випадків ми переходимо до наступного етапу;

визначення обсягу. Під час етапу визначення обсягу діяльності аналітики визначають масштаби зловмисної або високоризикової діяльності та її основну причину. Огляд відповідає на такі типи питань:

Які системи та користувачі були скомпрометовані?

Звідки виникла атака?

Як довго триває атака?

Чи є інша пов'язана діяльність, яку потрібно виявити? Наприклад, якщо зловмисник витягує дані з нашої системи, як він їх отримав?

Візуалізації в Amazon Detective можуть допомогти нам ідентифікувати інші сутності, які були залучені або постраждали;

відповідь. Останній крок є реагування на атаку, щоб зупинити її, мінімізувати збитки та запобігти повторенню подібної атаки.

Розглянемо відправні точки для розслідування в Amazon Detective. Кожне розслідування в Detective має важливу відправну точку. Наприклад, нам можуть доручити розслідування висновку Amazon GuardDuty або AWS Security Hub. Або ж у нас можуть виникнути занепокоєння щодо незвичайної активності для певної IP-адреси.

Типовими відправними точками для розслідування є результати, виявлені GuardDuty, та об'єкти, отримані з вихідних даних в Amazon Detective.

Виявлені GuardDuty результати: GuardDuty використовує дані нашого журналу для виявлення підозрілих випадків шкідливої або високоризикової діяльності. Detective надає ресурси, які допоможуть нам розслідувати ці висновки.

Для кожної знахідки Detective надає пов'язані деталі знахідки. Detective також показує об'єкти, такі як IP-адреси та облікові записи AWS, пов'язані зі знахідкою. Потім ми можемо дослідити активність залучених об'єктів, щоб визначити, чи є виявлена активність справжньою причиною для занепокоєння.

Висновки щодо безпеки AWS, зібрані Центром безпеки: Центр безпеки AWS об'єднує дані про безпеку від різних постачальників в одному місці та надає нам повний огляд стану вашої безпеки в AWS. Центр безпеки усуває складність обробки великих обсягів даних від кількох постачальників. Це зменшує зусилля,

необхідні для управління та покращення безпеки всіх наших облікових записів, ресурсів та робочих навантажень AWS. Detective надає ресурси, які допоможуть нам дослідити ці дані.

Для кожної знахідки Detective надає пов’язані деталі знахідки. Detective також показує об’єкти, такі як IP-адреси та облікові записи AWS, пов’язані зі знахідкою.

Розглянемо сутності, отримані з вихідних даних Detective. З отриманих вихідних даних Detective, Detective витягує такі об’єкти, як IP-адреси та користувачі AWS. Ми можемо використовувати один із них як відправну точку для розслідування.

Amazon Detective надає загальну інформацію про об’єкт, таку як IP-адреса або ім’я користувача. Він також надає детальну інформацію про історію активності. Наприклад, Amazon Detective може повідомити, до яких інших IP-адрес підключався, був підключений або які використовував об’єкт.

Розглянемо хід розслідування в Amazon Detective. Ми можемо використовувати Amazon Detective для дослідження такої сутності, як екземпляр EC2 або користувач AWS. Ми також можемо дослідити результати безпеки.

На рисунку 2.3 показано процес розслідування на загальному рівні в Amazon Detective.

Крок 1: Вибір об’єкта для дослідження.

Переглядаючи результати пошуку в GuardDuty, аналітики можуть дослідити пов’язану сутність у Detective.

Вибір сутності перенаправить нас до профілю сутності в Amazon Detective.

Крок 2: Аналіз візуалізацій на профілях.

Кожен профіль сутності містить набір візуалізацій, що генеруються з графа поведінки. Граф поведінки створюється з файлів журналів та інших даних, що надходять до Detective.

Візуалізації показують активність, пов’язану з сутністю. Ми використовуємо ці візуалізації, щоб відповісти на запитання, щоб визначити, чи є активність сутності незвичайною.

Щоб допомогти у розслідуванні, ми можемо скористатися інструкціями Amazon Detective, що надаються для кожної візуалізації. Інструкції окреслюють відображену інформацію, пропонують запитання, які ми можемо поставити, і пропонують наступні кроки на основі відповідей.

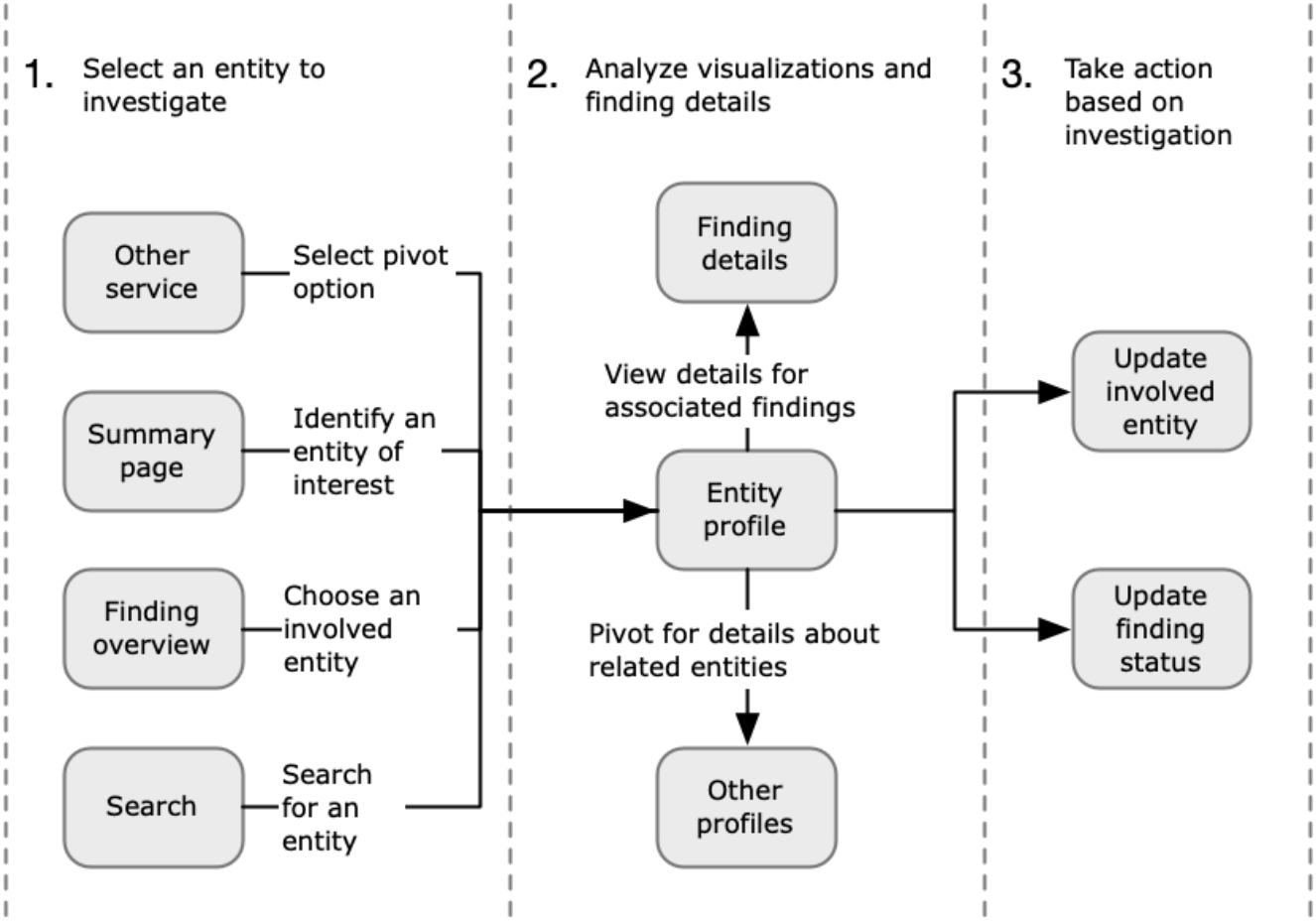

Рис. 2.3. Схема процесу розслідування на загальному рівні в середовищі Amazon Detective

Кожен профіль містить список пов’язаних знахідок. Ми можемо переглянути деталі знахідки та переглянути огляд знахідок.

З профілю сутності ми можемо перейти до інших сутностей та профілів пошуку, щоб детальніше дослідити активність пов’язаних активів.

Крок 3: Вживання заходів.

На основі результатів нашого розслідування вживаються відповідні заходи.

Якщо результат є хибнопозитивним, ми можемо архівувати його. У розділі

«Detective» ми можемо архівувати результати GuardDuty.

В іншому випадку ми вживаємо відповідних заходів для усунення вразливості та зменшення збитків. Наприклад, нам може знадобитися оновити конфігурацію ресурсу.

Рішення Amazon Detective пропонує інноваційний підхід до аналітики безпеки хмарних технологій та розслідування загроз завдяки своїй інтерактивній моделі графових даних. Автоматично агрегуючи та корелюючи дані журналів з таких сервісів, як CloudTrail, VPC Flow Logs та GuardDuty, Amazon Detective забезпечує єдине уявлення про активність облікових записів та ресурсів. Візуальний графік відображає взаємозв'язки між користувачами, активами, дозволами та змінами, щоб виявити тенденції, аномалії та зв'язки, які важко виявити за допомогою традиційного ведення журналу.

Вбудовані алгоритми машинного навчання допомагають виявляти підозрілі закономірності, водночас дозволяючи фільтрувати, перетворювати та динамічно досліджувати пов'язані події з високою швидкістю. Налаштована аналітика через блокноти Jupyter розширює можливості для вирішення нових загроз, адаптованих до кожної організації. Автоматизовані дії та інтеграції ще більше оптимізують робочі процеси реагування на інциденти, що запускаються на основі аналізу графів.

Хоча продумані політики джерел даних та їх збереження необхідні для управління складністю графів з часом, Amazon Detective змінює зміст пошуку загроз у хмарі. Його можливості безперервного аналізу на основі графів дозволяють командам безпеки проактивно досліджувати ризики та швидко відстежувати вплив подій, що розгортаються, в різних облікових записах, без необхідності вручну збирати та корелювати розподілені дані журналів. Це допомагає організаціям підвищити ефективність, результативність та гнучкість реагування на інциденти у сфері хмарної безпеки.

3 ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДО ХМАРНИХ КОРПОРАТИВНИХ РЕСУРСІВ НА БАЗІ AMAZON DETECTIVE

3.1. Порядок застосування рішення Amazon Detective

Розглянемо порядок застосування Amazon Detective для виявлення вторгнень до хмарних корпоративних ресурсів, структурований за основними етапами.

Етап 1: Підготовка та налаштування (Preparation)

Цей етап включає початкове налаштування сервісу в консолі AWS.

Вхід до консолі AWS. Необхідно увійти до консолі керування AWS (AWS Management Console) з правами адміністратора.

Перехід до Amazon Detective. У полі пошуку введіть Amazon Detective і вибираємо відповідний сервіс.

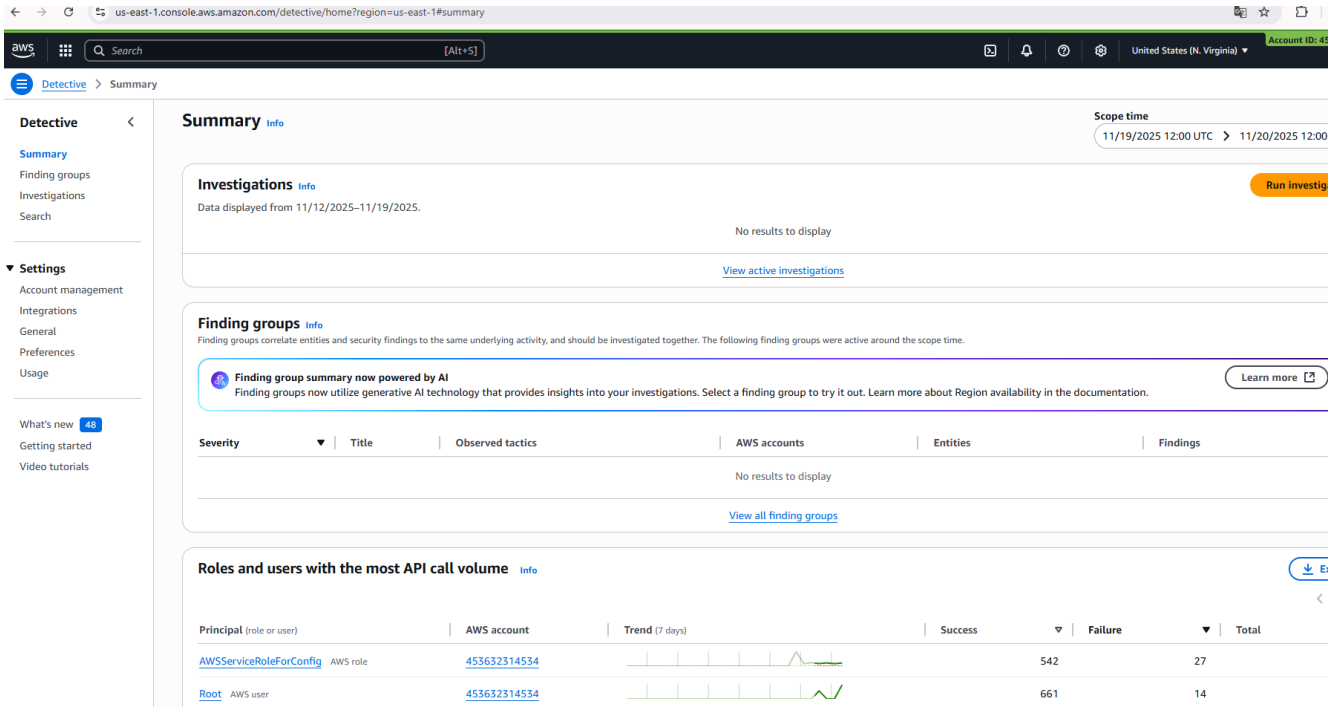

Рис. 3.1. Вкладка Summary Amazon Detective

Сторінка пошуку сервісів AWS з виділеним Amazon Detective.

Активація Amazon Detective. На початковій сторінці Amazon Detective

натисніть кнопку *Get Started* (Почати).

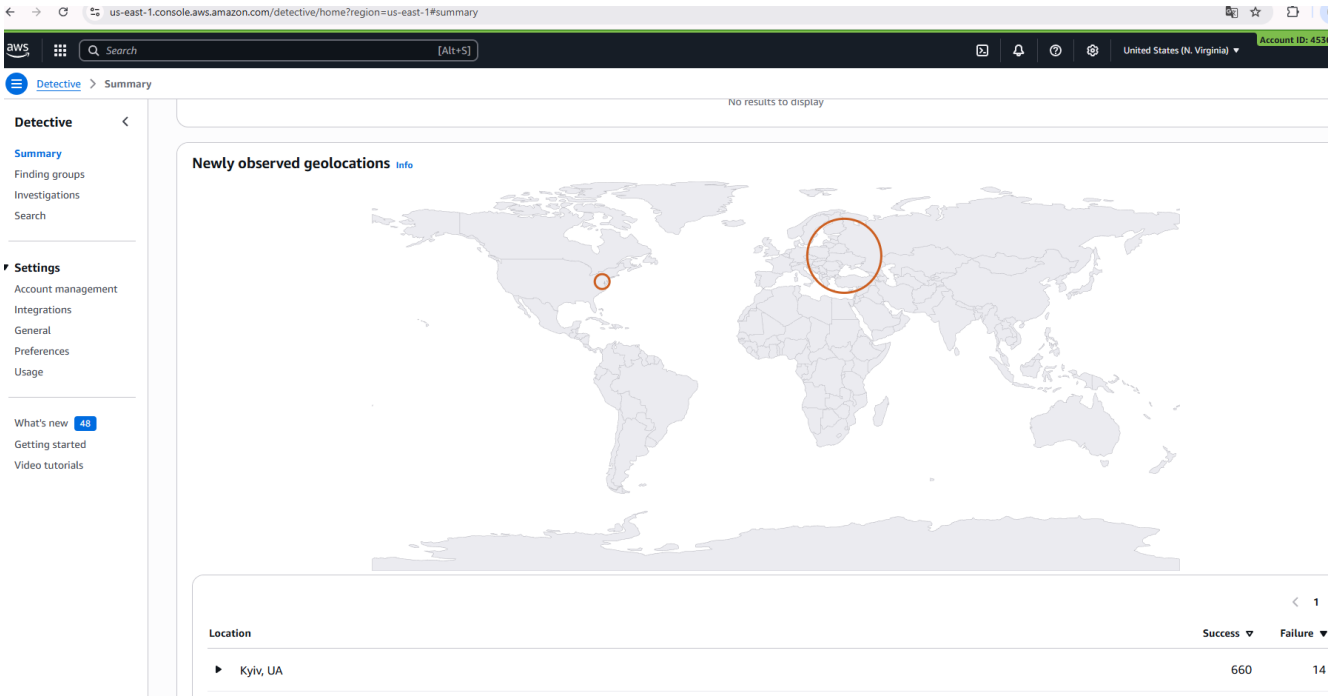

Рис. 3.2. Вкладка Summary Amazon Detective

Сторінка *Welcome to Amazon Detective* з кнопкою *Get Started*.

Налаштування облікового запису адміністратора. Якщо ми використовуємо AWS Organizations, на екрані налаштувань ми зможемо делегувати обліковий запис адміністратора для всієї організації.

Необхідно переконатися, що всі необхідні облікові записи членів (member accounts) вибрані для участі в Detective. Detective автоматично почне збирати дані з цих облікових записів.

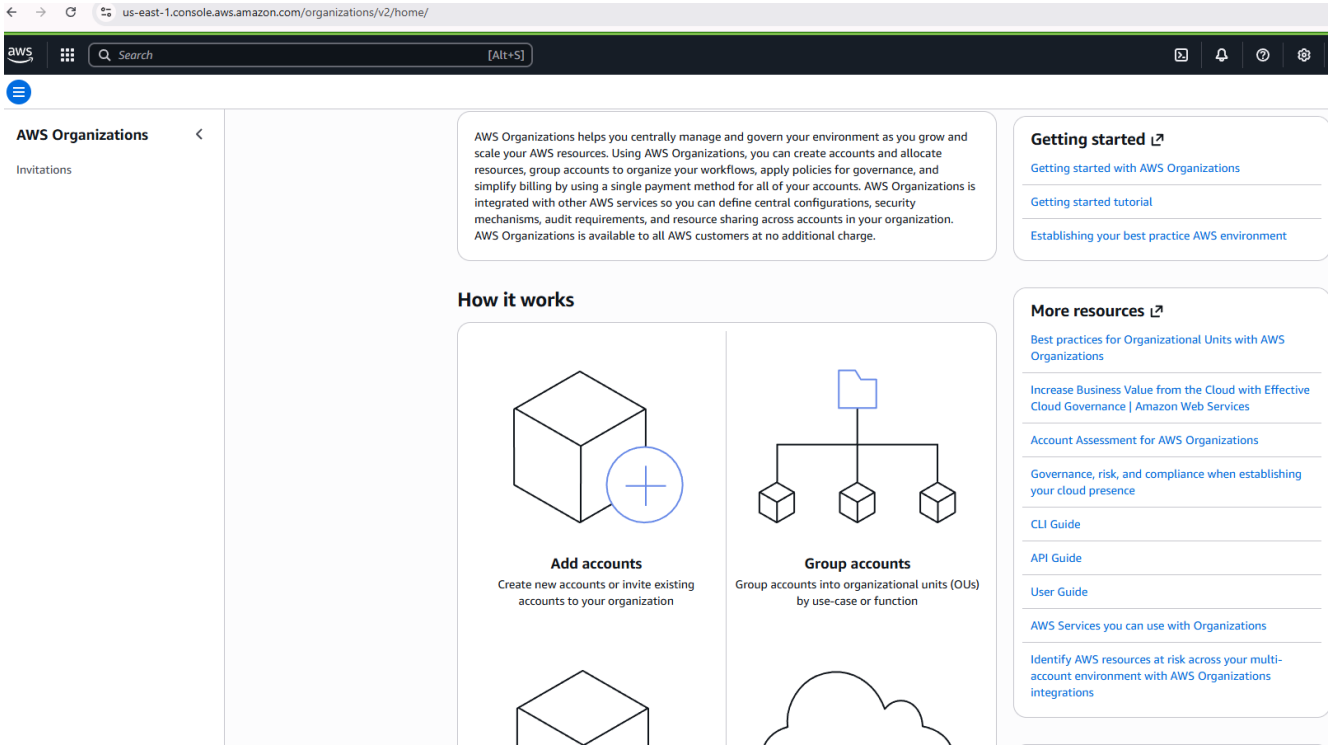

Рис. 3.3. Інструментальна панель AWS Organizations

Екран налаштування делегованого адміністратора та вибору облікових записів членів.

Перевірка інтеграції (автоматично). Amazon Detective автоматично інтегрується з GuardDuty, CloudTrail та VPC Flow Logs. Після активації він починає збір та обробку даних. Через кілька годин (зазвичай до 24 годин) граф поведінки (behavior graph) буде готовий до використання.

Етап 2: Виявлення та аналіз (Detection and Analysis)

Цей етап описує щоденну роботу з сервісом під час активного розслідування.

Отримання сповіщення про загрозу. Розслідування зазвичай починається з виявлення потенційної загрози іншим сервісом безпеки, наприклад Amazon GuardDuty або AWS Security Hub.

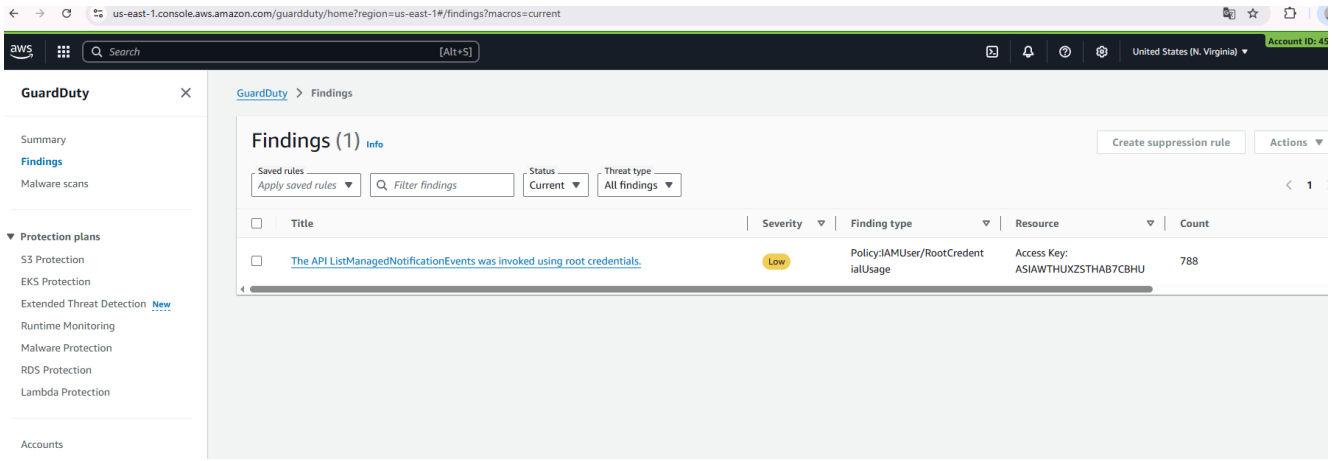

Рис. 3.4. Вкладка Findings Amazon GuardDuty

Список сповіщень (findings) у консолі Amazon GuardDuty або Security Hub.

Перехід до Detective для аналізу. Зі сторінки деталей сповіщення GuardDuty ми використовуємо опцію *Investigate in Detective* (Розслідувати в Detective).

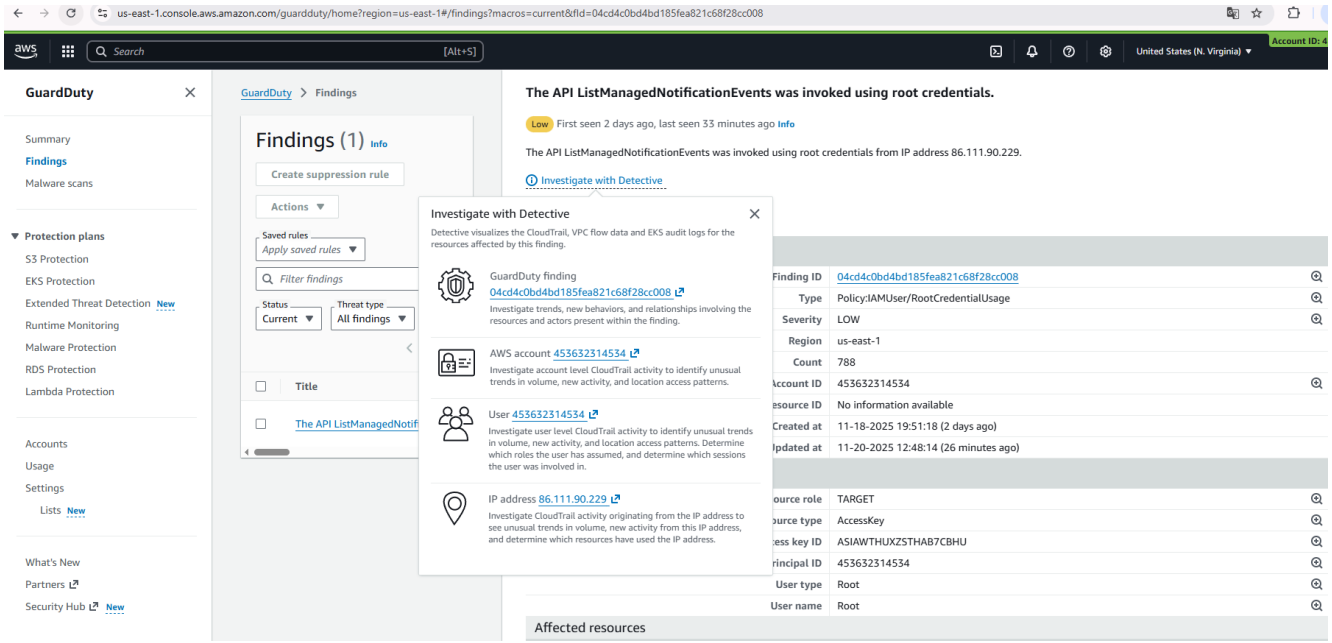

Рис. 3.5. Опція *Investigate in Detective*

Деталі сповіщення GuardDuty з виділеною кнопкою *Investigate in Detective*.

Аналіз профілю сутності (Entity Profile). Ми переходимо на сторінку профілю сутності в Amazon Detective (наприклад, профілю IP-адреси, користувача IAM або екземпляра EC2, пов’язаного зі сповіщенням).

На цій сторінці представлено візуалізовану інформацію про активність

сутності за певний проміжок часу.

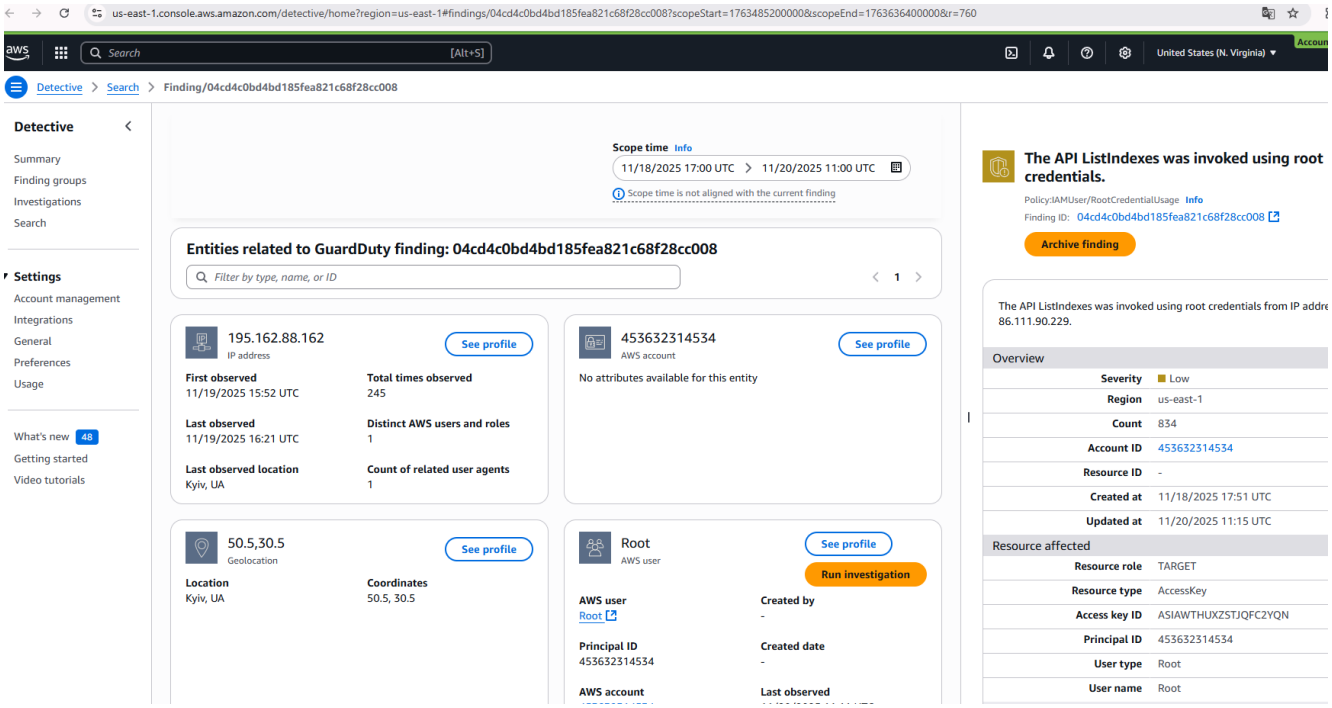

Рис. 3.6. Результати Entities related to GuardDuty finding

Огляд сторінки профілю сутності (наприклад, IP-адреси) в Amazon Detective, що показує графіки обсягу трафіку та кількість викликів API.

Вивчення графа поведінки (Behavior Graph). Необхідно використовувати інтерактивні візуалізації (графіки), щоб зрозуміти зв’язки між різними елементами: які облікові записи IAM використовували цю IP-адресу, до яких екземплярів EC2 зверталися, які ролі задіяні.

Приклад інтерактивного графа поведінки, що показує зв’язки між користувачем, IP-адресою та екземпляром EC2.

Аналіз часової шкали активності (Activity Timeline). Необхідно звернути увагу на часову шкалу подій, щоб побачити, що відбувалося до, під час та після інциденту. Це допомагає визначити повний обсяг вторгнення та хронологію дій зловмисника. Використовуємо детальну часову шкалу активності користувача IAM (API calls) з аномальною поведінкою.

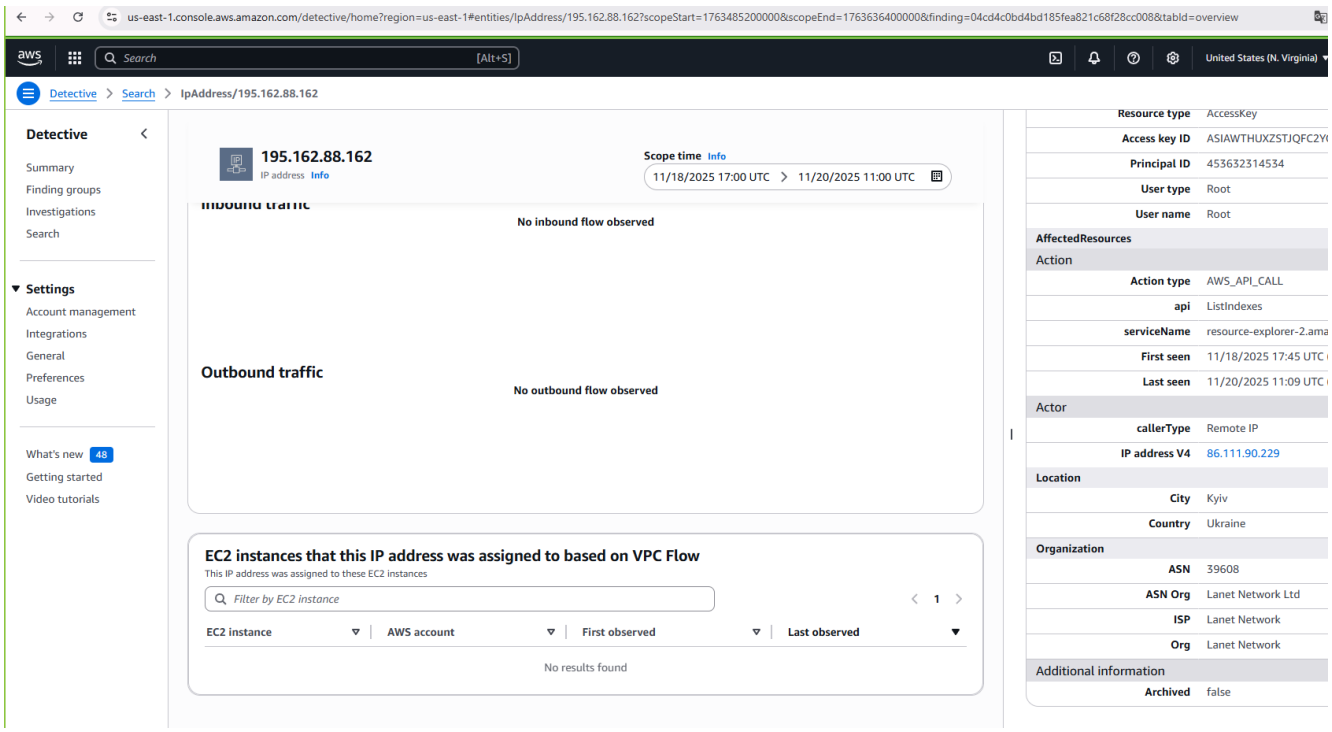

Рис. 3.7. Дані щодо EC2 instances that this IP address was assigned to based on VPC Flow

Етап 3: Локалізація та усунення (Containment and Eradication)

На цьому етапі ви використовуєте висновки з Detective для вжиття заходів.

Ізоляція скомпрометованих ресурсів. На основі аналізу виявлених IP-адрес або екземплярів EC2, перейдіть до консолі VPC або EC2.

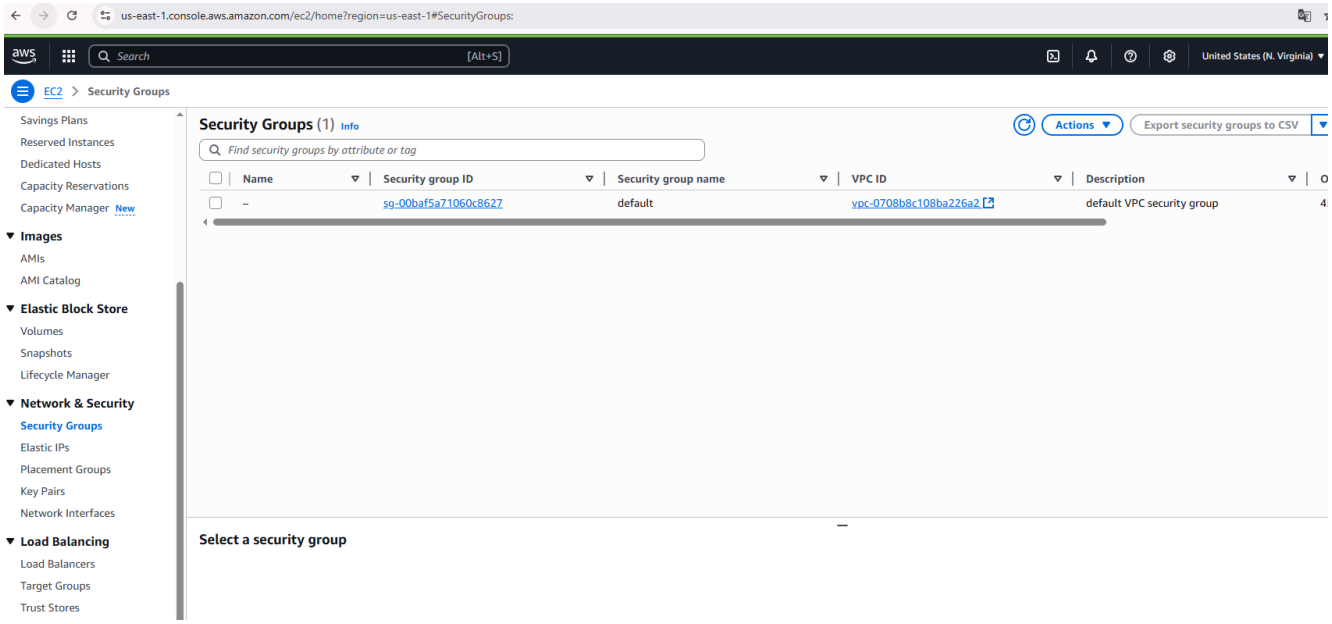

Рис. 3.9. Вкладка Security Groups EC2

Необхідно змінити налаштування груп безпеки (Security Groups) для ізоляції скомпрометованого екземпляра (наприклад, закрийте весь вхідний/вихідний трафік).

Налаштування правил Security Group в консолі EC2 для блокування трафіку.

Управління ідентифікацією (IAM). Якщо скомпрометовано облікові дані користувача IAM, необхідно негайно відкликати їх та скинути паролі.

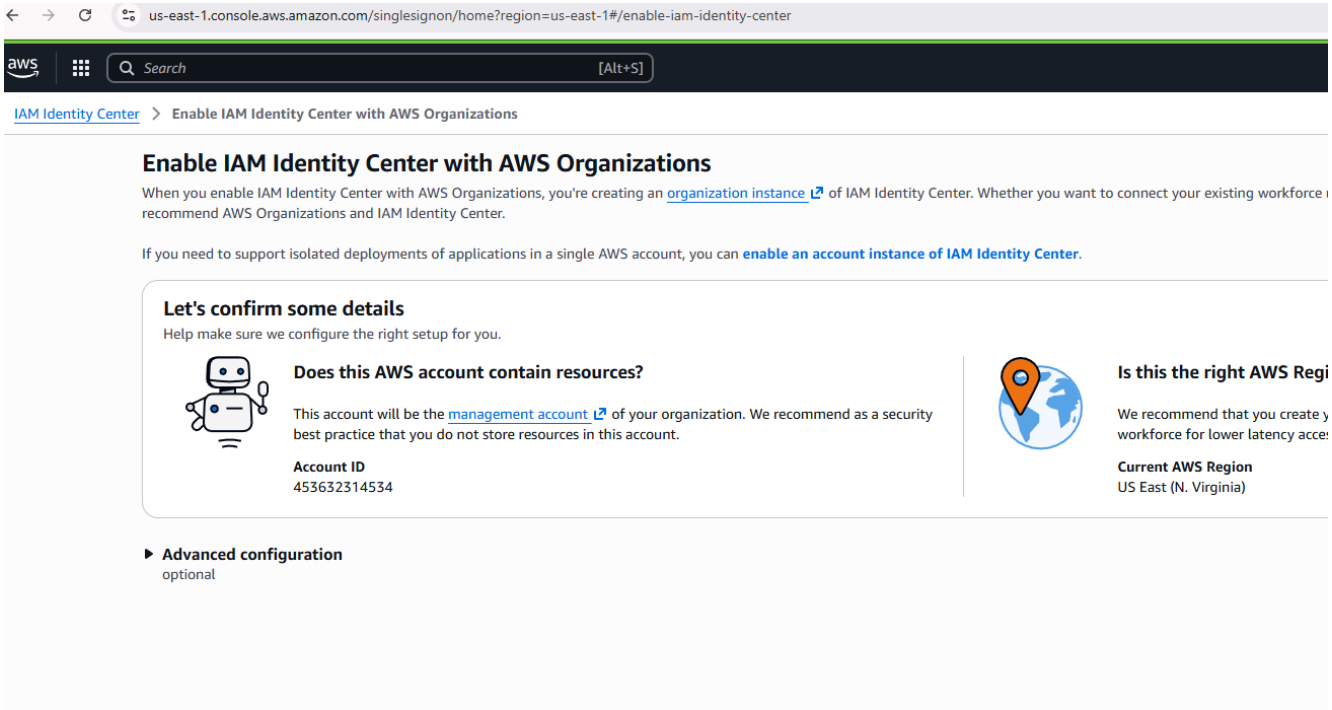

Рис. 3.10. Вкладка Enable IAM Identity Center with AWS Organizations

Сторінка управління користувачем IAM з опцією відкликання облікових даних.

Етап 4: Звітування та дії після інциденту (Reporting and Post-incident Activity)

Експорт даних для звіту. Amazon Detective дозволяє експортувати результати аналізу та візуалізації для документування інциденту та підготовки звіту для керівництва.

Розглянутий порядок забезпечує чітку послідовність дій для використання Amazon Detective як ключового інструменту в процесі реагування на інциденти кібербезпеки.

3.2. Технологія виявлення вторгнень до хмарних корпоративних ресурсів

Необхідно відмітити, що в Amazon Detective проводиться розслідування, використовуючи дані з графа поведінки. Граф поведінки – це зв’язаний набір даних, згенерованих з вихідних даних Amazon Detective, які надходять з одного або кількох облікових записів Amazon Web Services (AWS).

Граф поведінки використовує вихідні дані для виконання наступного:

створення загальної картини корпоративних систем, користувачів та взаємодії між ними з плином часу;

виконання детальнішого аналізу конкретної діяльності, щоб отримати відповіді на запитання, що виникають під час проведення розслідувань;

співвідношення колекції висновків, сутностей та доказів, які можуть бути пов’язані з однією подією або проблемою безпеки.

Все вилучення, моделювання та аналітика даних графа поведінки відбувається в контексті кожного окремого графа поведінки. Кожен граф поведінки містить дані з одного або кількох облікових записів. Коли обліковий запис увімкнено в Detective, він стає обліковим записом адміністратора для графа поведінки та вибирає облікові записи учасників для графа поведінки. Граф поведінки може містити до 1200 облікових записів учасників.

Щоб надати необроблені дані для розслідувань, Detective об’єднує дані з усього корпоративного середовища AWS та за його межами, включаючи наступне:

дані журналів, включаючи Amazon Virtual Private Cloud (Amazon VPC) та AWS CloudTrail;

висновки Amazon GuardDuty;

висновки з Центру безпеки AWS.

Коли надходять нові дані, Detective використовує комбінацію вилучення та аналітики для заповнення графа поведінки (рисунок 3.11).

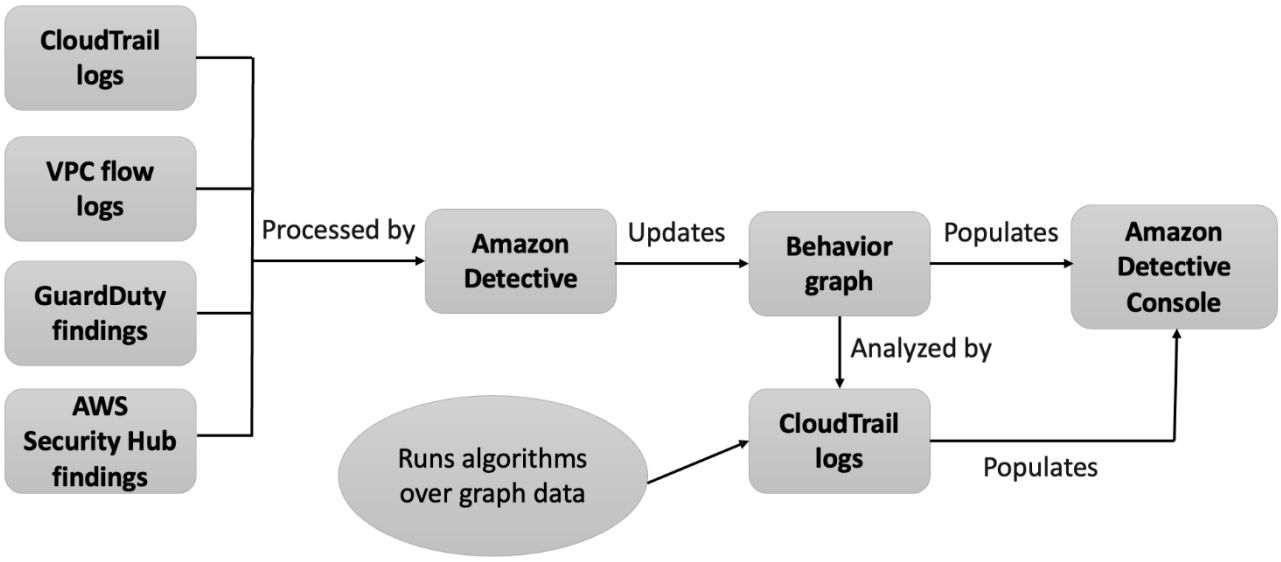

Рис. 3.11. Схема створення графа поведінки [10]

Вилучення Amazon Detective базується на налаштованих правилах відображення. Правило відображення по суті говорить: «Щоразу, коли ви бачите цей фрагмент даних, використовуйте його певним чином для оновлення даних графіка поведінки».

Наприклад, вхідний запис вихідних даних Amazon Detective може містити IP-адресу. Якщо це так, Amazon Detective використовує інформацію з цього запису для створення нової сутності IP-адреси або оновлення існуючої сутності IP-адреси.

Аналітика в Amazon Detective – це складніші алгоритми, які аналізують дані, щоб отримати уявлення про активність, пов’язану з сутностями. Наприклад, один тип аналітики в Amazon Detective аналізує частоту активності шляхом запуску алгоритмів. Для об’єктів, які здійснюють виклики API, алгоритм шукає виклики API, які об’єкт зазвичай не використовує. Алгоритм також шукає значне зростання кількості викликів API.

Аналітичні дані підтримують розслідування, надаючи відповіді на ключові запитання аналітиків, і часто використовуються для заповнення панелей результатів та профілів сутностей.

Один зі шляхів розслідування знахідки полягає у порівнянні активності протягом часу, визначеного для знахідки, з активністю, яка мала місце до її

виявлення. Активність, яка раніше не спостерігалася, може бути більш підозрілою.

Деякі панелі профілів Amazon Detective виділяють активність, яка не спостерігалася протягом періоду часу до знахідки. Кілька панелей профілів також відображають базове значення, щоб показати середню активність протягом 45 днів до часу визначення. Час визначення – це зведення активності об'єкта з плином часу.

Зі збільшенням кількості даних, отриманих у графіку поведінки, Detective формує точнішу картину того, яка діяльність є нормальною в організації, а яка – незвичайною.

Однак, щоб створити таку картину, Amazon Detective потрібен доступ щонайменше до двох тижнів даних. Зрілість аналізу Amazon Detective також зростає зі збільшенням кількості облікових записів у графі поведінки.

Перші два тижні після активації Amazon Detective вважаються періодом навчання. Протягом цього періоду на панелях профілю, які порівнюють активність за певний час з попередньою активністю, відображається повідомлення про те, що Amazon Detective перебуває у періоді навчання.

Протягом пробного періоду Detective рекомендує додавати якомога більше облікових записів учасників до графіка поведінки. Це надає Detective більший обсяг даних, що дозволяє йому створювати точнішу картину звичайної активності організації.

Структура даних графу поведінки визначає структуру витягнутих та проаналізованих даних. Вона також визначає, як вихідні дані відображаються на графі поведінки.

Розглянемо основні типи елементів у структурі даних графа поведінки. Структура даних графа поведінки складається з наступних інформаційних елементів.

Сутність. Сутність представляє елемент, отриманий з вихідних даних детектива. Кожна сутність має тип, який визначає тип об'єкта, який вона представляє. Прикладами типів сутностей є IP-адреси, екземпляри Amazon EC2 та користувачі AWS.

Для кожної сутності вихідні дані також використовуються для заповнення

властивостей сутності. Значення властивостей можуть бути отримані безпосередньо з вихідних записів або агреговані з кількох записів.

Деякі властивості складаються з одного скалярного або агрегованого значення. Наприклад, для екземпляра EC2 Detective відстежує тип екземпляра та загальну кількість оброблених байтів.

Властивості часових рядів відстежують активність з плином часу. Наприклад, для екземпляра EC2 Detective з плином часу відстежує унікальні порти, які він використовував.

Зв'язки. Зв'язок відображає діяльність, що відбувається між окремими сутностями. Зв'язки також витягуються з вихідних даних Amazon Detective.

Подібно до сутності, зв'язок має тип, який визначає типи задіяних сутностей та напрямок з'єднання. Прикладом типу зв'язку є IP-адреси, що підключаються до екземплярів EC2.

Для кожного окремого зв'язку, такого як підключення певної IP-адреси до певного екземпляра, Detective відстежує випадки з плином часу.

Розглянемо типи сутностей у структурі даних графа поведінки. Структура даних графу поведінки складається з типів сутностей та зв'язків, які виконують наступне:

відстеженні серверів, IP-адрес та агентів користувачів, що використовуються;

відстеження користувачів, ролей та облікових записів AWS, що використовуються;

відстеження мережевих підключень та авторизації, що відбуваються у корпоративному середовищі AWS.

Вихідні дані, що використовуються в графі поведінки Amazon Detective (рисунок 3.12).

Для заповнення графіка поведінки Amazon Detective використовує вихідні дані з облікового запису адміністратора графа поведінки та облікових записів учасників.

За допомогою Detective ми можемо отримати доступ до історичних даних про

події за період до одного року. Ці дані доступні через набір візуалізацій, які показують зміни в типі та обсязі активності протягом вибраного періоду часу. Detective пов’язує ці зміни з висновками GuardDuty.

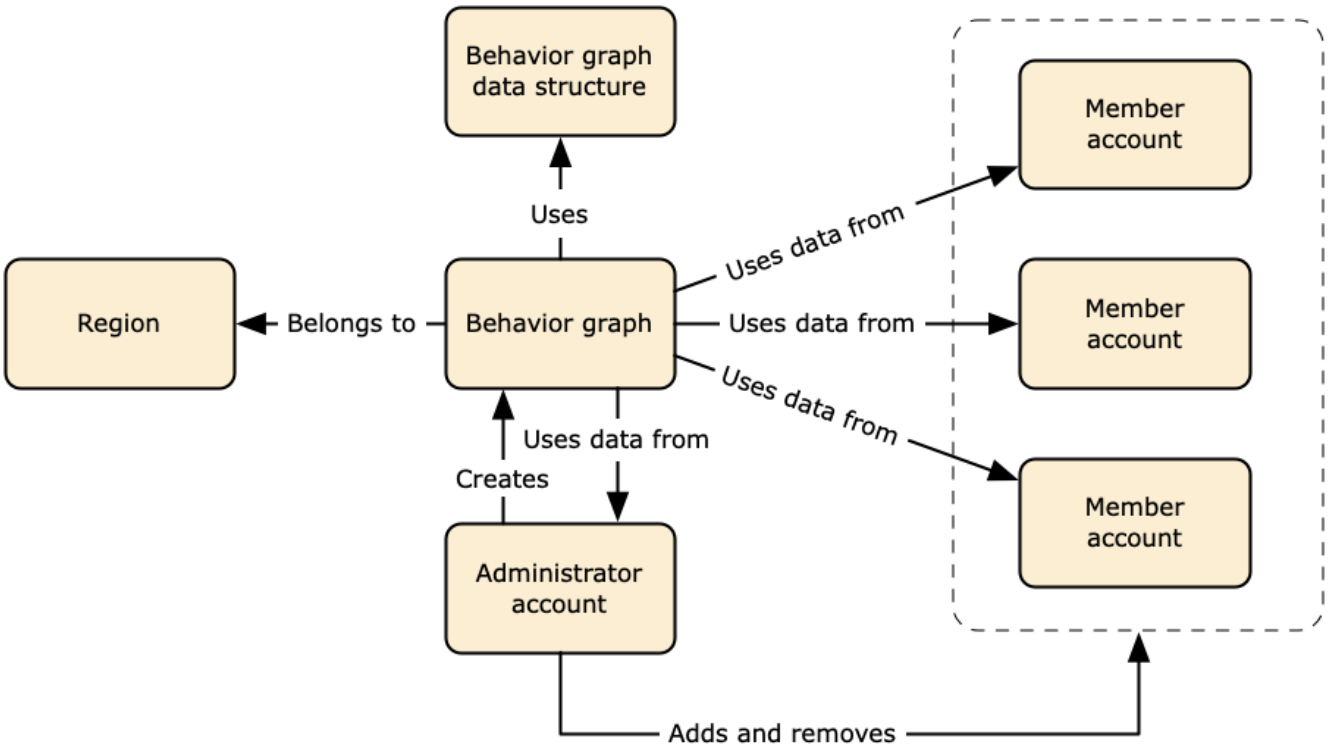

Рис. 3.12. Вихідні дані, що використовуються в графі поведінки Amazon Detective [9]

Розглянемо типи основних джерел даних у Amazon Detective. Amazon Detective отримує дані з таких типів журналів AWS:

журнали AWS CloudTrail;

журнали потоків Amazon Virtual Private Cloud (Amazon VPC) (завантажує записи IPv4 та IPv6, але не MAC-адреси, створені адаптерами Elastic Fabric; завантажує записи журналу, коли значення поля log-status перебуває у стані OK; завантажує журнали потоків, створені екземплярами Amazon Elastic Compute Cloud, що працюють лише в цих VPC. Жодні інші ресурси, такі як шлюзи NAT, екземпляри RDS або кластери Fargate, не використовуються; обробляє як прийнятий, так і відхилений трафік);

для облікових записів, зареєстрованих у GuardDuty, Detective також отримує

дані GuardDuty.

Amazon Detective використовує події журналів потоків CloudTrail та VPC, використовуючи незалежні та дубліковані потоки журналів потоків CloudTrail та VPC. Ці процеси не впливають на існуючі конфігурації журналів потоків CloudTrail та VPC та не використовують їх. Вони також не впливають на продуктивність цих послуг та не збільшують їх вартість.

Типи додаткових джерел даних у Amazon Detective: Detective пропонує додаткові пакети вихідних даних на додаток до трьох джерел даних, що пропонуються в основному пакеті Detective (основний пакет включає журнали AWS CloudTrail, журнали VPC Flow та результати GuardDuty). Додатковий пакет джерел даних можна запустити або зупинити для графіка поведінки в будь-який час.

Як Detective отримує та зберігає вихідні дані? Коли функцію «Detective» увімкнено, вона починає отримувати вихідні дані з облікового запису адміністратора графа поведінки. Коли облікові записи учасників додаються до графа поведінки, «Detective» також починає використовувати дані з цих облікових записів учасників.

Вихідні дані Detective складаються зі структурованих та оброблених версій оригінальних каналів. Для підтримки аналітики детектива, Detective зберігає копії вихідних даних Detective.

Процес отримання даних Detective передає дані до корзин Amazon Simple Storage Service (Amazon S3) у сховищі вихідних даних Detective. Коли надходять нові вихідні дані, інші компоненти Detective підбирають їх та запускають процеси вилучення та аналітики.

Як Detective забезпечує дотримання квоти обсягу даних для графіків поведінки? Amazon Detective має суворі квоти на обсяг даних, які він дозволяє використовувати в кожному графі поведінки. Обсяг даних – це кількість даних, що надходять на графік поведінки Amazon Detective за день.

Amazon Detective застосовує ці квоти, коли обліковий запис адміністратора вмикає Amazon Detective, а також коли обліковий запис учасника приймає

запрошення зробити внесок у створення графіка поведінки.

Якщо обсяг даних для облікового запису адміністратора перевищує 10 ТБ на день, то обліковий запис адміністратора не може ввімкнути Amazon Detective.

Якщо доданий обсяг даних з облікового запису учасника призведе до того, що графік поведінки перевищить 10 ТБ на день, обліковий запис учасника не можна буде ввімкнути.

Обсяг даних для графа поведінки також може природним чином зростати з часом. Amazon Detective щодня перевіряє обсяг даних графа поведінки, щоб переконатися, що він не перевищує квоту.

Якщо обсяг даних графа поведінки наближається до квоти, Detective відображає попередження на консолі. Щоб уникнути перевищення квоти, можна видалити облікові записи учасників.

Якщо обсяг даних графа поведінки перевищує 10 ТБ на день, то додати новий обліковий запис учасника до графіка поведінки неможливо.

Якщо обсяг даних графіка поведінки перевищує 15 ТБ на день, Amazon Detective припиняє надходження даних до графіка поведінки. Квота 15 ТБ на день відображає як нормальний обсяг даних, так і піки обсягу даних. Коли ця квота досягнута, нові дані до графіка поведінки не надходять, але існуючі дані не видаляються. Ми все ще можемо використовувати ці історичні дані для розслідування. Консоль відображає повідомлення про те, що надходження даних для графіка поведінки призупинено.

Якщо надходження даних призупинено, нам потрібно звернутися до служби підтримки, щоб його знову ввімкнути. Якщо можливо, перш ніж звертатися до служби підтримки, спробуйте видалити облікові записи учасників, щоб обсяг даних став меншим за квоту. Це полегшить повторне ввімкнення надходження даних для графа поведінки.

3.3. Рекомендації щодо виявлення вторгнень до хмарних корпоративних ресурсів

Виявлення загроз у хмарі – це практика виявлення, аналізу та реагування на загрози безпеці в середовищах хмарних обчислень за допомогою спеціалізованих інструментів і методів, розроблених для динамічної інфраструктури на основі API. На відміну від традиційної безпеки на основі периметра, виявлення загроз у хмарі працює в розподілених робочих навантаженнях, безсерверних функціях, контейнерах і багатохмарних розгортаннях, де активи з’являються та зникають за лічені хвилини [16].

Ефективне виявлення хмарних загроз вимагає поведінкової аналітики, машинного навчання та можливостей автоматизованого реагування, які розуміють тимчасові ресурси, атаки, керовані API, та модель спільної відповідальності, що визначає межі безпеки хмари.

Для ефективного виявлення вторгнень до хмарних корпоративних ресурсів рекомендується застосовувати комплексний підхід [14-16], який поєднує технології, процеси та навчання персоналу. Основні рекомендації наступні:

Технічні та процедурні заходи

впровадження комплексного моніторингу та журналювання (Logging and Monitoring):

збір журналів. Збирайте та централізуйте журнали подій з усіх хмарних ресурсів (віртуальних машин, баз даних, брандмауерів, балансувальників навантаження, дій користувачів, зміни політик IAM тощо);

використання систем SIEM/CDR. Аналізуйте зібрані дані в режимі реального часу за допомогою систем керування інформацією про безпеку та подіями (SIEM) або систем виявлення та реагування на хмарні загрози (CDR) для виявлення аномалій та підозрілої активності;

використання поведінкової аналітики (UEBA). Застосовуйте аналітику поведінки користувачів та об’єктів для встановлення базових показників «нормальної» активності та виявлення відхилень, що можуть свідчити про

несанкціонований доступ або зловмисну діяльність.

застосування спеціалізованих інструментів виявлення вторгнень (IDS):

мережеві IDS (NIDS). Використовуйте NIDS, адаптовані для хмарних середовищ (наприклад, AWS GuardDuty, Google Cloud IDS), для моніторингу мережевого трафіку та виявлення загроз на основі відомих сигнатур атак та поведінкових шаблонів;

хостові IDS (HIDS). Розгортайте HIDS на віртуальних машинах для моніторингу системних подій на рівні хоста.

управління ідентифікацією та доступом (IAM):

принцип найменших привілеїв. Надавайте користувачам та програмам лише мінімально необхідні дозволи (принцип найменших привілеїв);

багатофакторна автентифікація (MFA). Забезпечте використання MFA для всіх облікових записів, особливо привілейованих;

регулярний аудит доступу. Періодично переглядайте та оновлюйте права доступу.

управління конфігурацією та вразливостями:

моніторинг стану хмарної безпеки (CSPM). Використовуйте інструменти CSPM для постійного моніторингу хмарного середовища на предмет помилок конфігурації та недотримання стандартів безпеки;

регулярне сканування вразливостей. Періодично проводьте сканування вразливостей та застосовуйте оновлення безпеки (патчі).

шифрування даних:

забезпечте шифрування даних як під час передачі (in transit), так і під час зберігання (at rest).

Організаційні заходи

розробка та тестування Плану реагування на інциденти. Створіть чіткий, спеціалізований для хмари План реагування на інциденти, який визначає ролі, обов’язки та процедури комунікації. Регулярно проводьте навчання та симуляції інцидентів для перевірки його ефективності;

навчання персоналу. Проводьте регулярні тренінги з кібербезпеки для

співробітників, щоб підвищити їхню обізнаність про загрози та правила безпечного використання хмарних ресурсів;

прийняття моделі «Нульової довіри» (Zero Trust). Виходьте з припущення, що будь-який користувач чи пристрій потенційно може бути скомпрометований, і постійно перевіряйте та підтверджуйте їхню легітимність.

В кваліфікаційній роботі було розглянуто рішення Amazon Detective. Amazon Detective – це інструмент AWS, який спрощує аналіз, розслідування та швидке виявлення першопричин потенційних проблем безпеки або підозрілої активності. Він автоматично збирає дані журналів із ваших ресурсів AWS (AWS CloudTrail, Amazon VPC Flow Logs, Amazon GuardDuty findings) і використовує машинне навчання та графову теорію для створення пов’язаного набору даних.

Основними рекомендаціями щодо його застосування для виявлення вторгнень є:

попередня інтеграція та налаштування

обов’язкова інтеграція з Amazon GuardDuty. Amazon Detective працює на основі даних, зібраних іншими службами. Передумовою для використання Detective є активований Amazon GuardDuty (служба інтелектуального виявлення загроз, яка відстежує зловмисну активність);

інтеграція з AWS Security Hub. Активуйте інтеграцію з AWS Security Hub, щоб централізувати всі виявлені проблеми безпеки та використовувати Detective для їх детального розслідування;

збір необхідних даних. Переконайтеся, що активовано збір журналів CloudTrail (журнали дій API) та VPC Flow Logs (журнали мережевого трафіку);

налаштування частоти оновлення GuardDuty. Рекомендується змінити стандартну частоту експорту оновлень GuardDuty з 6 годин до 15 хвилин, щоб пришвидшити відображення актуальних даних у Detective;

централізоване управління обліковими записами. Використовуйте AWS Organizations для централізованого керування Detective на всіх облікових записах, призначивши один обліковий запис як адміністратора Detective.

використання можливостей Amazon Detective

аналіз Finding Groups (груп виявлень). Detective автоматично групує пов’язані знахідки з різних сервісів в єдиний інцидент. Використовуйте ці групи для отримання цілісної картини події, включаючи задіяні сутності (користувачі, IP-адреси, екземпляри EC2) та використані тактики згідно з фреймворком MITRE ATT&CK;

візуалізація активності. Використовуйте інтерактивні графіки (behavior graphs) для візуалізації взаємозв’язків між ресурсами та їхньої поведінки в часі. Це допомагає швидко визначити, які ресурси були скомпрометовані та як відбувалося поширення вторгнення;

дослідження сутностей (Entity investigation). Детально аналізуйте профілі конкретних сутностей, таких як користувачі IAM або екземпляри EC2. Detective надає інформацію про кількість успішних/невдалих викликів API, незвичні IP-адреси та часові рамки активності, що допомагає виявити аномалії;

використання функції Detective Investigation для IAM. Ця функція допомагає визначити, чи був обліковий запис IAM задіяний у підозрілій активності або скомпрометований, аналізуючи його поведінку на відповідність відомим TTP зловмисників;

проактивний пошук загроз (Threat hunting). Не обмежуйтесь лише розслідуванням автоматичних сповіщень. Використовуйте потужні функції пошуку та аналізу Detective для проактивного виявлення потенційних загроз у вашому середовищі, навіть якщо вони ще не були ідентифіковані автоматичними засобами.

інтеграція в операційні процеси

розробка Плану реагування на інциденти. Інтегруйте використання Amazon Detective у ваш План реагування на інциденти. Чітко визначте, як аналітики безпеки будуть використовувати інструмент для швидкого розслідування та мінімізації шкоди;

автоматизація з AWS Security Hub та EventBridge. Налаштуйте автоматичні сповіщення через Amazon EventBridge або AWS Security Hub, щоб миттєво реагувати на критичні знахідки та запускати процеси розслідування в Detective.

регулярне навчання команди. Переконайтеся, що ваша команда безпеки має достатню кваліфікацію для роботи з графовими візуалізаціями та даними Amazon Detective, щоб максимально використовувати потенціал інструменту.

ВИСНОВКИ

В роботі досліджено проблему виявлення вторгнень до хмарних корпоративних ресурсів, визначено його мету та завдання. Вразливості хмарних середовищ стають дедалі поширенішими, і організаціям надзвичайно важко керувати високо розподіленими та динамічними хмарними середовищами. Виявлення вторгнень – це практика моніторингу корпоративної мережі, серверів, робочих станцій та інших IT-активів на предмет будь-якої підозрілої активності, зловмисних дій або порушень певних політик. Ця практика є невід'ємною складовою безпеки інфраструктури будь-якої організації.

Визначено існуючі підходи до виявлення вторгнень до хмарних корпоративних ресурсів. Виявлення вторгнень до хмарних корпоративних ресурсів необхідно розглядати на трьох різних рівнях: рівень хмари; мережевий рівень; рівень обчислення (віртуальні машини, контейнери тощо).

Проаналізовано існуючі рішення для виявлення вторгнень до хмарних корпоративних ресурсів. Аналіз існуючих рішень для виявлення вторгнень до хмарних корпоративних ресурсів охоплює широкий спектр технологій, які розвинулися від традиційних систем виявлення вторгнень до комплексних платформ безпеки хмарних застосунків. Проведено порівняльний аналіз власних (нативних) інструментів виявлення вторгнень від провідних хмарних провайдерів.

Визначено призначення, основні функції та склад рішення Amazon Detective. Рішення Amazon Detective. Amazon Detective – служба безпеки, яка допомагає аналітикам розслідувати потенційні проблеми безпеки. Вона робить це, збираючи дані журналів з AWS CloudTrail, журналів потоків Amazon Virtual Private Cloud (VPC) та інших служб.

Проаналізовано методи та засоби виявлення вторгнень до хмарних корпоративних ресурсів на базі Amazon Detective. Відмічено, що Amazon Detective використовує машинне навчання, статистичний аналіз та теорію графів для створення пов'язаного набору даних, який називається графіком поведінки

безпеки, який можна використовувати для проведення швидших та ефективніших розслідувань безпеки.

Розглянуто порядок застосування Amazon Detective для виявлення вторгнень до хмарних корпоративних ресурсів, структурований за основними етапами. Розглянутий порядок забезпечує чітку послідовність дій для використання Amazon Detective як ключового інструменту в процесі реагування на інциденти кібербезпеки.

На основі досліджень проведених в роботі запропоновано порядок застосування технології виявлення вторгнень до хмарних корпоративних ресурсів на базі Amazon Detective. Необхідно відмітити, що в Amazon Detective проводиться розслідування, використовуючи дані з графа поведінки. Граф поведінки – це зв’язаний набір даних, згенерованих з вихідних даних Amazon Detective, які надходять з одного або кількох облікових записів Amazon Web Services (AWS).

Розроблено рекомендації фахівцям з кібербезпеки щодо виявлення вторгнень до хмарних корпоративних ресурсів.

Таким чином, правильна реалізація технології вторгнень до хмарних корпоративних ресурсів має забезпечити ефективний захист корпоративних даних та кібербезпеку інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Karishma Asthana. Top 8 Cloud Vulnerabilities. CrowdStrike, November 26, 2024. URL: https://www.crowdstrike.com/en-us/cybersecurity-101/cloud-security/cloud-vulnerabilities/

2. CrowdStrike 2025 Threat Hunting Report. URL: https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/

3. 2025 Cisco Cybersecurity Readiness Index. URL: https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/2025/documents/2025_Cisco_Cybersecurity_Readiness_Index.pdf

4. ENISA THREAT LANDSCAPE 2025. October 2025. URL: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025_0.pdf

5. Amber Picotte. Cloud Computing: Top Intrusion Detection Techniques. February 06, 2020. URL: https://www.uptycs.com/blog/intrusion-detection-in-cloud-computing

6. Charlie Klein. AWS vs. Azure vs. Google Cloud: A Security Feature Comparison. Published December 18, 2024. URL: https://www.jit.io/resources/cloud-sec-tools/aws-vs-azure-vs-google-cloud-a-security-feature-comparison

7. AWS vs Azure vs Google Cloud Security: Comparison. Published on 29 April 2024. URL: https://www.bizbot.com/blog/aws-vs-azure-vs-google-cloud-security-comparison/#google_vignette

8. AWS vs. Azure vs. Google Cloud: Security comparison. URL: https://www.sysdig.com/learn-cloud-native/threat-detection-in-the-cloud-defender-vs-guardduty-vs-security-command-center

9. Amazon Detective. User Guide. URL: https://docs.aws.amazon.com/detective/latest/userguide/what-is-detective.html

10. Amazon Detective: Overview | Working, Use Cases, & Benefits. URL: https://k21academy.com/amazon-web-services/amazon-detective/

11. John Lynch. Cloud intrusions have skyrocketed. CISOs should wise up. Tech Monitor, September 2, 2025. URL: https://www.techmonitor.ai/comment-2/cloud-intrusions-strategies?cf-view

12. Christopher Adamson. AWS Detective for Security Analysis and Investigation. Medium, Dec 27, 2023. URL: https://medium.com/@christopheradamson253/aws-detective-for-security-analysis-and-investigation-0540dd82f15a

13. Rich Vorwaller and Nicholas Doropoulos. Improve your security investigations with Detective finding groups visualizations. AWS Security Blog, 29 AUG 2023. URL: https://aws.amazon.com/blogs/security/improve-your-security-investigations-with-detective-finding-groups-visualizations/

14. Cloud Security Best Practices. Fortinet. URL: https://www.fortinet.com/resources/cyberglossary/cloud-security-best-practices

15. Kate O'Flaherty. Cloud security: How to detect breaches and stop them quickly. Features, October 16, 2025. URL: https://www.itpro.com/cloud/cloud-security/cloud-security-how-to-detect-breaches-and-stop-them-quickly

16. Cameron Sipes. Cloud Threat Detection & Defense: Advanced Methods 2025. SentinelOne, October 17, 2025. URL: https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-threat-detection/

17. Богданович Олексій Дмитрович. Технологія виявлення та аналізу загроз корпоративним додаткам і API на базі Akamai API Security. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». 29 жовтня 2025 року. Державний університет інформаційно-комунікаційних технологій, м. Київ. Тези доповідей. С. 116-118. URL: https://duikt.edu.ua/uploads/p_2779_58326207.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)