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

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія управління вразливостями хмарних корпоративних ресурсів на основі Amazon Inspector»

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

_____ Радомир ГОНЧАРЕНКО
(підпис)

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

CIPS – Cloud Infrastructure and Platform Service

CNAPP – Cloud-Native Application Protection Platform

CSPM – Cloud Security Posture Management

CVM – Cloud Vulnerability Management

CWPP – Cloud Workload Protection Platforms

DAST – Dynamic Application Security Testing

DDoS – Distributed Denial of Service

DNS – Domain Name System

IaaS – Infrastructure as a Service

IAM – Identity and Access Management

MSSP – Managed Security Service Provider

WAAP – Web Application and API protection

SAST – Static Application Security Testing

SCA – Software Composition Analysis

SOC – Security Operations Center

OWASP – Open Web Application Security Project

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. Управління вразливостями хмарних технологій є надзвичайно важливим у сучасному цифровому середовищі, оскільки організації все більше покладаються на хмарні сервіси. Ефективне управління допомагає виявляти та пом’якшувати вразливості, запобігаючи несанкціонованому доступу, порушенням безпеки даних та перебоям у наданні послуг. Воно забезпечує цілісність, конфіденційність та доступність хмарних ресурсів, захищаючи конфіденційну інформацію та підтримуючи довіру клієнтів.

Вразливості хмарних систем виникають через неправильні конфігурації, застаріле програмне забезпечення, неадекватні засоби контролю доступу або незахищені API. Їх використання може призвести до несанкціонованого доступу до даних, їх втрати, перебоїв у наданні послуг, порушень відповідності вимогам, фінансових збитків, репутаційної шкоди, правових наслідків та порушення довіри.

Постійний моніторинг, управління виправленнями, сканування вразливостей та проактивна оцінка ризиків є важливими компонентами надійної стратегії управління вразливостями хмарних технологій. Для забезпечення безпеки хмарних середовищ організаціям потрібні надійні засоби контролю доступу, моніторинг, шифрування, сегментація мережі, встановлення патчів та навчання співробітників. Дотримання цих практик є важливим для підтримки безпеки хмари та зменшення ризиків, пов’язаних з вразливостями.

Amazon Web Services – це комплексна хмара, яка надає клієнтам багато інноваційних хмарних можливостей та досвід у найбільшій глобальній інфраструктурі з найкращими в галузі показниками безпеки, надійності та продуктивності. Amazon Inspector – це служба керування вразливостями, яка автоматично виявляє робочі навантаження та постійно сканує їх на наявність програмних вразливостей та ненавмисного мережевого впливу.

Вищесказане визначає актуальність теми даної кваліфікаційної роботи, основний зміст якої становлять дослідження технології управління вразливостями

хмарних корпоративних ресурсів на основі Amazon Inspector.

Об'єкт дослідження – управління вразливостями хмарних корпоративних ресурсів.

Предмет дослідження – технологія управління вразливостями хмарних корпоративних ресурсів на основі Amazon Inspector.

Мета роботи – розробити порядок застосування технології управління вразливостями хмарних корпоративних ресурсів на основі Amazon Inspector та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми управління вразливостями хмарних корпоративних ресурсів;

проаналізувати підходи до управління вразливостями хмарних корпоративних ресурсів;

проаналізувати існуючі рішення для управління вразливостями хмарних корпоративних ресурсів;

проаналізувати методи та засоби управління вразливостями хмарних корпоративних ресурсів на основі Amazon Inspector;

розкрити порядок реалізації технології управління вразливостями хмарних корпоративних ресурсів на основі Amazon Inspector.

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

Практичне значення одержаних результатів: запропоновано порядок застосування технології управління вразливостями хмарних корпоративних ресурсів на основі Amazon Inspector, 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 УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ХМАРНИХ КОРПОРАТИВНИХ РЕСУРСІВ

1.1. Дослідження проблеми управління вразливостями хмарних корпоративних ресурсів

Вибір стратегії розгортання хмарних технологій організацією безпосередньо впливає на її потреби в безпеці, операційні результати та вимоги до інфраструктури, що робить його ключовим рішенням у сучасних багатогранних IT-середовищах [1].

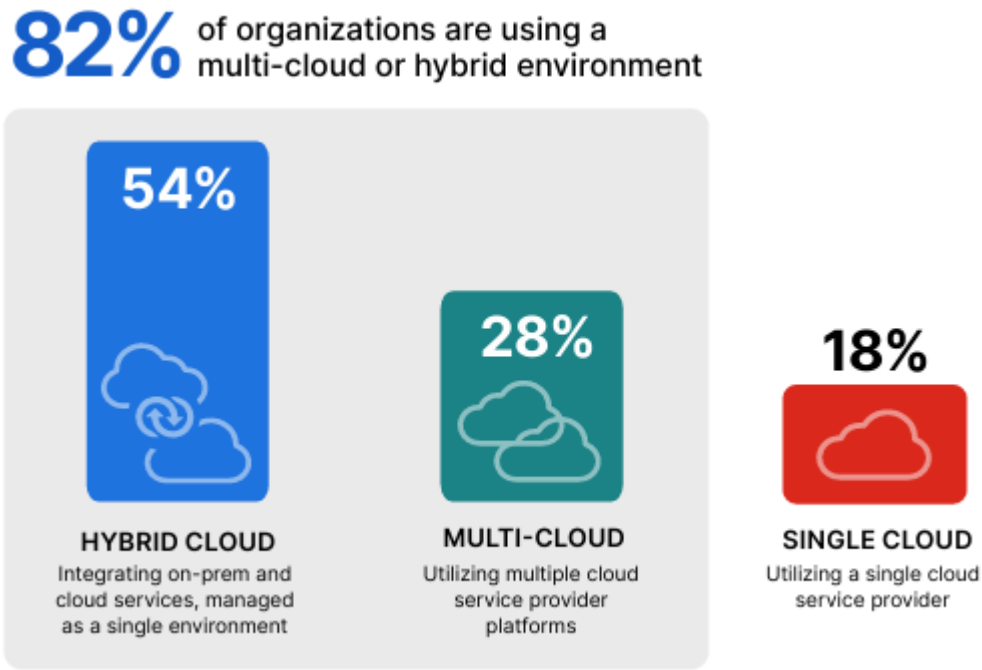

Рис. 1.1. Вибір організаціями стратегій щодо розгортання хмарних технологій [1]

Результати дослідження [1] підтверджують, що Microsoft Azure та AWS є домінуючими гравцями, причому 76% та 70% респондентів повідомляють про поточне використання цих послуг відповідно. Хмарна платформа Google, яку наразі використовують 52% респондентів, набирає популярності, про що свідчать 25% респондентів, які планують впровадити її в майбутньому. Тим часом Oracle

Cloud та IBM Cloud зберігають менші частки ринку, але бачать значний інтерес у майбутньому, ймовірно, завдяки їхньому досвіду в інтеграції зі застарілими корпоративними системами.

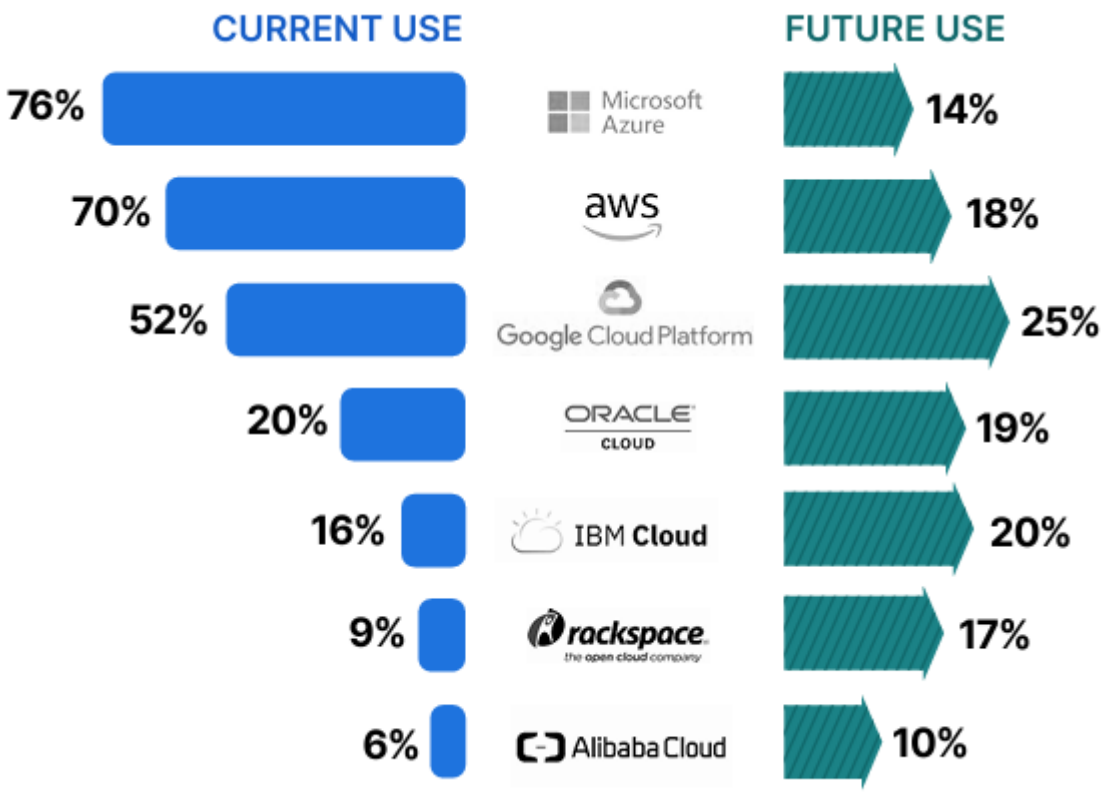

Рис. 1.2. Основні постачальники хмарних IaaS [1]

В Звіті [9] зазначається, що зі зростанням впровадження хмарних технологій та хмарно-орієнтованих технологій зростає обсяг і серйозність хмарних ризиків. Майже третина хмарних активів сьогодні занедбана, і кожен актив містить в середньому 115 вразливостей. Обидва ці показники є одними з багатьох, що ілюструють цю тривожну тенденцію. 58% організацій мають принаймні одну вразливість, якій понад 20 років. Вперше більшість організацій стикаються з вразливостями, які існують вже понад два десятиліття.

Вразливості часто потрапляють у життєвий цикл розробки програмного забезпечення (SDLC) через компоненти програмного забезпечення з відкритим вихідним кодом та сторонніх розробників, а також через ризики, що вносяться до кодових баз власних розробників. Згідно з нашим аналізом, понад сім із десяти

організацій мають серйозні вразливості в репозиторіях коду, таких як GitHub, GitLab, Azure DevOps або Bitbucket. Це свідчить про значне зростання у порівнянні з минулим роком і свідчить про постійну проблему для організацій. Якщо серйозні вразливості потрапляють у виробниче середовище та стають доступними для зловмисників, це може призвести до серйозних інцидентів безпеки, включаючи витоки даних [9].

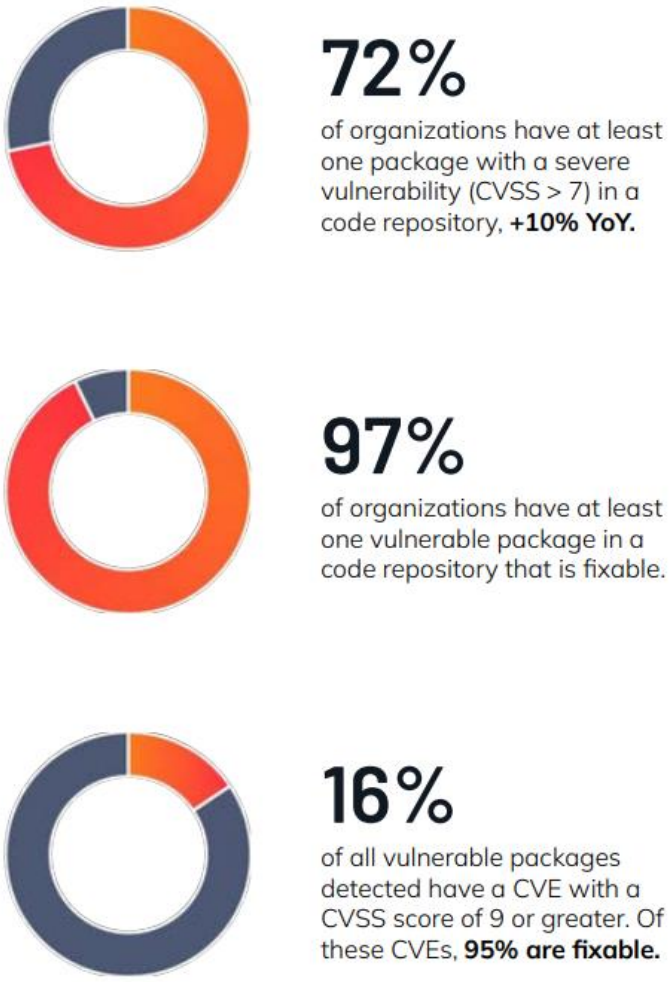

Рис. 1.3. Статистичні дані щодо вразливостей хмари [9]

Розглянемо поширені вразливості хмарних технологій. Вразливості в хмарі виникають з багатьох джерел, зокрема [6]:

ризики безпеки хмари. Платформи «інфраструктура як послуга» (IaaS), що надають доступ до віртуалізованих обчислювальних ресурсів, наражають користувачів на такі ризики, як невиправлені операційні системи або неправильно налаштовані групи безпеки. Середовища «платформа як послуга» (PaaS), які

пропонують попередньо створені керовані послуги, все ще становлять ризики у вигляді слабких засобів контролю автентифікації, недостатніх дозволів на доступ або незахищених інтеграцій;

неправильні конфігурації. Нездатність змінити налаштування безпеки за замовчуванням може ненавмисно розкрити конфіденційні дані. Ресурси сховища, що передаються в Інтернет без належної автентифікації або шифрування, можуть призвести до витоку даних, тоді як надмірно дозвільні права доступу користувачів або членство в групах можуть призвести до несанкціонованого доступу та компрометації даних;

незахищені API та сторонні сервіси. API зі слабкою автентифікацією, неадекватним обмеженням швидкості або відсутністю шифрування можуть забезпечити несанкціонований доступ до ресурсів. Інтеграція сторонніх сервісів збільшує поверхню для атаки та наражає хмарне середовище на вразливості в цих залежностях.

Проактивне усунення цих хмарних вразливостей вимагає підходу, що використовує постійний моніторинг, регулярні аудити та автоматизоване виправлення [6].

Виділяються такі проблеми управління вразливостями хмарних технологій [6]:

проблеми масштабованості. Оскільки хмарні ресурси часто є тимчасовими, а сервіси масштабуються залежно від попиту, поверхня атаки постійно змінюється. Традиційним сканерам вразливостей може бути важко встигати за зміною короткочасних груп та екземплярів контейнерів, наприклад;

багатохмарні та гібридні IT. Організації зазвичай використовують кількох хмарних провайдерів або гібриди локальної інфраструктури та хмарних сервісів. Складність цих середовищ часто вимагає значних зусиль для підтримки безпеки, що зумовлює необхідність одночасного використання кількох інструментів сканування вразливостей;

тіньові IT. Несанкціоноване використання хмарних сервісів внутрішніми бізнес-підрозділами або окремими користувачами ускладнює управління

вразливостями. Співробітники, які використовують особисті хмарні облікові записи для виконання робочих завдань, ще більше знижують видимість, а також можуть створювати ризики для безпеки;

дефіцит кваліфікованих кадрів. Хмарні сервіси швидко розвиваються, а зміни та нові функції випереджають можливості організацій встигати за ними. Як наслідок, існуючий дефіцит кваліфікованих кадрів у командах безпеки стає все більш серйозним. Організаціям може бути дедалі важче знаходити та утримувати кваліфікований персонал для роботи з системами CVM.

Організації можуть покращити свої можливості CVM та краще керувати ризиками, визнаючи ці проблеми та вживаючи заходів для проактивного управління ними.

Еволюція хмарних загроз та вразливостей вимагає проактивних заходів в управлінні виправленнями, тестуванні, моніторингу відповідності, інтеграції оцінки вразливостей та використанні штучного інтелекту й машинного навчання. Майбутнє хмарної безпеки принесе як виклики, так і досягнення, вимагаючи від організацій вирішення складних багатохмарних середовищ, проблем конфіденційності та складних кібератак.

Вимоги до відповідності, галузеві норми та правила конфіденційності даних мають значний вплив на управління вразливостями хмарних технологій. Розуміння та дотримання цих норм мають вирішальне значення для організацій, щоб підтримувати надійний рівень безпеки, захищати конфіденційні дані та дотримуватися правових зобов’язань. Впровадження передових технологій та відстеження нових загроз будуть важливими для ефективного управління вразливостями в постійно мінливому хмарному середовищі.

1.2. Аналіз підходів до управління вразливостями хмарних корпоративних ресурсів

Управління вразливостями хмарних технологій передбачає постійне виявлення та виправлення слабких місць безпеки в хмарних середовищах. Цей процес є критично важливим для запобігання витокам даних та перебоям у наданні послуг [10].

Управління вразливостями хмарних технологій передбачає впровадження управління вразливостями хмарних технологій шляхом виявлення та зменшення вразливостей безпеки в хмарній інфраструктурі. Цей безперервний процес включає класифікацію, визначення пріоритетів та усунення ризиків, щоб забезпечити безпеку та стійкість корпоративного хмарного середовища до кіберзагроз.

Управління вразливостями хмарних технологій має вирішальне значення для запобігання витокам даних, перебоям у наданні послуг та іншим інцидентам безпеки. Усунення цих вразливостей знижує ризики, а безпека та стійкість поверхні атаки хмари та хмарної інфраструктури посилюються за допомогою інструменту управління вразливостями хмарних технологій.

Проактивне виявлення та вирішення проблем підвищує операційну стійкість та зміцнює безпеку хмарних технологій.

Певні вразливості в хмарних обчисленнях є більш поширеними та створюють значні ризики. Виявлення цих поширених проблем, таких як незахищені API, неправильні конфігурації та витоки даних, має вирішальне значення для ефективного управління (рисунок 1.4) [10].

Ці вразливості можуть мати серйозні наслідки, якщо їх використовувати. Незахищені API можуть призвести до несанкціонованого доступу, неправильні конфігурації можуть розкрити конфіденційні дані, а витоки даних можуть завдати значної фінансової шкоди та завдати шкоди репутації.

Управління вразливостями хмарних середовищ (CVM) стосується процесу виявлення, класифікації та зменшення вразливостей безпеки в хмарних середовищах. CVM допомагає організаціям, що працюють у хмарі, захищати

конфіденційні дані, підтримувати відповідність вимогам та мінімізувати ризики [6].

Системи CVM використовують поетапний підхід для оцінки, визначення пріоритетів та усунення вразливостей [6, 10]:

виявлення. Використовуючи автоматизовані інструменти сканування та аналізу різних джерел даних, API, сторонніх сервісів та контенту, створеного користувачами, система CVM виявляє потенційні вразливості;

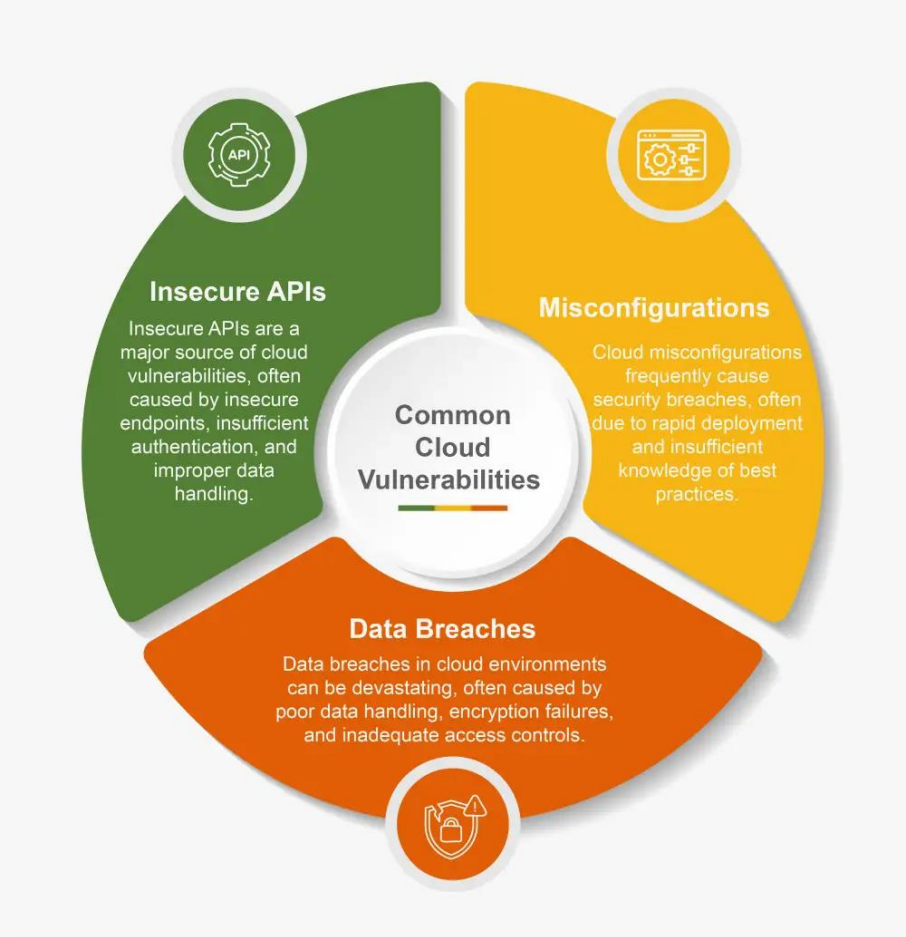

Рис. 1.4. Найбільш поширені вразливості хмарних обчислень [10]

пріоритизація. Система призначає кожній вразливості оцінку ризику на основі таких факторів, як серйозність, вплив та уражені ресурси;

оцінка. Далі оцінюються пріоритетні вразливості та надаються рекомендації щодо їх усунення, включаючи зміни конфігурації, оновлення або виправлення програмного забезпечення, вимкнення непотрібних служб або впровадження

заходів безпеки;

виправлення. Система може автоматично виконувати рекомендовані дії для усунення кожної вразливості, забезпечуючи швидке завершення процесу;

моніторинг. Системи CVM розроблені для постійного моніторингу хмарного середовища на наявність нещодавно виявлених вразливостей, автоматично повторюючи цикл виявлення та усунення.

Використання правильних інструментів має вирішальне значення для ефективного управління вразливостями хмарних технологій. Автоматизовані інструменти оптимізують завдання в хмарних середовищах, зменшуючи ручне навантаження та підвищуючи ефективність. Використання штучного інтелекту та машинного навчання ще більше покращує можливості виявлення загроз та реагування на них [10].

Такі технології, як CSPM (Cloud Security Posture Management), CNAPP (Cloud-Native Application Protection Platform), CWPP (Cloud Workload Protection Platforms) та інструменти оцінки вразливостей на основі штучного інтелекту, пропонують покращене виявлення загроз, автоматизовані реагування та інтегровані заходи безпеки, що робить їх незамінними для безпечної хмарної інфраструктури [10].

Сканери вразливостей мають вирішальне значення для виявлення відомих вразливостей безпеки в хмарних середовищах. Сканування вразливостей хостів, контейнерів, безсерверних функцій та інших ресурсів виявляє потенційні вразливості за допомогою інструментів сканування вразливостей та самих сканувань вразливостей.

Автоматизація та машинне навчання в процесах сканування зменшують ручне навантаження та підвищують ефективність. Інтеграція бази даних вразливостей з інструментами сканування сприяє швидшому аналізу та реагуванню.

Управління станом безпеки хмари (Cloud Security Posture Management, CSPM). Рішення CSPM є важливими для виявлення та усунення неправильних конфігурацій та вразливостей хмари, забезпечення безпеки хмарної

інфраструктури. Вони використовують автоматизовані перевірки та оцінки для ефективного виявлення неправильних конфігурацій та ризиків.

Впровадження рішень CSPM покращує прозорість та контроль над безпекою хмари, зменшуючи вразливості та ризики. Безперервне дотримання вимог та управління безпекою є критично важливими для надійного хмарного середовища.

Платформи захисту хмарних робочих навантажень (CWPP). CWPP забезпечують заходи безпеки, призначені для захисту хмарних робочих навантажень від різних загроз. Вони реалізують захист під час виконання та виявлення вторгнень для запобігання атакам, ефективно захищаючи робочі навантаження.

Пропонуючи інтегровані заходи безпеки, CWPP гарантує, що хмарні робочі навантаження залишаються захищеними від загроз, що постійно змінюються, що робить їх безцінними для управління вразливостями хмари.

Ефективне управління вразливостями хмарних технологій вимагає таких передових практик, як [10]:

регулярне сканування вразливостей;

комплексна оцінка ризиків;

своєчасне усунення недоліків;

постійний моніторинг.

Керування ідентифікацією та доступом (IaM) має вирішальне значення для управління автентифікацією та авторизацією в хмарних середовищах.

Автоматизація та правильні інструменти оптимізують процес управління вразливостями , пропонуючи централізовані панелі інструментів для моніторингу безпеки в різних середовищах. Регулярна оцінка ризиків та впровадження систем хмарної безпеки є ключовими практиками для зменшення ризиків у хмарному середовищі [10].

Безперервний моніторинг має вирішальне значення для виявлення вразливостей у міру розвитку хмарних середовищ. На відміну від періодичного сканування, безперервний моніторинг запобігає появі нових вразливостей. CWPP пропонують безперервний моніторинг і захист хмарних робочих навантажень ,

забезпечуючи безпеку в різних середовищах [10].

Регулярні аудити хмарних сервісів забезпечують належне керування дозволами та доступом.

Включення сканування вразливостей у процеси CI/CD дозволяє їх раннє виявлення до розгортання у виробничому середовищі. Сканування повинно охоплювати хости, контейнери та безсерверні функції. Погана співпраця між командами може призвести до непорозумінь та затримок у виправленні вразливостей. Інтеграція сканування вразливостей у процеси CI/CD підвищує безпеку, виявляючи проблеми на ранній стадії та оперативно усуваючи вразливості.

Регулярне повторне сканування та тестування на проникнення підтверджують, що критичні вразливості усунені. Сканування всіх IT-активів є важливим для виявлення вразливостей організації.

Постійне навчання співробітників методам хмарної безпеки має вирішальне значення для зменшення вразливостей. Неефективне управління виправленнями може зробити організації вразливими, якщо оновлення затримуються. Обмеження ресурсів може перешкоджати ефективному управлінню вразливостями та затримувати виправлення критичних проблем.

Впровадження програми управління вразливостями хмарних технологій передбачає встановлення чітких цілей та встановлення ключових показників ефективності (KPI) для кількісної оцінки результатів. Такий покроковий підхід гарантує ефективне вирішення всіх аспектів безпеки хмарних технологій.

Періодичне повторне сканування хмарного середовища забезпечує своєчасне виявлення та усунення нових вразливостей, підтримуючи безпеку та цілісність.

Постійне вдосконалення управління вразливостями допомагає організаціям випереджати загрози, що розвиваються, адаптуючи стратегії та процеси на основі нових ризиків. Відгуки про минулі заходи з усунення вразливостей покращують майбутні практики, роблячи їх ефективнішими та результативнішими.

Культура постійного вдосконалення сприяє кращій командній співпраці, покращуючи загальну безпеку організації. Інструменти на основі штучного

інтелекту підвищують ефективність і точність оцінки вразливостей, сприяючи постійному вдосконаленню.

Розглядаючи ландшафт управління вразливостями хмарних технологій, стає зрозуміло, що проактивний та безперервний підхід є надзвичайно важливим. Розуміння поширених вразливостей хмарних технологій, таких як незахищені API, неправильні конфігурації та витоки даних, формує основу ефективних практик безпеки. Впроваджуючи структурований процес управління вразливостями, який включає виявлення вразливостей, оцінку ризиків та застосування стратегій усунення недоліків, організації можуть значно покращити свій рівень безпеки хмарних технологій.

Більше того, використання передових інструментів, таких як сканери вразливостей, CSPM та CWPP, а також дотримання найкращих практик, таких як постійний моніторинг, інтеграція сканування вразливостей у CI/CD та проведення регулярних оцінок безпеки, гарантує, що хмарні середовища залишатимуться стійкими до загроз, що постійно змінюються. Постійне вдосконалення та адаптація до нових вразливостей і загроз мають вирішальне значення для підтримки надійної безпеки хмари.

1.3. Аналіз існуючих рішень для управління вразливостями хмарних корпоративних ресурсів

Для ефективного управління вразливостями в хмарних середовищах слід використовувати різноманітні спеціалізовані інструменти, розроблені для оптимізації процесу. Використання цих інструментів дозволяє розробляти надійні стратегії управління вразливостями в хмарі, адаптовані до унікального профілю загроз корпоративним ресурсам.

Різні сторонні сервіси пропонують окреме програмне забезпечення CVM для оцінки стану безпеки

Nessus, що пропонується компанією Tenable, – це широко використовуваний сканер вразливостей для постачальників хмарних послуг, який пропонує

безперервний моніторинг, перевірку відповідності та робочі процеси для виправлення вразливостей.

Qualys надає платформу сканування вразливостей у хмарі з можливостями виявлення активів, оцінки вразливостей, безпеки веб-застосунків та управління відповідністю вимогам.

Управління вразливостями Cisco, зосереджена на пріоритезації вразливостей на основі ризику, пропозиція Cisco включає оцінювання на основі ризиків, аналіз вразливостей та відстеження виправлення.

Сканери вразливостей, специфічні для хмари. Можливості CVM доступні в рамках пропозицій послуг кількох постачальників хмарних послуг [6]:

AWS Inspector автоматизує виявлення активів та оцінку вразливостей в екземплярах EC2 та AMI, з опціями інтеграції для інших сервісів. Він надає детальні звіти про свої результати для аналізу;

Microsoft Defender for Cloud – служба пропонує безперервний моніторинг та оцінку вразливостей для ресурсів Azure, а також включає автоматичне виправлення, виявлення загроз та інтеграцію з іншими продуктами безпеки Microsoft;

Google Cloud Security Scanner – сервіс Google Cloud регулярно сканує комп'ютери, щоб оцінити їхню безпеку на наявність відомих вразливостей. Він інтегрується з іншими сервісами Google Cloud для широкого охоплення моніторингу та сповіщень.

Інструменти CVM зазвичай пропонують інтеграцію з іншими системами для забезпечення кращого захисту та покращення загальної оборонної позиції [6]:

управління інформацією та подіями безпеки (SIEM) – підключення інструментів CVM до систем SIEM дозволяє централізовано збирати журнали, корелювати події та сповіщати про загрози;

інфраструктура в коді (IaC) – інтеграція систем CVM в інструменти IaC гарантує автоматичне застосування безпеки в життєвому циклі розробки та під час виділення хмарних ресурсів;

бази даних керування конфігураціями (CMDB) – інтеграція CVM у CMDB

допомагає вести точну інвентаризацію активів та покращувати відстеження змін у різних конфігураціях.

Amazon Inspector автоматично виявляє робочі навантаження, такі як екземпляри Amazon Elastic Compute Cloud (Amazon EC2), образи контейнерів та функції AWS Lambda, а також репозиторії коду, і сканує їх на наявність програмних вразливостей та ненавмисного мережевого впливу.

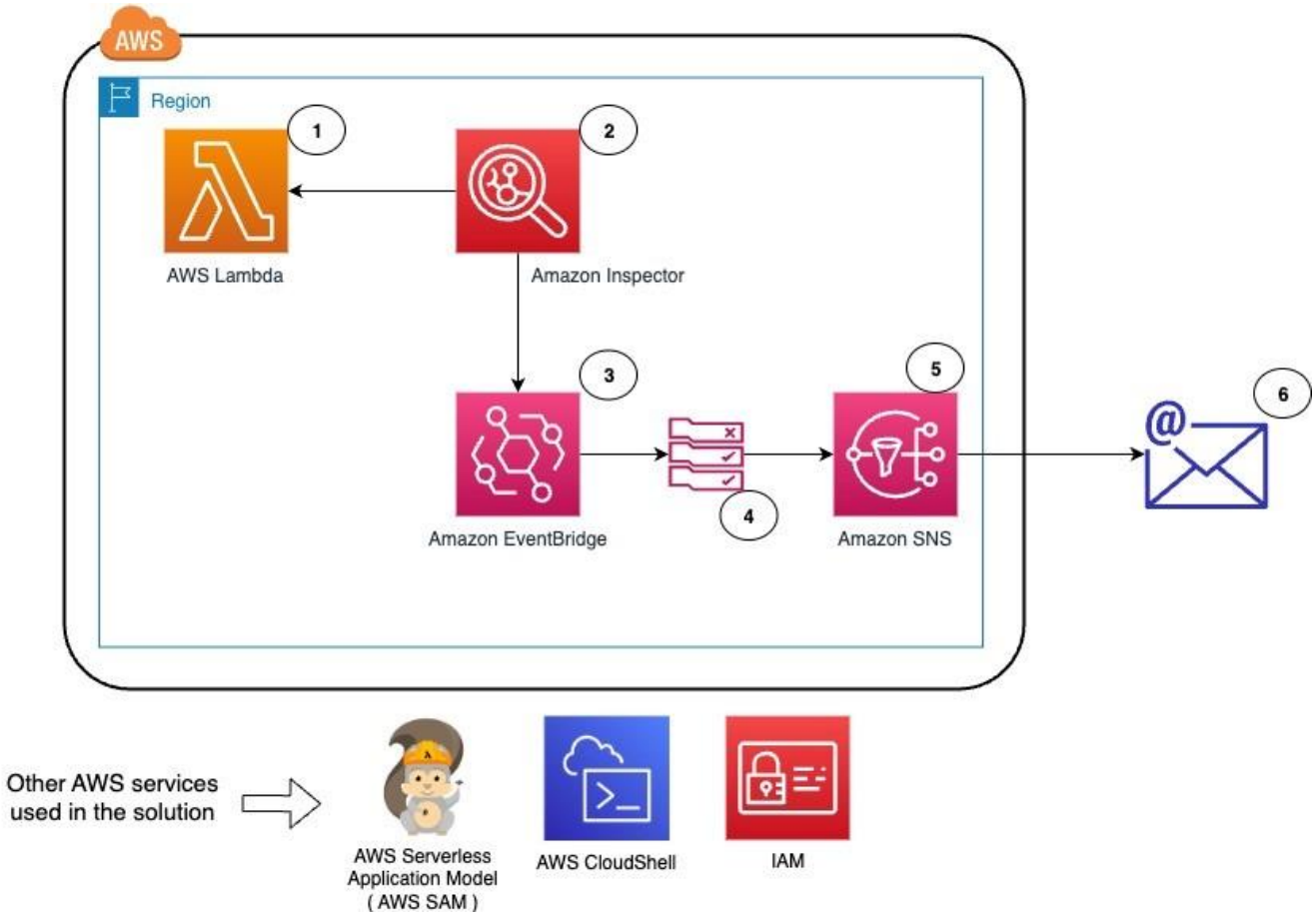

Рис. 1.5. Місце Amazon Inspector в архітектурі AWS

Платформи захисту хмарних додатків (CNAPP) представляють собою модернізований підхід до безпеки, розроблений для вирішення складних проблем, що виникають у сучасних хмарних середовищах. На відміну від традиційних моделей безпеки, які працюють ізольовано, CNAPP надає цілісну, інтегровану основу для захисту складних хмарних додатків та інфраструктур, забезпечуючи комплексний захист протягом усього життєвого циклу додатка. У своїй основі CNAPP об’єднує кілька функцій безпеки в єдину платформу.

Управління станом безпеки хмари (CSPM) відіграє вирішальну роль у виявленні та виправленні неправильних конфігурацій, допомагаючи організаціям підтримувати відповідність вимогам та знижувати ризики безпеки.

Платформи захисту хмарних робочих навантажень (CWPP) пропонують надійні механізми захисту від загроз, спрямованих на віртуальні машини, контейнери та API, гарантуючи, що робочі навантаження залишаються більш безпечними у високодинамічних середовищах.

Крім того, управління ідентифікацією та доступом (IAM) та засоби контролю безпеки додатків посилюють захист, забезпечуючи доступ з найменшими привілеями та захищаючи додатки від несанкціонованих дій. Механізми безпеки даних, включаючи шифрування та передові методи запобігання загрозам, забезпечують цілісність та конфіденційність конфіденційної інформації в розподілених хмарних екосистемах.

Ключовою відмінністю CNAPP є його відповідність підходу до безпеки зі зсувом вліво в DevOps. Вбудовуючи засоби контролю безпеки на ранніх етапах розробки, організації можуть виявляти вразливості до розгортання, зменшуючи ризик поширення недоліків безпеки у виробничому середовищі. Крім того, CNAPP розроблений для того, щоб виходити за межі обмежень платформи, безперешкодно інтегруючись з існуючими інструментами безпеки, що дозволяє організаціям налаштовувати рішення безпеки, не будучи прив’язаними до власних екосистем.

Його залежність від постачальника сприяє взаємодії та автоматизації, підвищуючи прозорість безпеки та зменшуючи складність. Об’єднуючи безпеку в різних хмарних середовищах, CNAPP надає організаціям можливість впроваджувати цілісну стратегію, яка ефективно протидіє кіберзагрозам, що розвиваються, зміцнюючи їх загальний рівень безпеки та стійкість у дедалі складнішому хмарному ландшафті.

Рішення Microsoft Defender for Cloud є Cloud Native Application Protection Platform (CNAPP) [11].

Microsoft Defender for Cloud – це уніфіковане рішення, що поєднує кілька хмарних інструментів безпеки для захисту програм протягом усього їхнього

життєвого циклу. Рішення надає комплексне уявлення про стан безпеки в хмарних та локальних ресурсах. Воно також допомагає захистити багатохмарні та гібридні середовища й інтегрує безпеку в робочі процеси DevOps. Є три основні компоненти [11]:

операції безпеки розробки (DevSecOps) керують безпекою на рівні коду в багатохмарних та багатоконвеєрних середовищах;

управління станом безпеки хмари (CSPM) перевіряє та покращує стан безпеки хмарних ресурсів;

платформа захисту хмарних робочих навантажень (CWPP) захищає від загроз такі робочі навантаження, як віртуальні машини (ВМ), контейнери, сховища, бази даних та безсерверні функції.

Defender for Cloud використовує свої ширші можливості платформи захисту Cloud Native Application Protection Platform (CNAPP) для об'єднання захисту в один інтерфейс. Defender for Cloud вбудовує безпеку на ранніх етапах життєвого циклу розробки. Це допомагає командам DevOps виявляти неправильні конфігурації, застосовувати політики та виправляти ризики на ранніх етапах.

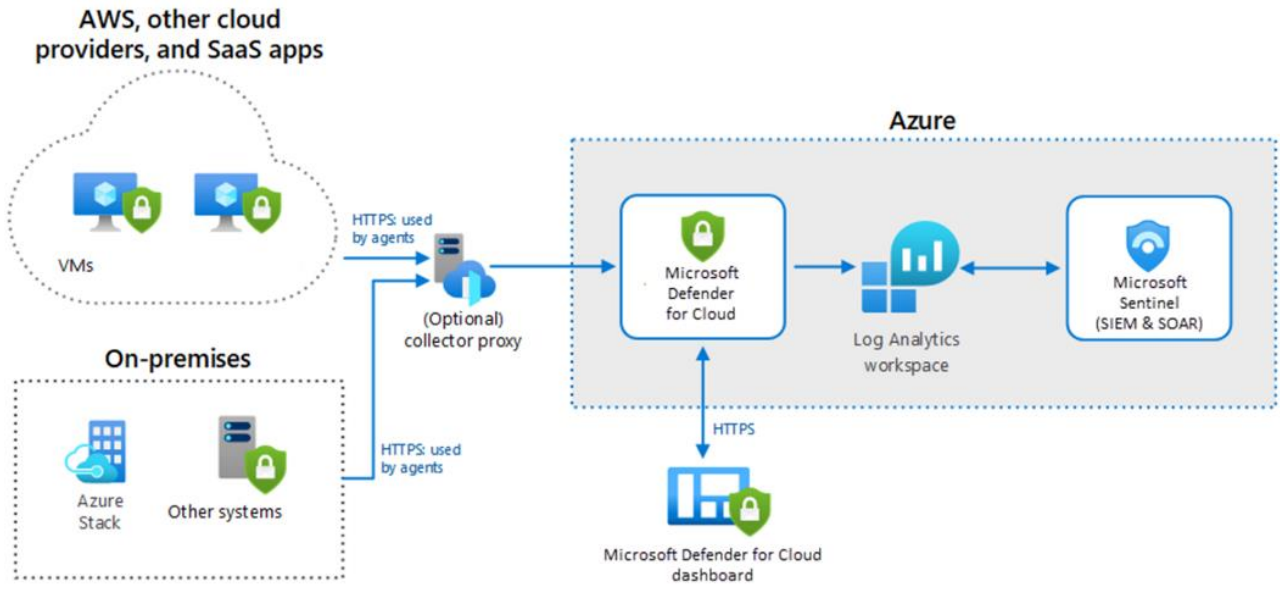

Рис. 1.6. Місце Microsoft Defender for Cloud в архітектурі безпеки Azure

Після ввімкнення рішення Defender for Cloud у підписці Azure система збирає дані безпеки з корпоративних багатохмарних середовищ та середовищ DevOps. Defender for Cloud використовує ці дані, щоб надавати аналітичні дані, рекомендації та дії, які допомагають захистити корпоративні хмарні робочі навантаження та ресурси. Ми можемо ввімкнути додаткові плани, щоб отримати розширені функції безпеки, такі як Defender Cloud Security Posture Management (CSPM), Defender for Databases та Defender for Containers [11].

Google Cloud Security Scanner – це інструмент сканування безпеки, що пропонується Google Cloud Platform, який перевіряє веб-застосунки, розміщені на GCP, на наявність поширених вразливостей. Він сканує на наявність широкого спектру проблем безпеки, таких як міжсайтовий скриптинг (XSS), відсутні заголовки безпеки, застаріле програмне забезпечення та інші поширені вразливості. Він імітує атаку на веб-застосунок та аналізує відповіді для виявлення вразливостей [12].

Його можна інтегрувати з Google App Engine, Compute Engine та Kubernetes Engine. Після завершення сканування генерується звіт, у якому висвітлюються всі знайдені вразливості та надаються рекомендації щодо їх виправлення; таким чином, це дозволяє покращити безпеку веб-застосунку. Це корисний інструмент для фахівців з безпеки та розробників, який дозволяє виявляти та усувати потенційні вразливості у своїх веб-застосунках, що працюють на інфраструктурі GCP.

Google Cloud Security Scanner перевіряє веб-застосунки на наявність проблем безпеки, видаючи себе за справжнього користувача або навіть хакера. Він відвідує сайт, натискає на посилання, заповнює форми та спостерігає за реакцією застосунку. Потім він пробує поширені хитрощі, які використовують хакери, такі як додавання підроблених скриптів або перевірка, чи використовує ваш застосунок старе програмне забезпечення. Якщо він виявляє щось небезпечне (наприклад, відсутні налаштування безпеки або застарілі інструменти), він повідомляє про це, щоб виправити це та забезпечити безпеку застосунку [12].

Рис. 1.7. Основні функції Google Cloud Security Scanner [12]

Google Cloud Security Scanner – це простий та ефективний інструмент для виявлення поширених вразливостей веб-застосунків, таких як XSS, відсутні заголовки та застаріле програмне забезпечення в застосунках, розміщених на GCP. Він моделює реальні атаки, аналізує відповіді та надає практичні звіти, щоб допомогти розробникам виправити проблеми, перш ніж вони стануть серйозними загрозами. Хоча він економічно вигідний та добре інтегрований з GCP, його обмежений обсяг та залежність від платформи означають, що його найкраще використовувати разом з іншими інструментами безпеки для повного покриття.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ХМАРНИХ КОРПОРАТИВНИХ РЕСУРСІВ НА ОСНОВІ AMAZON INSPECTOR

2.1. Призначення та основні функції рішення Amazon Inspector

Рішення Amazon Inspector – це служба керування вразливостями, яка автоматично виявляє робочі навантаження та постійно сканує їх на наявність програмних вразливостей та ненавмисного мережевого впливу. Amazon Inspector виявляє та сканує екземпляри Amazon EC2, образи контейнерів в Amazon ECR та функції Lambda. Коли Amazon Inspector виявляє програмну вразливість або ненавмисний мережевий вплив, він створює звіт про виявлення, який є детальним звітом про проблему. Ми можемо керувати результатами в консолі Amazon Inspector або API [13].

Розглянемо основні функції рішення Amazon Inspector:

Централізоване керування кількома обліковими записами Amazon Inspector

Якщо корпоративне середовище AWS має кілька облікових записів, ми можемо централізовано керувати своїм середовищем через один обліковий запис за допомогою AWS Organizations. За допомогою цього підходу ми можемо призначити обліковий запис як делегованого облікового запису адміністратора для Amazon Inspector.

Amazon Inspector можна активувати для всієї організації одним клацанням миші. Крім того, ми можемо автоматизувати активацію сервісу для майбутніх учасників щоразу, коли вони приєднуються до організації. Делегований обліковий запис адміністратора Amazon Inspector може керувати даними про результати та певними налаштуваннями для учасників організації. Це включає перегляд сукупних відомостей про результати для всіх облікових записів учасників, активацію або деактивацію сканувань для облікових записів учасників та перегляд сканованих ресурсів в організації AWS [13].

Постійно сканування власного середовища на наявність вразливостей та мережевих ризиків

Завдяки Amazon Inspector не потрібно вручну планувати або налаштовувати сканування оцінки. Amazon Inspector автоматично виявляє та починає сканування корпоративних відповідних ресурсів. Amazon Inspector продовжує оцінювати корпоративне середовище протягом усього життєвого циклу корпоративних ресурсів, автоматично повторно скануючи ресурси у відповідь на зміни, які можуть призвести до появи нової вразливості, такі як: встановлення нового пакета в екземплярі EC2, встановлення патча та публікація нових поширених вразливостей та експозицій (CVE), що впливають на ресурс. На відміну від традиційного програмного забезпечення для сканування безпеки, Amazon Inspector має мінімальний вплив на продуктивність парку корпоративних ресурсів.

Коли виявляються вразливості або відкриті мережеві шляхи, Amazon Inspector створює звіт, який ми можемо дослідити. Висновок містить вичерпну інформацію про вразливість, уражений ресурс і рекомендації щодо усунення. Якщо належним чином усунено виявлену проблему, Amazon Inspector автоматично виявить це та закриє звіт.

Точна оцінка вразливості за допомогою оцінки ризиків Amazon Inspector

Збираючи інформацію про корпоративне середовище за допомогою сканувань, Amazon Inspector надає оцінки серйозності, спеціально адаптовані до корпоративного середовища. Amazon Inspector аналізує показники безпеки, що складають Національну базу даних вразливостей.(NVD) базовий бал для вразливості та коригує його відповідно до корпоративного обчислювального середовища. Наприклад, сервіс може знизити бал Amazon Inspector для знахідки для екземпляра Amazon EC2, якщо вразливість можна використати через мережу, але з екземпляра немає відкритого мережевого шляху до Інтернету. Цей бал надається у форматі CVSS та є модифікацією базової Загальної системи оцінювання вразливостей (Common Vulnerability Scoring System).Оцінка (CVSS) надана NVD.

Визначення важливих результатів за допомогою панелі інструментів

Amazon Inspector

Панель інструментів Amazon Inspector пропонує загальний огляд результатів сканування з усього корпоративного середовища. З панелі інструментів ми можемо отримати доступ до детальної інформації про результат. Панель інструментів містить оптимізовану інформацію про охоплення скануванням у вашому середовищі, найважливіші результати та ресурси з найбільшою кількістю результатів. Панель виправлення на основі ризиків на панелі інструментів Amazon Inspector відображає результати, які впливають на найбільшу кількість екземплярів та зображень. Ця панель спрощує визначення результатів, які мають найбільший вплив на корпоративне середовище, перегляд деталей результатів та запропонованих рішень.

Керування своїми висновками за допомогою налаштовуваних подань

Окрім панелі інструментів, консоль Amazon Inspector пропонує перегляд результатів. На цій сторінці перераховано всі результати для корпоративного середовища та наведено детальну інформацію про окремі результати. Ми можемо переглядати результати, згруповані за категоріями або типами вразливостей. У кожному перегляді ми можемо додатково налаштувати результати за допомогою фільтрів. Також можна використовувати фільтри для створення правил придушення, які приховують небажані результати з переглядів.

Ми можемо використовувати фільтри та правила блокування для створення звітів про результати, які відображають усі результати або налаштований вибір результатів. Звіти можна створювати у форматах CSV або JSON.

Моніторинг та обробка результатів за допомогою інших служб та систем

Для підтримки інтеграції з іншими сервісами та системами Amazon Inspector публікує результати пошуку в Amazon EventBridge як події пошуку. EventBridge – це безсерверний сервіс шини подій, який може направляти дані пошуку до таких цільових об’єктів, як функції AWS Lambda та теми Amazon Simple Notification Service (Amazon SNS). За допомогою EventBridge ми можемо відстежувати та обробляти результати пошуку майже в режимі реального часу в рамках існуючих робочих процесів безпеки та відповідності.

Якщо активовано AWS Security Hub, Amazon Inspector також опублікує результати в Security Hub. Security Hub – це сервіс, який надає комплексне уявлення про стан безпеки в середовищі AWS і допомагає перевірити корпоративне середовище на відповідність стандартам галузі безпеки та передовим практикам. За допомогою Security Hub ми можемо легше контролювати та обробляти свої результати в рамках ширшого аналізу стану безпеки організації в AWS.

AWS Inspector – це сервіс сканування вразливостей від AWS, який використовується для сканування корпоративних екземплярів EC2, образів контейнерів та функцій Lambda. Його результати повідомлять про вразливості, відомі як CVE (Common Vulnerabilities and Exposure), які являють собою недоліки безпеки, що оприлюднюються з метою підвищення обізнаності та прозорості [14].

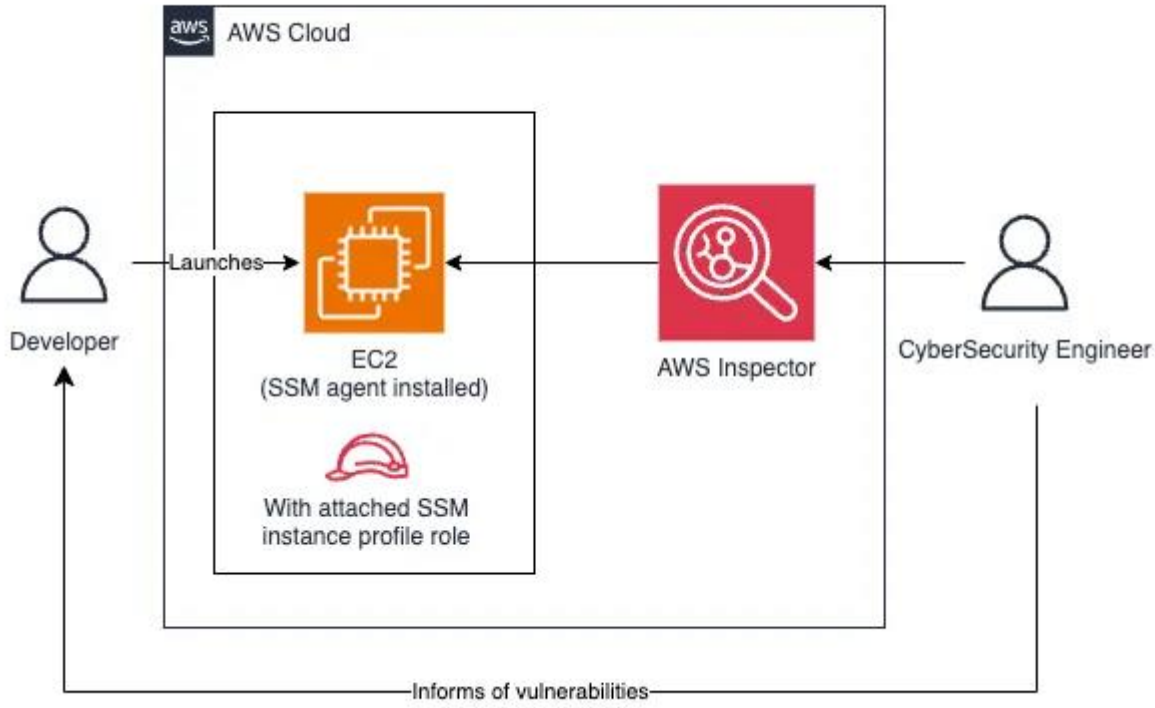

Рис. 2.1. Місце Amazon Inspector в архітектурі AWS [14]

У високорівневій архітектурі (рисунок 2.1) рішення AWS Inspector залежить від агента, встановленого в екземплярі EC2, який використовуватиметься для сканування та звітування про результати безпеки. Крім того, EC2 потребуватиме ролі, яка надає SSM доступ до екземпляра EC2. AWS Inspector використовує агент

SSM для підключення до екземпляра.

2.2. Основні компоненти рішення Amazon Inspector. Типи автоматизованого сканування в Amazon Inspector

Основними компонентами високорівневої архітектури рішення AWS Inspector є [13]:

консоль керування AWS. Консоль керування AWS – це інтерфейс на основі браузера, який можна використовувати для створення та керування ресурсами AWS. У рамках цієї консолі консоль Amazon Inspector надає доступ до облікового запису та ресурсів Amazon Inspector. Ми можемо виконувати завдання Amazon Inspector з консолі Amazon Inspector;

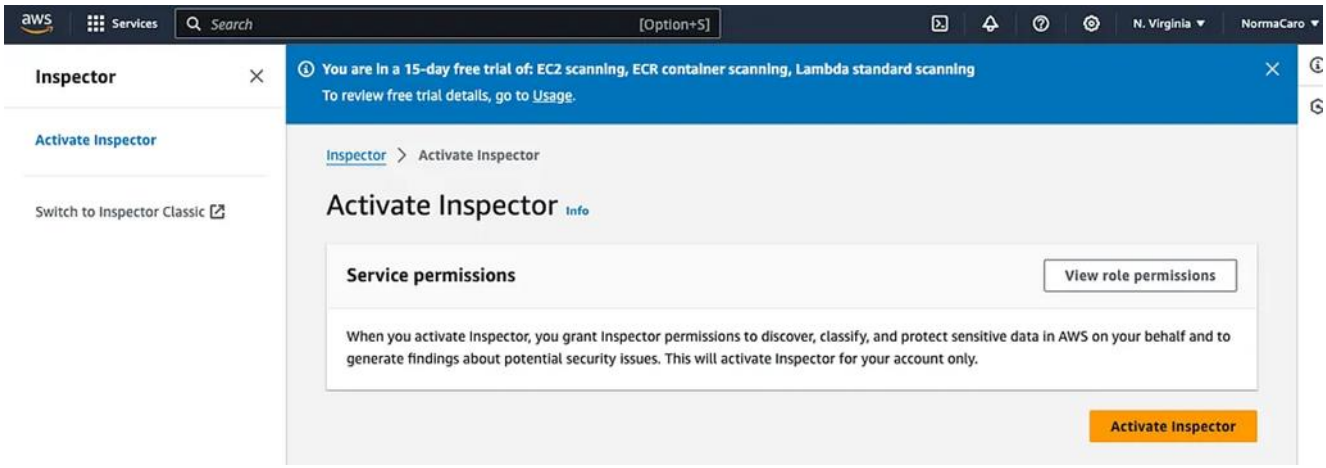

Рис. 2.2. Консоль керування AWS

інструменти командного рядка AWS. За допомогою інструментів командного рядка AWS ми можемо видавати команди в командному рядку нашої системи для виконання завдань Amazon Inspector. Використання командного рядка може бути швидшим і зручнішим, ніж використання консолі. Інструменти командного рядка також корисні, якщо ми хочемо створювати скрипти, які виконують завдання. AWS надає два набори інструментів командного рядка: інтерфейс командного рядка AWS (AWS CLI) та інструменти AWS Tools for PowerShell;

AWS SDK. AWS надає SDK, що складаються з бібліотек та зразків коду для різних мов програмування та платформ, включаючи Java, Go, Python, C++ та .NET. SDK забезпечують зручний програмний доступ до Amazon Inspector та інших сервісів AWS. Вони також обробляють такі завдання, як криптографічне підписання запитів, керування помилками та автоматичний повторний запит;

REST API Amazon Inspector. REST API Amazon Inspector надає нам повний програмний доступ до нашого облікового запису та ресурсів Amazon Inspector. За допомогою цього API ми можемо надсилати HTTPs-запити безпосередньо до Amazon Inspector. Однак, на відміну від інструментів командного рядка та SDK AWS, використання цього API вимагає від корпоративного додатка обробки низькорівневих деталей, таких як створення хешу для підписання запиту.

Розглянемо типи автоматизованого сканування в Amazon Inspector. Amazon Inspector пропонує різні типи сканування, які зосереджені на певних типах ресурсів у корпоративному середовищі AWS.

Сканування Amazon EC2. Коли ми активуємо сканування Amazon EC2, Amazon Inspector сканує корпоративні екземпляри EC2 на наявність поширених вразливостей та ризиків (CVE), проблем із мережевими ризиками, проблем із доступністю мережі, вразливостей операційної системи та пакетів мов програмування. Amazon Inspector виконує сканування за допомогою агента SSM, встановленого на корпоративному екземплярі, або за допомогою знімків екземплярів Amazon EBS. За замовчуванням, коли ми активуємо сканування Amazon EC2, ми автоматично вмикаємо гібридний режим сканування.

Цей тип сканування витягує метадані з екземпляра Amazon EC2, перш ніж порівнювати їх із правилами, зібраними з рекомендацій щодо безпеки. Коли ви активуєте цей тип сканування, Amazon Inspector сканує всі відповідні екземпляри Amazon EC2 у нашому обліковому записі на наявність вразливостей пакетів і проблем з доступністю мережі. Після активації цього типу сканування ми можемо переглянути, скільки екземплярів сканується, на вкладці «Екземпляри».

Сканування Amazon ECR (Elastic Container Registry). Коли активується сканування Amazon ECR, Amazon Inspector перетворює всі репозиторії у

корпоративному приватному реєстрі з базових репозиторіїв контейнерів сканування на репозиторії розширеного сканування. Ми можемо налаштувати цей параметр із правилами включення для сканування лише під час надсилання або для сканування вибраних репозиторіїв. Amazon Inspector сканує всі образи, надіслані протягом останніх 30 днів або отримані протягом останніх 90 днів. Amazon Inspector продовжує моніторинг образів протягом 90 днів за замовчуванням. Ми можемо змінити цей параметр будь-коли.

Цей тип сканування сканує образи контейнерів та репозиторії контейнерів в Amazon ECR. Під час активації цього типу сканування ми змінюємо налаштування конфігурації сканування для нашого приватного реєстру з базового сканування на розширене сканування. Після активації сканування Amazon ECR ми можемо переглянути, скільки образів та репозиторіїв сканується, на вкладках «Образи контейнерів» та «Репозиторії контейнерів».

Стандартне сканування Lambda. Коли ми активуємо стандартне сканування Lambda, Amazon Inspector виявляє всі функції Lambda у нашому обліковому записі та негайно сканує їх на наявність вразливостей. Amazon Inspector сканує нові функції та шари Lambda під час їх розгортання. Amazon Inspector повторно сканує їх під час оновлення або публікації нових CVE.

Стандартне сканування Lambda – це тип сканування Lambda за замовчуванням. Коли ми активуємо стандартне сканування Lambda, усі наші функції Lambda скануються на наявність програмних вразливостей, якщо вони були викликані або оновлені протягом останніх 90 днів. Після активації стандартного сканування лямбда ми можемо переглянути, скільки функцій Lambda сканується, на вкладці «Функції Lambda».

Сканування Lambda-коду сканує користувацький код програми в Lambda-функції. Коли ми активуємо сканування Lambda-коду, всі наші Lambda-функції будуть скановані на наявність вразливостей коду, якщо вони були викликані або оновлені протягом останніх 90 днів. Після активації стандартного сканування Lambda ми можемо переглянути, скільки Lambda-функцій сканується на наявність вразливостей коду, на вкладці «Lambda-функції».

Стандартне сканування Lambda + сканування Lambda-коду. Коли ми активуємо сканування коду Lambda, Amazon Inspector виявляє функції та шари Lambda у нашому обліковому записі та сканує їх на наявність вразливостей коду. Цей тип сканування оцінює залежності пакетів додатків, що використовуються у функції Lambda, на наявність CVE. Коли ми активуємо цей тип сканування, ми також активуємо стандартне сканування Lambda.

Безпека коду для Amazon Inspector. Цей тип сканування використовує механізм сканування Amazon Q Developer для сканування коду власних програм, залежностей сторонніх програм та інфраструктури як коду на наявність вразливостей.

Цей тип сканування сканує код власних застосунків, залежності сторонніх застосунків та інфраструктуру як код на наявність вразливостей. Після активації Code Security Amazon Inspector починає сканувати корпоративні репозиторії коду на наявність вразливостей коду на основі наших конфігурацій сканування. Після активації Amazon Inspector Code Security ми можемо переглянути, скільки репозиторіїв коду сканується, на вкладці Code Repositories.

2.3. Порядок сканувань рішенням Amazon Inspector. Можливості сканування екземплярів Amazon EC2

Amazon Inspector – це служба керування вразливостями, яка постійно сканує корпоративні екземпляри Amazon Elastic Compute Cloud (Amazon EC2), образи контейнерів Amazon Elastic Container Registry (Amazon ECR) та функції AWS Lambda на наявність програмних вразливостей та ненавмисного мережевого впливу. Ми можемо використовувати Amazon Inspector для отримання видимості та визначення пріоритетів вирішення програмних вразливостей у корпоративних середовищах AWS [13].

Amazon Inspector постійно оцінює корпоративне середовище протягом усього життєвого циклу ресурсів. Він автоматично повторно сканує ресурси у відповідь на зміни, які можуть призвести до появи нової вразливості. Наприклад,

він повторно сканує ресурси, коли ми встановлюємо новий пакет на екземпляр EC2, коли ми встановлюємо патч або коли публікується нова поширена вразливість та експозиція (CVE), яка впливає на ресурс. Коли Amazon Inspector виявляє вразливість або відкритий мережевий шлях, він створює висновки, які ми можемо дослідити. Виявлені висновки містять вичерпну інформацію про вразливість, включаючи наступне [13]:

оцінка ризику Amazon Inspector;

оцінка за Загальною системою оцінювання вразливостей (CVSS);

уражений ресурс;

дані розвідки вразливостей щодо CVE від Amazon, Recorded Future та Агентства з кібербезпеки та безпеки інфраструктури (CISA);

рекомендації щодо усунення недоліків.

Під час активації Amazon Inspector пропонується два варіанти конфігурації: окреме середовище облікових записів та середовище з кількома обліковими записами. Рекомендується використовувати опцію середовища з кількома обліковими записами, якщо треба контролювати кілька облікових записів AWS, які є членами організації в AWS Organizations.

Під час налаштування Amazon Inspector для середовища з кількома обліковими записами ми призначаємо обліковий запис в організації як делегованого адміністратора Amazon Inspector. Делегований адміністратор може керувати результатами пошуку та деякими налаштуваннями для учасників організації. Наприклад, делегований адміністратор може переглядати деталі сукупних результатів пошуку для всіх облікових записів учасників, вмикати або вимикати сканування для облікових записів учасників та переглядати скановані ресурси. AWS SRA рекомендує створити обліковий запис Security Tooling та використовувати його як делегованого адміністратора Amazon Inspector [13].

Amazon Elastic Compute Cloud (Amazon EC2) надає масштабовані обчислювальні потужності на вимогу в хмарі Amazon Web Services (AWS). Використання Amazon EC2 знижує витрати на обладнання, що дозволяє швидше розробляти та розгортати додатки. Ми можемо використовувати Amazon EC2 для

запуску стільки віртуальних серверів, скільки нам потрібно, налаштування безпеки та мережі, а також керування сховищем. Ми можемо збільшувати потужність (масштабувати) для обробки обчислювально ресурсоємних завдань, таких як щомісячні або щорічні процеси або піки трафіку веб-сайту. Коли використання зменшується, ми можемо знову зменшити потужність (масштабувати) [13].

Екземпляр EC2 – це віртуальний сервер у хмарі AWS Cloud. Під час запуску екземпляра EC2 вказаний нами тип екземпляра визначає обладнання, доступне для нього. Кожен тип екземпляра пропонує різний баланс обчислювальних, пам’яттєвих, мережевих та сховищних ресурсів.

Розглянемо можливості сканування екземплярів Amazon EC2 за допомогою Amazon Inspector.

Amazon Inspector Сканування Amazon EC2 витягує метадані з корпоративного екземпляра EC2, перш ніж порівнювати їх із правилами, зібраними з рекомендацій щодо безпеки. Amazon Inspector сканує екземпляри на наявність вразливостей пакетів та проблем з доступністю мережі, щоб отримати відповідні висновки. Amazon Inspector виконує сканування доступності мережі кожні 12 годин та сканування вразливостей пакетів зі змінною частотою, яка залежить від методу сканування, пов’язаного з екземпляром EC2.

Сканування пакетів на вразливості можна виконувати за допомогою методу сканування на основі агента або без агента. Обидва ці методи сканування визначають, як і коли Amazon Inspector збирає інвентаризацію програмного забезпечення з екземпляра EC2 для сканування пакетів на вразливості. Сканування на основі агента збирає інвентаризацію програмного забезпечення за допомогою агента SSM, а сканування без агента збирає інвентаризацію програмного забезпечення за допомогою знімків Amazon EBS.

Amazon Inspector використовує методи сканування, які ми активуємо для свого облікового запису. Під час першої активації Amazon Inspector ваш обліковий запис автоматично реєструється в гібридному скануванні, яке використовує обидва методи сканування. Однак ми можемо змінити цей параметр у будь-який час.

Сканування на основі агентів. Сканування на основі агентів виконується

безперервно за допомогою агента SSM на всіх відповідних екземплярах. Для сканування на основі агентів Amazon Inspector використовує асоціації SSM та плагіни, встановлені через ці асоціації, для збору інвентаризації програмного забезпечення з наших екземплярів. Окрім сканування вразливостей пакетів операційних систем, сканування на основі агентів Amazon Inspector також може виявляти вразливості пакетів мов програмування додатків в екземплярах на базі Linux за допомогою глибокої перевірки Amazon Inspector для екземплярів Amazon EC2 на базі Linux.

У наступному процесі пояснюється, як Amazon Inspector використовує SSM для збору інвентаризації та виконання сканування на основі агентів [13]:

Amazon Inspector створює асоціації SSM у нашому обліковому записі для збору даних про інвентаризацію з ваших екземплярів. Для деяких типів екземплярів (Windows та Linux) ці асоціації встановлюють плагіни на окремі екземпляри для збору даних про інвентаризацію;

за допомогою SSM Amazon Inspector витягує інвентаризацію пакетів з екземпляра;

Amazon Inspector оцінює витягнутий інвентар і генерує висновки щодо будь-яких виявлених вразливостей.

Amazon Inspector використовуватиме агентний метод для сканування екземпляра, якщо він відповідає таким умовам:

екземпляр має підтримувану ОС;

екземпляр не виключається зі сканування тегами виключення Amazon Inspector EC2;

екземпляр керується SSM.

Під час використання методу сканування на основі агентів Amazon Inspector ініціює нові сканування вразливостей екземплярів EC2 у таких ситуаціях:

коли ми запускаємо новий екземпляр EC2;

під час встановлення нового програмного забезпечення на існуючий екземпляр EC2 (Linux та Mac);

коли Amazon Inspector додає новий елемент поширених вразливостей та

ризиків (CVE) до своєї бази даних, і цей CVE стосується корпоративного екземпляра EC2 (Linux та Mac).

Amazon Inspector оновлює поле «Останнє скановане» для екземпляра EC2 після завершення початкового сканування. Після цього поле «Останнє скановане» оновлюється, коли Amazon Inspector оцінює інвентаризацію SSM (за замовчуванням кожні 30 хвилин) або коли екземпляр сканується повторно, оскільки до бази даних Amazon Inspector було додано нове CVE, що впливає на цей екземпляр.

Ми можемо перевірити, коли екземпляр EC2 востаннє сканувався на вразливості, на вкладці «Екземпляри» на сторінці «Керування обліковими записами» або за допомогою команди ListCoverage.

Налаштування агента SSM. Щоб Amazon Inspector міг виявити вразливості програмного забезпечення для екземпляра Amazon EC2 за допомогою методу сканування на основі агентів, екземпляр має бути керованим екземпляром в Amazon EC2 Systems Manager (SSM). На керованому екземплярі SSM встановлено та запущено агент SSM, а SSM має дозвіл на керування екземпляром. Якщо ми вже використовуємо SSM для керування своїми екземплярами, жодних інших кроків для сканування на основі агентів не потрібно виконувати.

Агент SSM інстальовано за замовчуванням на екземплярах EC2, створених з деяких образів машин Amazon (AMI).

Розглянемо, як налаштувати екземпляр Amazon EC2 як керований екземпляр за допомогою профілю екземпляра IAM.

AmazonSSMManagedInstanceCore – це рекомендована політика для використання під час підключення профілю екземпляра. Ця політика має всі дозволи, необхідні для сканування Amazon Inspector EC2.

Ресурси SSM, створені для сканування

Для запуску сканування Amazon Inspector EC2 у нашому обліковому записі потрібна низка ресурсів SSM. Під час першої активації сканування Amazon Inspector EC2 створюються такі ресурси [13]:

InspectorInventoryCollection-do-not-delete

Це асоціація Systems Manager State Manager (SSM), яку Amazon Inspector використовує для збору даних про інвентаризацію програмних застосунків з ваших екземплярів Amazon EC2. Якщо наш обліковий запис вже має асоціацію SSM для збору даних про інвентаризацію з *InstanceIds**, Amazon Inspector використовуватиме її замість створення власної.

InspectorResourceDataSync-do-not-delete

Це синхронізація даних ресурсів, яку Amazon Inspector використовує для надсилання зібраних даних інвентаризації з наших екземплярів Amazon EC2 до корзини Amazon S3, що належить Amazon Inspector.

InspectorDistributor-do-not-delete

Це асоціація SSM, яку Amazon Inspector використовує для сканування екземплярів Windows. Ця асоціація встановлює плагін Amazon Inspector SSM на наші екземпляри Windows. Якщо файл плагіна буде випадково видалено, ця асоціація перевстановить його під час наступного інтервалу асоціації.

InvokeInspectorSsmPlugin-do-not-delete

Це асоціація SSM, яку Amazon Inspector використовує для сканування екземплярів Windows. Ця асоціація дозволяє Amazon Inspector ініціювати сканування за допомогою плагіна, ми також можемо використовувати його для встановлення власних інтервалів для сканування екземплярів Windows.

InspectorLinuxDistributor-do-not-delete

Це асоціація SSM, яку Amazon Inspector використовує для глибокої перевірки Amazon EC2 Linux. Ця асоціація встановлює плагін Amazon Inspector SSM на наші екземпляри Linux.

InvokeInspectorLinuxSsmPlugin-do-not-delete

Це асоціація SSM, яку Amazon Inspector використовує для глибокої перевірки Amazon EC2 Linux. Ця асоціація дозволяє Amazon Inspector ініціювати сканування за допомогою плагіна.

Розглянемо безагентне сканування.

Amazon Inspector використовує метод безагентного сканування у відповідних випадках, коли наш обліковий запис перебуває в гібридному режимі сканування.

Гібридний режим сканування включає сканування на основі агентів та без агентів і автоматично вмикається, коли ви активуєте сканування Amazon EC2.

Для безагентного сканування Amazon Inspector використовує знімки EBS для збору інвентаризації програмного забезпечення з наших екземплярів. Безагентне сканування сканує екземпляри на наявність вразливостей операційної системи та пакетів мов програмування додатків.

У наведеному нижче процесі пояснюється, як Amazon Inspector використовує знімки EBS для збору даних про інвентаризацію та виконання сканування без агента [13]:

Amazon Inspector створює знімок EBS усіх томів, підключених до екземпляра. Поки Amazon Inspector його використовує, знімок зберігається у нашому обліковому записі та позначений InspectorScanяк ключ тегу, а також унікальним ідентифікатором сканування як значенням тегу;

Amazon Inspector отримує дані зі знімків за допомогою прямих API EBS та оцінює їх на наявність вразливостей. Для будь-яких виявлених вразливостей генеруються висновки;

Amazon Inspector видаляє створені ним знімки EBS у нашому обліковому записі.

Amazon Inspector використовуватиме безагентний метод для сканування екземпляра, якщо він відповідає таким умовам [13]:

екземпляр має підтримувану ОС;

екземпляр має статус *Unmanaged EC2 instance*, *Stale inventory* або *No inventory*;

екземпляр підтримується Amazon EBS та має один із таких форматів файлової системи:

ext3

ext4

xfs

екземпляр не виключається зі сканування за допомогою тегів виключення Amazon EC2;

кількість томів, підключених до екземпляра, менша за 8, а їхній загальний розмір не перевищує 1200 ГБ.

Розглянемо поведінку сканування без агента.

Якщо наш обліковий запис налаштовано на гібридне сканування, Amazon Inspector виконує безагентне сканування відповідних екземплярів кожні 24 години. Amazon Inspector виявляє та сканує нові відповідні екземпляри щогодини, включаючи нові екземпляри без агентів SSM або вже існуючі екземпляри зі статусом, що змінився на SSM_UNMANAGED.

Amazon Inspector оновлює поле «Останнє сканування» для екземпляра Amazon EC2 щоразу, коли він сканує витягнуті знімки з екземпляра після сканування без агента.

Ми можемо перевірити, коли екземпляр EC2 востаннє сканувався на вразливості, на вкладці «Екземпляри» на сторінці «Керування обліковими записами» або за допомогою команди ListCoverage.

Розглянемо керування режимом сканування.

Режим сканування EC2 визначає, які методи сканування використовуватиме Amazon Inspector під час виконання сканування EC2 у нашому обліковому записі. Ми можемо переглянути режим сканування для свого облікового запису на сторінці налаштувань сканування EC2 у розділі Загальні налаштування. Окремі облікові записи або уповноважені адміністратори Amazon Inspector можуть змінювати режим сканування. Якщо ми встановлюємо режим сканування як уповноважений адміністратор Amazon Inspector, цей режим сканування встановлюється для всіх облікових записів учасників нашої організації. Amazon Inspector має такі режими сканування [13]:

сканування на основі агента – у цьому режимі сканування Amazon Inspector використовуватиме виключно метод сканування на основі агента під час сканування пакетів на наявність вразливостей. Цей режим сканування сканує лише керовані екземпляри SSM у нашому обліковому записі, але має перевагу в забезпеченні безперервного сканування у відповідь на нові CVE або зміни в екземплярах. Сканування на основі агента також забезпечує глибоку перевірку

Amazon Inspector для відповідних екземплярів. Це режим сканування за замовчуванням для щойно активованих облікових записів;

гібридне сканування – у цьому режимі сканування Amazon Inspector використовує комбінацію методів на основі агентів та без агентів для сканування пакетів на наявність вразливостей. Для відповідних екземплярів EC2, на яких встановлено та налаштовано агент SSM, Amazon Inspector використовує метод на основі агентів. Для відповідних екземплярів, які не керуються SSM, Amazon Inspector використовуватиме метод без агентів для відповідних екземплярів, що підтримуються EBS.

3 ТЕХНОЛОГІЯ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ХМАРНИХ КОРПОРАТИВНИХ РЕСУРСІВ НА ОСНОВІ AMAZON INSPECTOR

3.1. Порядок застосування рішення Amazon Inspector

Розглянемо порядок практичного застосування AWS Inspector для сканування корпоративних хмарних ресурсів, зокрема екземплярів EC2.

Необхідно увійти до свого облікового запису AWS, використовуючи обліковий запис адміністратора або обліковий запис із правами адміністратора, щоб увімкнути сервіс, і перейти до Inspector.

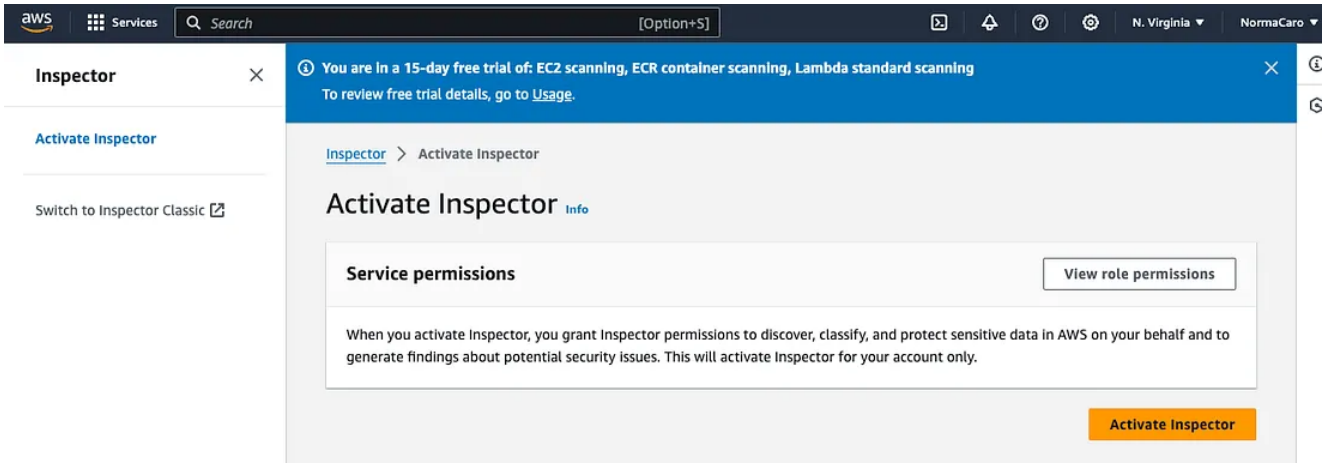

Рис. 3.1. Активація AWS Inspector

В AWS Inspector ми побачимо панель інструментів зі зведеним виглядом, що містить інформацію про охоплення навколишнього середовища, критичні висновки та заходи щодо усунення наслідків на основі ризиків.

Ліворуч ми побачимо результати з різним розподілом, таким як за вразливістю, за екземпляром тощо (рисунок 3.2).

AWS Inspector залежить від ролі SSM або ролі з дозволами SSM для можливості зв’язку з агентом SSM всередині EC2. Тому створюється ця роль, використовуючи опцію швидкого налаштування SSM.

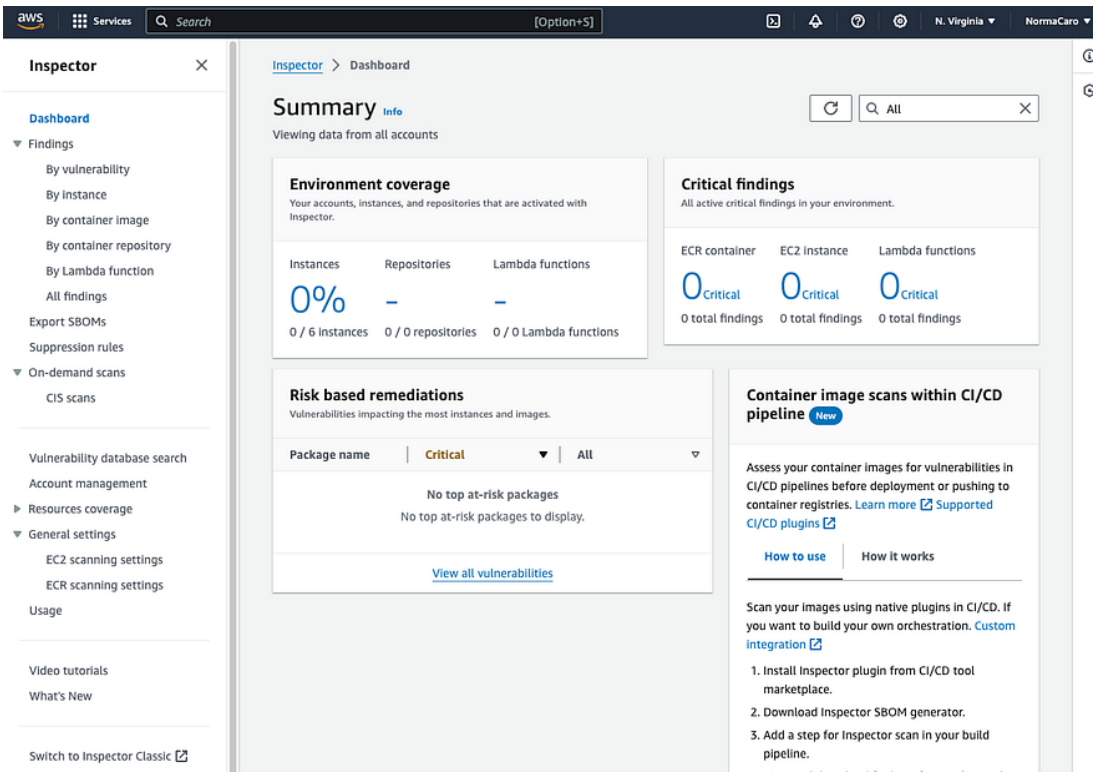

Рис. 3.2. Панель інструментів Amazon Inspector

Далі створюється EC2 та підтверджується встановлення агента для тесту (рисунок 3.3).

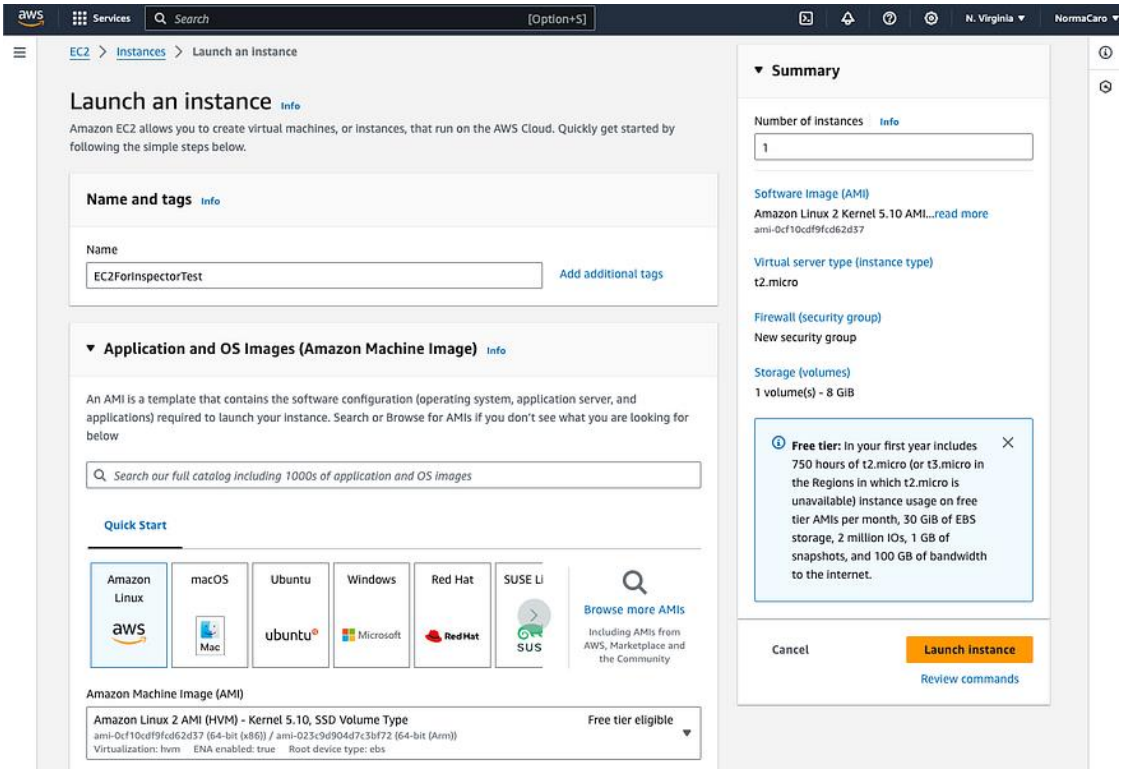

Рис. 3.3. Створення середовища EC2

У розділі «Пара ключів (вхід)» створюється нова пара ключів, яку нам потрібно буде використовувати для входу до EC2 через термінал (рисунок 3.4).

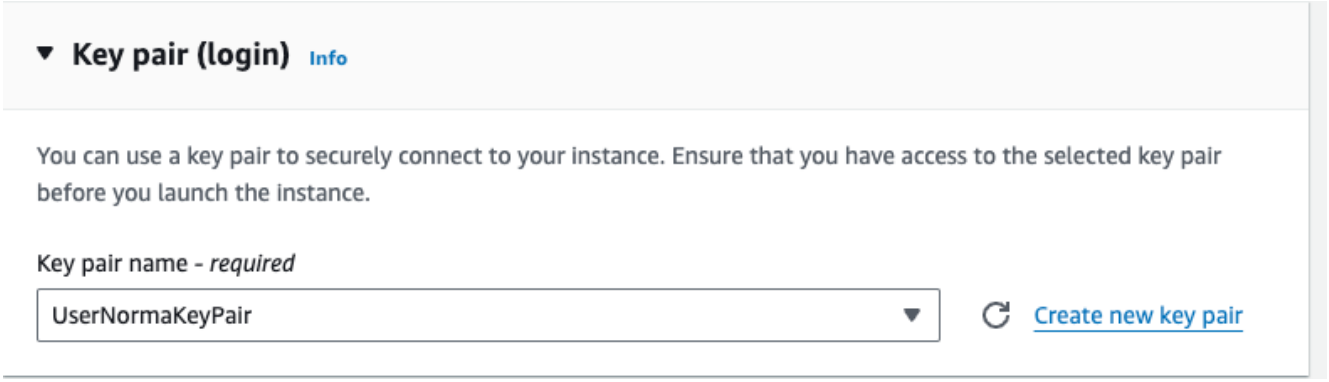

Рис. 3.4. Створення пари ключів для входу до EC2

Запускаємо екземпляр. Має відобразитися повідомлення про успіх разом з ідентифікатором екземпляра (рисунок 3.5).

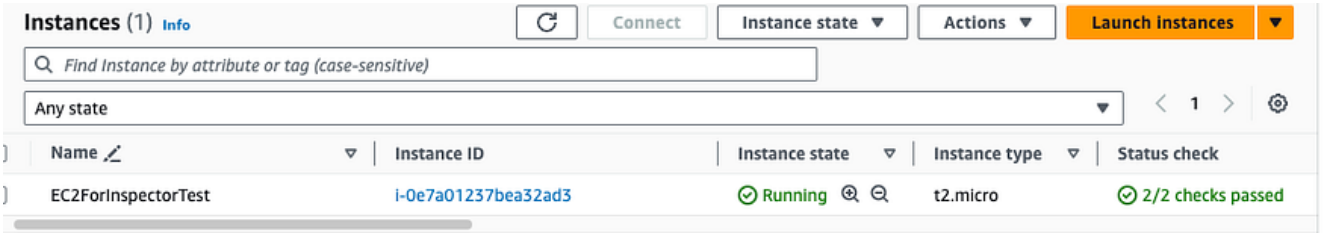

Рис. 3.5. Запуск екземпляра EC2

Далі підключимося до екземпляра EC2, щоб підтвердити існування агента SSM. Ми повинні побачити підтвердження того, що агент «активний (працює)». Далі необхідно прикріпити роль агента SSM до екземпляра EC2. Виберіть свій екземпляр, натисніть «Дії», потім «Безпека», а потім «Змінити роль IAM» (рисунок 3.6).

На екрані «Змінити роль IAM» вибираємо роль, яку ми створили раніше, вибираємо *SSMRoleForInspectorScans*. Натискаємо «Оновити роль IAM» (рисунок 3.7).

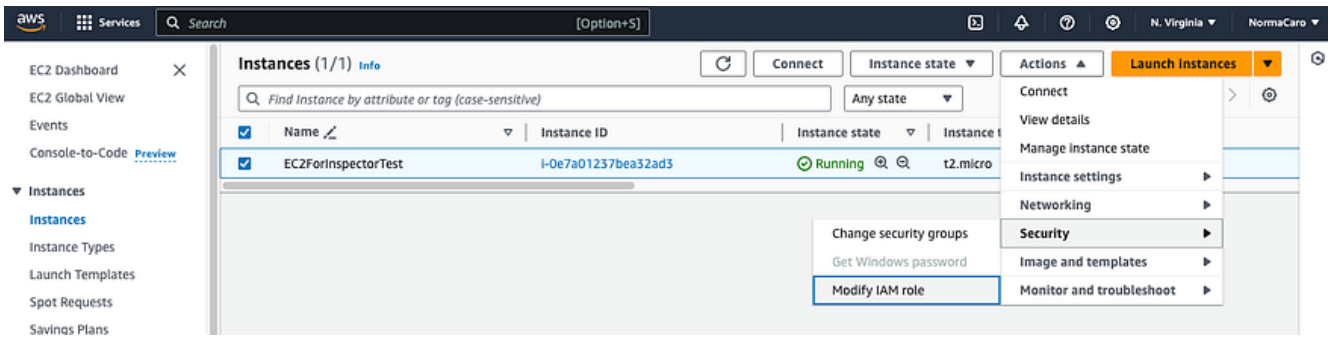

Рис. 3.6. Зміна ролі IAM для можливості сканування

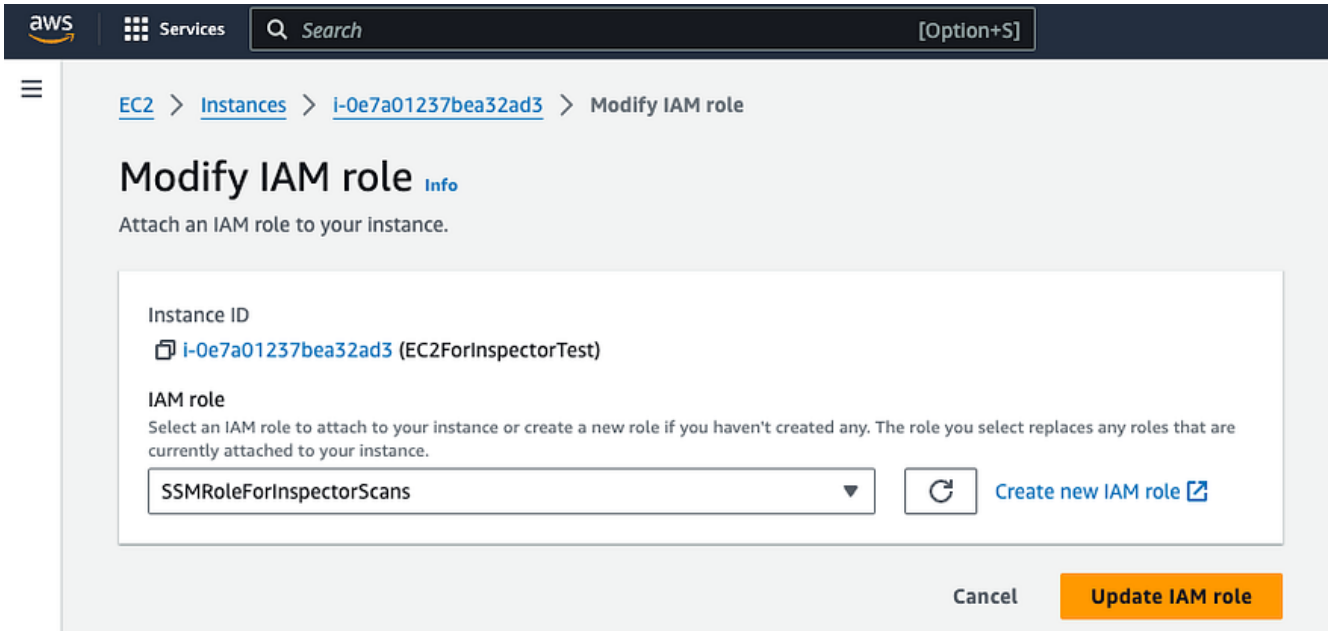

Рис. 3.7. Зміна ролі IAM

Коли створено екземпляр та одночасно підключено роль SSM, початкове сканування Inspector почне одразу. Після завершення сканування ми можемо повернутися до своєї інформаційної панелі та переглянути результати (рисунок 3.8).

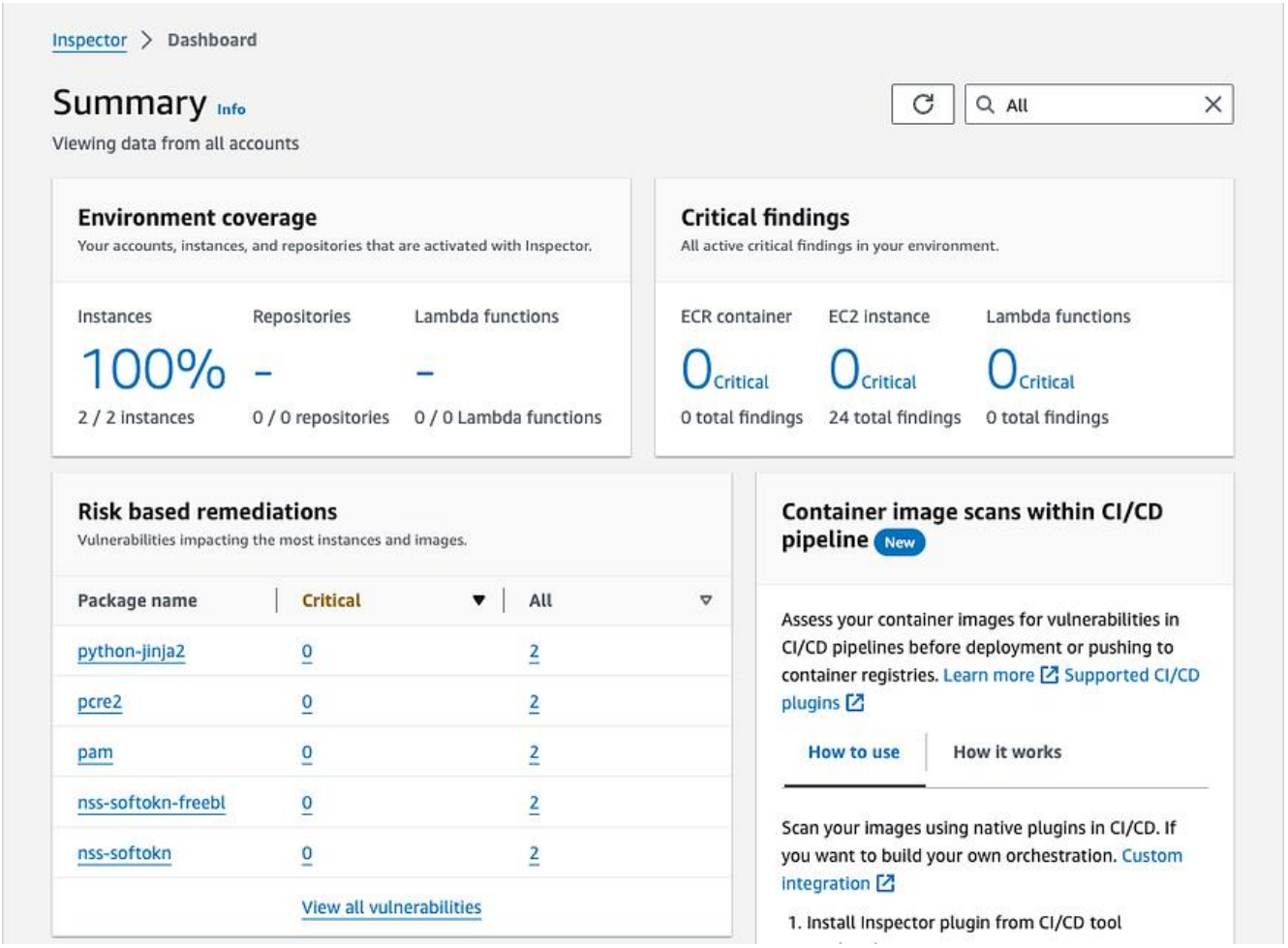

Рис. 3.8. Результати сканування корпоративного середовища

У розділі «Підсумок» ми побачимо оновлений відсоток, що відображає кількість екземплярів, що скануються AWS Inspector. Ми також можемо побачити критичні результати для функцій ECR, EC2 та Lambda. У нас також є подання «Виправлення на основі ризиків», яке покаже, скільки екземплярів постраждали від одного й того ж пакета.

Обираючи «За вразливістю» в розділі «Виявлені проблеми» ми побачимо знайдені вразливості, а також їх рейтинг «критичний» або «високий» (рисунок 3.9).

Розділ «За екземплярами» містить представлення критичних та високих рівнів для кожного екземпляра (рисунок 3.10).

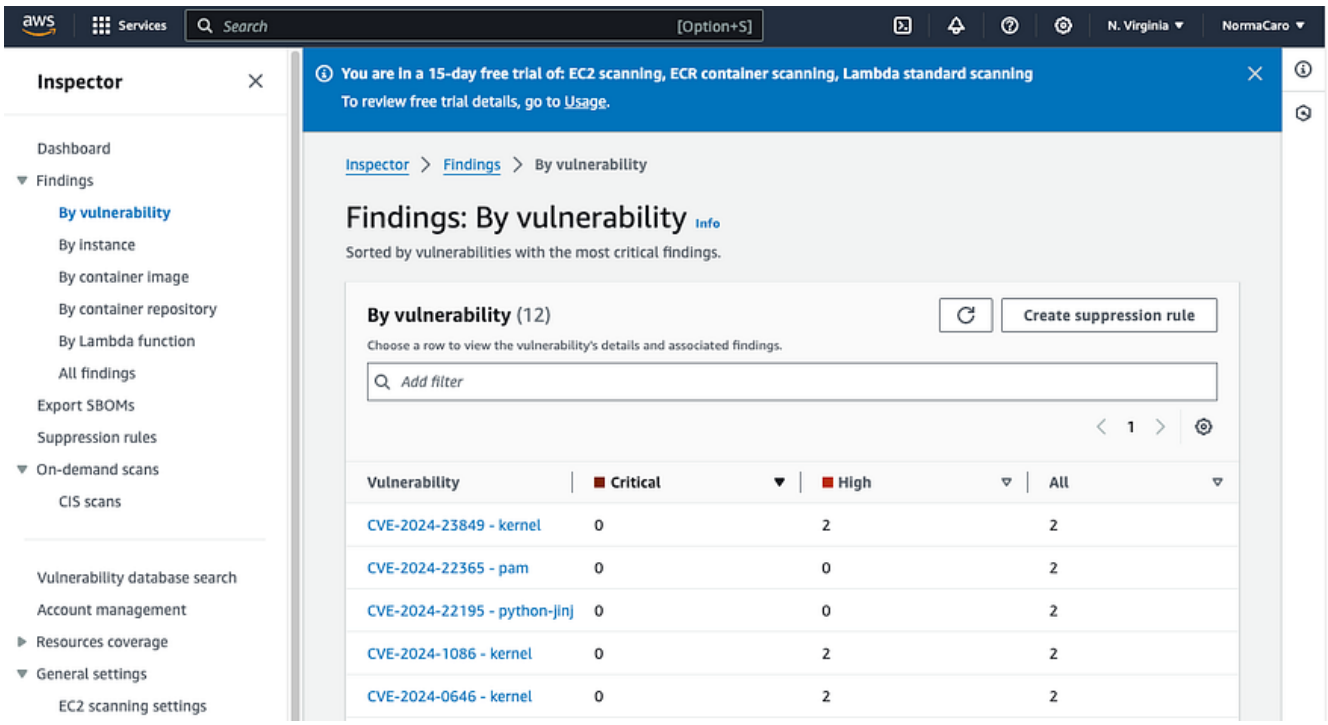

Рис. 3.9. Виявлені вразливості

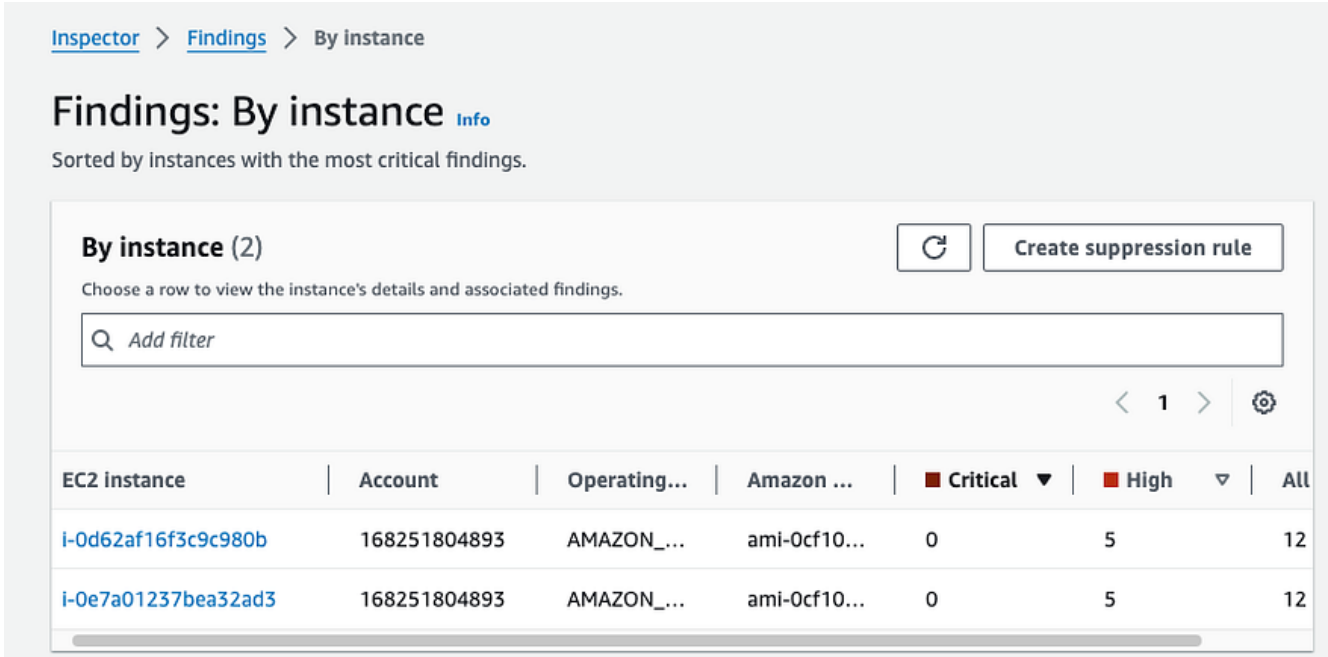

Рис. 3.10. Знахідки за екземплярами

Приклад детальної інформації про вразливість, включаючи рівень серйозності, тип, час її створення, уражений пакет, а також рекомендовані способи усунення показано на рисунку 3.11

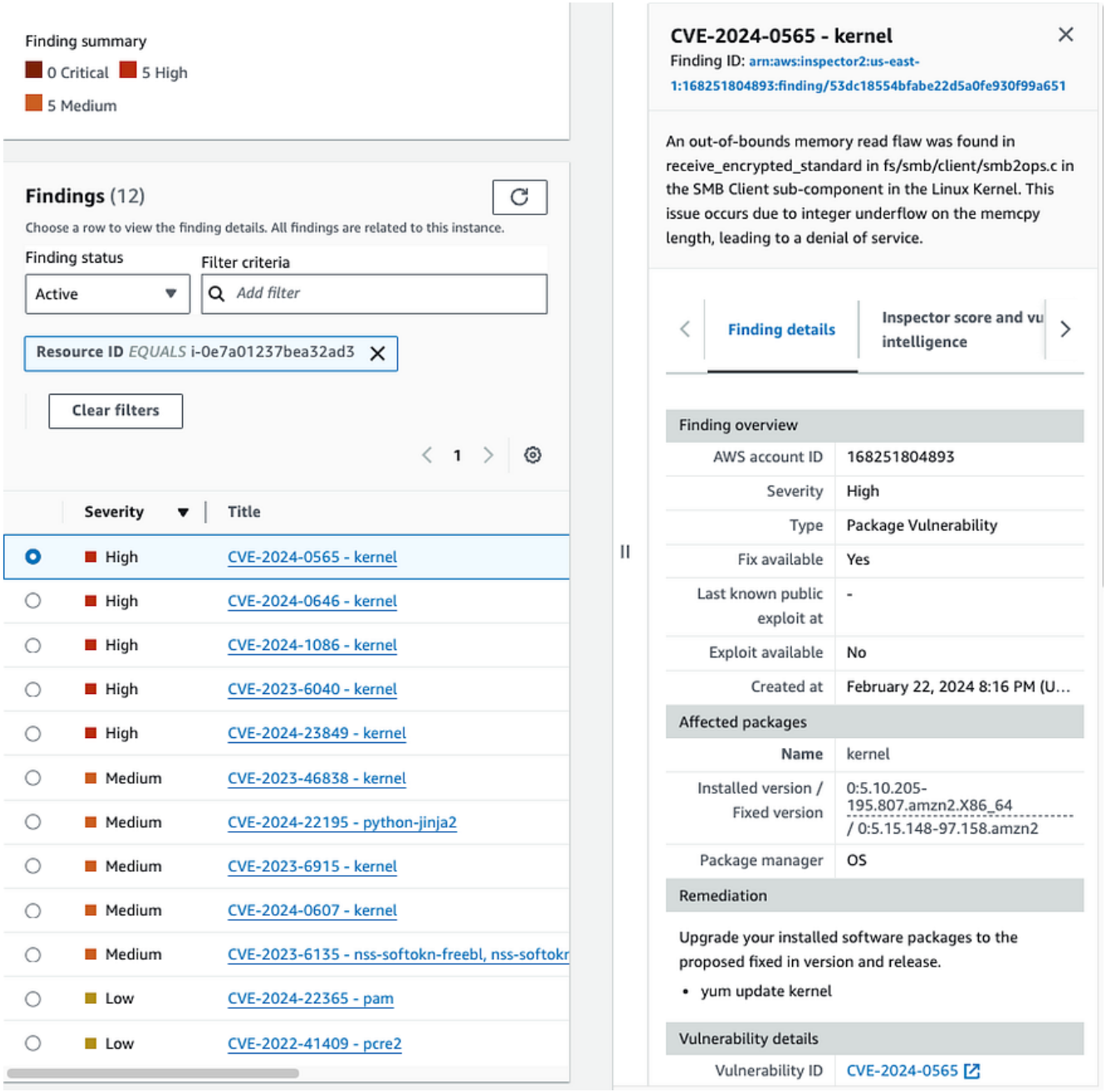

Рис. 3.11. Детальна інформація про вразливість

На вкладці «Оцінка Inspector та інформація про вразливості» (рисунок 3.12) ми побачимо порівняння оцінок. Оцінка CVSS V3 – це стандартна оцінка, оприлюднена для спільноти. Однак Amazon Inspector має власну логіку, згідно з якою він застосовує оцінку CVSS та знижує її, якщо виявляє, що вразливість не така висока, залежно від таких факторів, як мережа. Тобто, вразливість, яка знаходиться в загальнодоступній мережі, менш схильна до проблеми в приватній мережі. AWS Inspector враховує ці сценарії та позначає оновлену оцінку як свою

оцінку. У даному випадку різниці немає, оскільки систему розгорнуто в загальнодоступній підмережі.

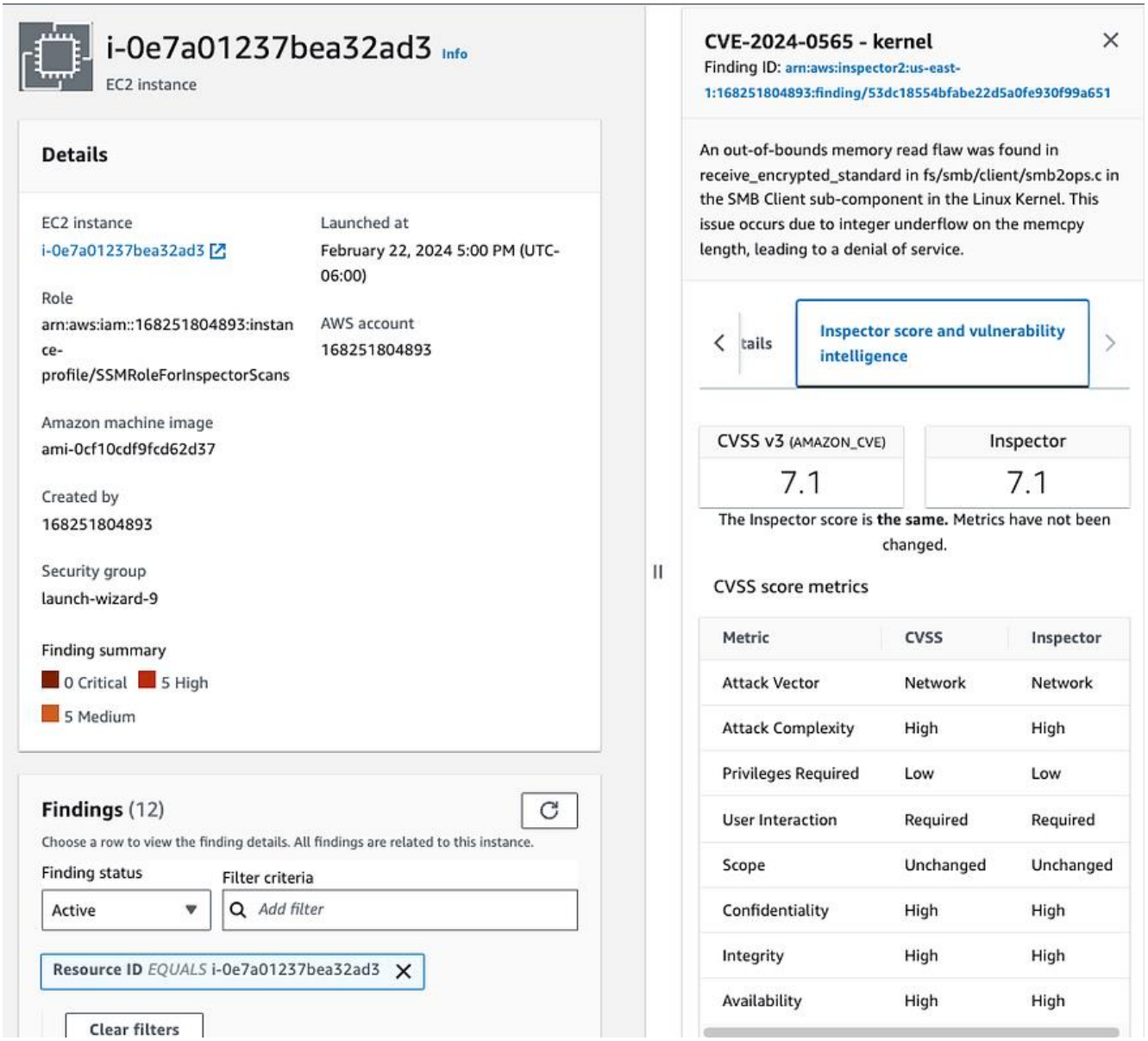

Рис. 3.12. Оцінка Inspector та інформація про вразливості

За назвою CVE-2024–0565 у Національній базі даних вразливостей NIST ми можемо знайти більше деталей (перехід за посиланням https://nvd.nist.gov/vuln/detail/CVE-2024-0565). У розділі «Коротка інформація» зазначено, що цей CVE вперше був опублікований 15.01.2024.

Отже, ми розглянули на прикладі, як правильно налаштувати екземпляр, роль та консоль AWS Inspector для виконання сканування. Ми не розглядали інші

області AWS Inspector, такі як Amazon ECR та AWS Lambda.

3.2. Технологія управління вразливостями хмарних корпоративних ресурсів на основі Amazon Inspector

Управління вразливостями – це процес виявлення, оцінки та зменшення вразливостей безпеки у корпоративній IT-інфраструктурі для зменшення ризику кібератак. У сучасному швидкозмінному ландшафті загроз проактивне управління вразливостями є критично важливим для захисту корпоративних систем, захисту конфіденційних даних та забезпечення дотримання галузевих норм.

Необхідно відмітити, що управління вразливостями хмарних корпоративних ресурсів на основі Amazon Inspector здійснюється шляхом безперервного, автоматизованого сканування робочих навантажень AWS, виявлення вразливостей, оцінки ризиків та надання детальних рекомендацій для їх усунення.

Amazon Inspector – це сервіс управління вразливостями, який автоматично виявляє робочі навантаження AWS (наприклад, інстанси Amazon EC2, образи контейнерів в Amazon ECR, функції AWS Lambda, а також вихідний код і інфраструктуру як код (IaC)) та безперервно їх оцінює.

Визначимо основні етапи управління вразливостями за допомогою Amazon Inspector.

1. Автоматичне виявлення та активація:

виявлення ресурсів: Amazon Inspector автоматично знаходить підтримувані ресурси AWS в організації;

організаційне управління: використовуючи AWS Organizations, можна централізовано керувати Amazon Inspector через єдиний обліковий запис (делегований адміністратор), активуючи сканування для всіх облікових записів організації одним кліком.

2. Безперервне сканування. Amazon Inspector здійснює постійне сканування ресурсів на наявність:

вразливостей програмного забезпечення (Software Vulnerabilities).

Здійснюється сканування операційних систем, мов програмування та залежностей, включаючи поширені вразливості та експозиції (CVE). Для EC2-інстансів використовується як агентне, так і безагентне сканування;

ненавмисного мережевого доступу (Unintended Network Exposure). Здійснюється оцінка мережевої доступності EC2-інстансів, виявляючи потенційні шляхи доступу з Інтернету або зовнішніх мереж;

недоліків у коді та конфігурації (Code and Configuration Flaws). Проводиться сканування вихідного коду (Static Application Security Testing – SAST) для виявлення вразливостей і помилок конфігурації. Здійснюється аналіз залежностей сторонніх розробників (Software Composition Analysis – SCA). Проводиться сканування Інфраструктури як Коду (IaC) для перевірки визначень інфраструктури (наприклад, CloudFormation, Terraform).

3. Генерація та пріоритезація знахідок (Findings):

формування знахідок. Коли Amazon Inspector виявляє вразливість або проблему конфігурації, він створює знахідку (finding) – детальний звіт про проблему;

оцінка ризиків. Знахідки автоматично пріоритезуються на основі оцінки ризиків Inspector. Це допомагає зосередитися на найбільш критичних проблемах, які мають високу тяжкість (severity) та мережеву доступність або пов’язані з критичними робочими навантаженнями;

деталізація. Кожна знахідка містить детальні рекомендації щодо усунення проблеми.

4. Етап усунення та інтеграції:

централізоване управління. Знахідками можна керувати в консолі Amazon Inspector або через API;

інтеграція з AWS Security Hub. Amazon Inspector автоматично надсилає знахідки до AWS Security Hub, забезпечуючи централізовану видимість стану безпеки всього середовища AWS;

«Shift-Left Security». Засоби захисту коду Amazon Inspector дозволяють інтегрувати сканування безпосередньо в процеси CI/CD (наприклад, GitHub,

GitLab), що дозволяє розробникам виявляти та виправляти проблеми на ранніх етапах розробки («зсув безпеки вліво»);

експорт SBOM. Сервіс дозволяє централізовано керувати та експортувати специфікації програмного забезпечення (SBOM – Software Bill of Materials) для відстежуваних ресурсів.

Цей процес забезпечує проактивний підхід до управління вразливостями, скорочуючи середній час на усунення проблем (MTTR) та допомагаючи підтримувати відповідність галузевим стандартам (наприклад, бенчмарки CIS).

Отже, основний зміст технології управління вразливостями хмарних корпоративних ресурсів на основі Amazon Inspector полягає в автоматизованому та безперервному скануванні робочих навантажень AWS (таких як інстанси EC2, образи контейнерів ECR та функції Lambda) для виявлення вразливостей програмного забезпечення та ненавмисного мережевого доступу.

Після активації, Amazon Inspector автоматично виявляє всі підтримувані ресурси у корпоративному середовищі AWS без необхідності ручного втручання чи встановлення додаткового програмного забезпечення (хоча для деяких функцій сканування EC2 використовується агент SSM).

Корпоративні інформаційні ресурси постійно скануються. Повторне сканування також ініціюється автоматично у відповідь на зміни, які можуть внести нові вразливості (наприклад, встановлення нових пакетів, оновлення програмного забезпечення або публікація нових загальновідомих вразливостей та експлойтів – CVE).

Amazon Inspector оцінює вразливості на основі галузевих стандартів, таких як перелік CVE та система оцінки CVSS (Common Vulnerability Scoring System). Кожній знайденій проблемі присвоюється контекстуалізований рівень ризику (Amazon Inspector risk score), що допомагає сфокусуватись на найбільш критичних загрозах.

При виявленні вразливості або ненавмисного мережевого доступу генерується детальний звіт (finding), який містить інформацію про проблему, уражений ресурс, рівень серйозності та рекомендації щодо усунення.

Результати сканування агрегуються в консолі Amazon Inspector та можуть бути передані до інших сервісів AWS, таких як AWS Security Hub для централізованого управління безпекою та Amazon EventBridge для автоматизації робочих процесів реагування.

3.3. Рекомендації щодо управління вразливостями хмарних корпоративних ресурсів

Найкращі практики управління вразливостями хмарних технологій включають постійне виявлення та інвентаризація всіх активів, автоматизоване та безперервне сканування для виявлення вразливостей, а також визначення пріоритетів вразливостей на основі контексту та інформації про загрози. Також критично важливо безпечно виправляти та перевіряти виправлення, інтегрувати безпеку в життєвий цикл розробки («зсув ліворуч») та впроваджувати надійний контроль доступу, керування конфігурацією та шифрування даних.

Основними рекомендаціями та вимогами щодо управління вразливостями хмарних корпоративних ресурсів є:

необхідні постійні виявлення та інвентаризація активів. Ведіть комплексну інвентаризацію всіх хмарних активів у режимі реального часу. Ви не можете захистити те, що не бачите, тому використовуйте автоматизовані інструменти для постійного сканування та категоризації нових або змінених активів;

впроваджуйте безперервне сканування. Автоматизуйте сканування вразливостей для регулярного виявлення неправильних конфігурацій, застарілого програмного забезпечення та інших вразливостей. Інтегруйте канали інформації про загрози для підвищення точності;

забезпечте суворий контроль доступу користувачів. Використовуйте принцип найменших привілеїв, впроваджуючи контроль доступу на основі ролей (RBAC) та багатофакторну автентифікацію (MFA). Регулярно проводьте аудит облікових записів користувачів та видаляйте невикористовувані ролі;

застосовуйте шифрування даних. Використовуйте шифрування для захисту

даних як у стані спокою, так і під час передачі. Класифікуйте дані для застосування відповідних політик шифрування, використовуйте надійні алгоритми та безпечно керуйте ключами шифрування.

Основними рекомендаціями та вимогами щодо відновлення та пом’якшення наслідків атак на хмарні корпоративні ресурси є:

використовуйте визначення пріоритетів вразливостей. Спочатку зосередьтеся на найважливіших ризиках, використовуючи такі фактори, як інформація про загрози, критичність активів та контекст, для визначення пріоритетів;

застосовуйте виправлення та перевірки. Негайно встановлюйте виправлення, оновлюйте програмне забезпечення або коригуйте конфігурації. Після виправлення виконайте перевірки, щоб підтвердити усунення вразливості;

використовуйте альтернативні методи пом’якшення наслідків атак. Коли встановлення виправлень неможливе, використовуйте альтернативні методи, такі як сегментація мережі або посилення конфігурації, щоб зменшити ризик;

застосовуйте інтеграцію безпеки в розробку. Вбудовуйте перевірки безпеки на ранніх етапах розробки (CI/CD), включаючи сканування IaC, перевірки залежностей та сканування образів контейнерів.

Також основними рекомендаціями та вимогами щодо постійного управління вразливостями хмарних корпоративних ресурсів є:

здійснення постійного моніторинуг та перевірок. Використовуйте постійний моніторинг для виявлення нових вразливостей та перевірки ефективності заходів щодо їх усунення. Проводьте періодичне тестування на проникнення для підтвердження рівня безпеки;

необхідно сприяти міжфункціональній співпраці. Забезпечте спільну роботу команд безпеки, IT-операцій та розробників для узгодження зусиль щодо усунення недоліків з пріоритетами бізнесу;

використовуйте автоматизацію та інструменти. Використовуйте інструменти управління вразливостями, які інтегруються з іншими рішеннями безпеки та забезпечують повну видимість;

необхідно застосовувати звітування та комунікацію. Використовуйте інформаційні панелі та регулярні звіти, щоб повідомляти про стан вразливостей та ризиків відповідним зацікавленим сторонам, допомагаючи керувати розподілом ресурсів.

Щоб створити ефективну стратегію управління вразливостями хмарних корпоративних ресурсів, організації повинні враховувати низку факторів, таких як:

толерантність до ризику. Визначте толерантність організації до ризику та необхідно розставити пріоритети у розподілі ресурсів, спочатку оцінивши потенційні загрози, вразливості та вплив порушення;

вимоги до відповідності. Переконайтеся, що управління вразливостями хмарних корпоративних ресурсів враховує вимоги щодо відповідності, що застосовуються до організації, такі як GDPR або HIPAA, або галузеві стандарти, такі як CIS Benchmarks або NIST SP 800-53;

модель спільної відповідальності. Модель спільної відповідальності стверджує, що постачальники хмарних послуг (CSP) відповідають за фізичну інфраструктуру та оновлення, тоді як їхні клієнти несуть відповідальність за правильне та безпечне налаштування послуг для захисту конфіденційних даних;

чіткі обов’язки. Ефективна співпраця забезпечує як безпеку, так і підзвітність в організації. Встановіть чіткі ролі та канали зв’язку між командою хмарної безпеки, командою IT/операцій та розробниками для сприяння культурі безпеки;

вразливості. Використовуйте ризико орієнтований підхід до управління вразливостями. Використовуйте канали аналітики загроз, галузеві звіти та рекомендації постачальників, а також оцінюйте ймовірність експлуатації та потенційної шкоди під час розробки та впровадження стратегій усунення недоліків.

Розглянемо рекомендації щодо побудови процесу управління вразливостями для хмарних ресурсів, використовуючи Amazon Inspector. Цей сервіс дозволяє автоматизувати виявлення вразливостей програмного забезпечення та ненавмисного мережевого доступу.

1. Архітектура та налаштування (Deployment & Configuration)

Перший крок – це правильна активація сервісу для забезпечення

максимального покриття. Централізоване управління (AWS Organizations):

використовуйте *Delegated Administrator* для Amazon Inspector. Це дозволяє команді безпеки керувати налаштуваннями для всіх акаунтів організації з одного місця;

увімкніть авто-активацію (Auto-enable) для нових акаунтів та ресурсів (EC2, ECR, Lambda), щоб уникнути «сліпих зон» при масштабуванні інфраструктури.

Щодо забезпечення видимості (SSM Agent):

для сканування EC2 критично важливо, щоб AWS Systems Manager (SSM) Agent був встановлений, запущений та мав відповідні IAM-ролі;

необхідно налаштувати SSM State Manager або Default Host Management Configuration, щоб агент автоматично оновлювався і був активним на всіх інстансах.

2. Стратегія сканування (Scanning Strategy)

Amazon Inspector працює в режимі безперервного сканування (continuous scanning), що відрізняється від традиційних сканерів, які запускаються за розкладом.

Типи ресурсів та особливості, які необхідно враховувати:

Amazon EC2: необхідно налаштувати сканування для автоматичного запуску при встановленні нового пакету або виявленні нової CVE (Common Vulnerabilities and Exposures);

Amazon ECR (Контейнери): необхідно налаштувати Enhanced Scanning. Це дозволяє сканувати образи не лише при завантаженні (on-push), а й безперервно моніторити їх на нові загрози протягом всього життєвого циклу.

AWS Lambda: необхідно активувати сканування коду (Lambda code scanning) для пошуку вразливостей у залежностях та самому коді функцій (наприклад, hardcoded secrets);

використовуйте Deep Inspection для EC2 (Linux), щоб аналізувати не тільки пакети ОС, але й бібліотеки додатків (Python, Java, Node.js, Go тощо).

3. Пріоритезація ризиків (Risk Prioritization)

Не всі вразливості однакові. Використовуйте контекстний скоринг Amazon

Inspector для зменшення шуму.

Amazon Inspector Score на відміну від стандартного CVSS (Common Vulnerability Scoring System), Inspector враховує контекст середовища.

Необхідно воаховувати фактори: Чи доступний ресурс з інтернету? Чи є активний експлойт для цієї вразливості?

Необхідно пріоритезувати виправлення вразливостей, які мають високий Inspector Score, а не просто високий CVSS.

Звертайте особливу увагу на знахідки типу «Network Reachability». Вони вказують на порти, які відкриті для інтернету (наприклад, SSH на порту 22), що є критичним ризиком.

4. Автоматизація реагування та виправлення (Remediation)

Ручне виправлення неефективне в хмарі. Тому, побудуйте автоматизований процес. Для цього необхідно:

інтеграція з AWS Security Hub. Налаштуйте відправку всіх знахідок (Findings) у AWS Security Hub. Це дозволить бачити вразливості в контексті загальної безпекової оцінки (Compliance scores);

сценарії автоматизації (EventBridge & Lambda):

для сповіщення при виявленні вразливості з Critical Severity, EventBridge тригерить SNS топік для відправки повідомлення в Slack/Teams або створення тікета в Jira (через API);

використовуйте AWS Systems Manager Patch Manager для використання автоматичного патчингу;

створіть правило для того щоб, якщо Inspector знаходить вразливість, яку можна виправити оновленням пакету, автоматично запускати SSM Run Command для оновлення цього пакету (для Dev/Test середовищ).

5. Управління виключеннями (Suppression Rules)

Щоб уникнути втоми від сповіщень (Alert Fatigue), налаштуйте правила придушення, а саме:

створіть Suppression Rules для вразливостей, які ви приймаєте як ризик, або які неможливо виправити (наприклад, через legacy софт у внутрішньому

периметрі);

використовуйте теги ресурсів (наприклад, Environment: Sandbox), щоб ігнорувати певні типи сповіщень для некритичних середовищ, але продовжувати їх фіксувати для звітності.

6. Звітність та метрики (Reporting)

Необхідне зробити наступне:

для експорту у S3 налаштуйте регулярний експорт знахідок у Amazon S3 bucket;

для візуалізація (Amazon QuickSight) підключіть QuickSight до S3 для створення дашбордів для керівництва (наприклад, «Середній час виправлення критичних вразливостей – MTTR»);

відстежуйте відсоток покриття інфраструктури (чи всі EC2 мають SSM агент?) та динаміку зменшення кількості відкритих вразливостей.

ВИСНОВКИ

В роботі досліджено проблему управління вразливостями хмарних корпоративних ресурсів, визначено його мету та завдання. Хмарні технології забезпечують бізнес надійним та безпечним середовищем для розміщення критично важливих даних і послуг. Але без чіткої стратегії безпеки та контролю доступу до хмари, який здійснюється користувачем, вразливості можуть перетворитися на руйнівну бізнес-загрозу.

Визначено існуючі підходи до управління вразливостями хмарних корпоративних ресурсів. Управління вразливостями в хмарних обчисленнях – це процес виявлення, визначення пріоритетів та усунення слабких місць безпеки в хмарній інфраструктурі, системах і додатках. Проактивно усуваючи вразливості хмари, ми можемо впровадити заходи контролю, які запобігатимуть використанню зловмисниками неправильних конфігурацій та інших проблем безпеки хмари.

Проаналізовано існуючі провідні рішення для управління вразливостями хмарних корпоративних ресурсів. Для ефективного управління вразливостями в хмарних середовищах слід використовувати різноманітні спеціалізовані інструменти, розроблені для оптимізації процесу. Використання цих інструментів дозволяє розробляти надійні стратегії управління вразливостями в хмарі, адаптовані до унікального профілю загроз корпоративним ресурсам.

Визначено призначення, основні функції та склад рішення Amazon Inspector. Рішення Amazon Inspector – це автоматизована служба управління вразливостями, розроблена для забезпечення безпеки корпоративних робочих навантажень AWS. Воно автоматично виявляє такі ресурси, як екземпляри Amazon EC2, образи контейнерів в Amazon ECR та функції Lambda, а потім постійно сканує їх на наявність програмних вразливостей та ненавмисного мережевого впливу. Коли виявляється потенційна проблема, Amazon Inspector генерує детальний звіт про виявлену вразливість або ризик. Ці дані можна легко керувати через консоль Amazon Inspector або API, що надає фахівцям інструменти для ефективного та

проактивного вирішення ризиків безпеки.

На основі досліджень проведених в роботі запропоновано порядок застосування технології управління вразливостями хмарних корпоративних ресурсів. Розроблено рекомендації фахівцям з кібербезпеки щодо управління вразливостями хмарних корпоративних ресурсів.

Отже, в умовах постійного зростання кіберзагроз та витоків даних, управління вразливостями хмари є життєво важливою практикою для захисту корпоративного хмарного середовища. Розуміючи поширені вразливості хмари, впроваджуючи ефективні стратегії пом’якшення наслідків та дотримуючись найкращих практик, можна значно знизити ризик інцидентів безпеки. Використання автоматизації та правильних інструментів може оптимізувати процес управління вразливостями, зробивши його керованим та економічно ефективним. Регулярне сканування вразливостей, оцінка ризиків та усунення наслідків мають вирішальне значення для підтримки цілісності та безпеки хмарних корпоративних ресурсів. Завдяки надійній програмі управління вразливостями хмарних корпоративних ресурсів ми можемо впевнено використовувати переваги хмарних технологій, зберігаючи при цьому безпеку корпоративних даних та активів.

ПЕРЕЛІК ПОСИЛАНЬ

1. 2025 State of Cloud Security Report. Cybersecurity Insiders. URL: https://www.securenetworkhub.com/sites/securenetworkhub/files/2025-Cloud-Security-Report-Fortinet.pdf

2. Cloud Security is a Shared Responsibility. Check Point. URL: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/

3. Top 11 Cloud Security Vulnerabilities and How to Fix Them. Wiz Experts Team, August 12, 2025. URL: https://www.wiz.io/academy/common-cloud-vulnerabilities

4. Ron Reiter. Cloud Vulnerability Management Best Practices for 2025. November 26, 2024. Sentra. URL: https://www.sentra.io/learn/cloud-vulnerability-management

5. Amazon Inspector: A Guide to AWS Vulnerability Management. Cloudchipr, November 26, 2024. URL: https://cloudchipr.com/blog/amazon-inspector

6. What Is Cloud Vulnerability Management (CVM)? Check Point Software Technologies Ltd. URL: https://www.checkpoint.com/fr/cyber-hub/threat-prevention/what-is-threat-detection-and-response-tdr/what-is-cloud-vulnerability-management-cvm/#:~:text=What%20Is%20Cloud%20Vulnerability%20Management%20(CVM)?%20Cloud,sensitive%20data%2C%20maintain%20compliance%2C%20and%20minimize%20risks

7. Most Common Cloud Security Threats. Darktrace. URL: https://www.darktrace.com/cyber-ai-glossary/the-most-common-cloud-security-threats

8. Cloud Vulnerability Management: Process, Best Practices & Benefits. Oct 15, 2025 by OPSWAT. URL: https://www.opswat.com/blog/cloud-vulnerability-management-process-best-practices-benefits

9. 2025 State Of Cloud Security Report. ORCA. URL: https://orca.security/wp-content/uploads/2025/06/2025-State-of-Cloud-Security-Report-v2.pdf

10. Neeraja Hariharasubramanian. Cloud Security. Breaking Down Cloud

Vulnerability Management: Top Strategies. March 19, 2025. URL: https://fidelissecurity.com/cybersecurity-101/cloud-security/cloud-vulnerability-management/

11. What is Microsoft Defender for Cloud? 10/15/2025. URL: https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction

12. Google Cloud Security Scanner. Last Updated: 23 Jul, 2025. URL: https://www.geeksforgeeks.org/devops/google-cloud-security-scanner/

13. Amazon Inspector. User Guide. URL: https://docs.aws.amazon.com/inspector/latest/user/what-is-inspector.html

14. Norma Caro. An introduction to AWS Inspector for EC2 vulnerability scanning. Medium, Feb 23, 2024. URL: https://medium.com/@nvcaro/an-introduction-to-aws-inspector-for-ec2-vulnerability-scanning-e34b81041f66

15. Гончаренко Радомир Сергійович. Технологія управління вразливостями хмарних корпоративних ресурсів на основі Amazon Inspector. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». 29 жовтня 2025 року. Державний університет інформаційно-комунікаційних технологій, м. Київ. Тези доповідей. С. 110-112. URL: https://duikt.edu.ua/uploads/p_2779_58326207.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)