# РЕФЕРАТ

Текстова частина магістерської роботи: 58 сторінок, 57 рисунки, 15 джерела.

*Об'єкт дослідження* – виявлення та реагування на загрози в хмарному середовищі підприємства.

*Предмет дослідження* – технологія виявлення та реагування на загрози в хмарному середовищі підприємства Amazon GuardDuty.

*Мета роботи* – запропонувати технологію виявлення та реагування на загрози в хмарному середовищі підприємства та рекомендації щодо її застосування.

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

В роботі визначено концепцію хмари, її призначення та функції; проаналізовані сучасні загрози в хмарі та підходи щодо їх виявлення та реагування.

Проаналізовано ринок рішень хмарних технологій та існуючі рішення щодо виявлення та реагування на сучасні загрози в хмарі.

Розглянуто основні сервіси AWS та їх призначення.

Визначено призначення, основні функції та місце в архітектурі AWS рішення GuardDuty.

Проведено експерименти для дослідження можливостей Amazon GuardDuty.

На основі функціональних особливостей Amazon GuardDuty, а також результатів експериментів, розроблено загальні рекомендації щодо виявлення та реагування на загрози в хмарному середовищі підприємства.

Галузь використання – кібербезпека хмарного середовища підприємства.

ІНФОРМАЦІЙНА СИСТЕМА ПІДПРИЄМСТВА, ХМАРНЕ СЕРЕДОВИЩЕ, СУЧАСНІ ЗАГРОЗИ, ХМАРА, КІБЕРБЕЗПЕКА, ЗАХИСТ ХМАРИ, ЗАСОБИ ВИЯВЛЕННЯ, ХМАРНА ІНФРАСТРУКТУРА, ЗАСОБИ РЕАГУВАННЯ.

# ABSTRACT

Master’s thesis: 72 pages, 57 figures, 15 sources.

*Object of research* – detection and response to threats in the cloud environment of the enterprise.

*Subject of research* – Amazon GuardDuty enterprise cloud-based threat detection and response technology.

*The aim of research* – to propose a technology for detecting and responding to threats in the enterprise cloud environment and recommendations for its application.

*Research methods* – elaboration of literature on the topic, analysis of operational documentation, international standards and their comparison, conducting experiments.

The paper defines the concept of the cloud, its purpose and functions; analyzed modern threats in the cloud and approaches to their detection and response.

The market for cloud technology solutions and existing solutions for detecting and responding to modern threats in the cloud are analyzed.

The main AWS services and their purpose are considered.

The purpose, main functions and place in the AWS architecture of the GuardDuty solution are defined.

Experiments were conducted to explore the capabilities of Amazon GuardDuty.

Based on the functional features of Amazon GuardDuty, as well as the results of experiments, general recommendations for detecting and responding to threats in the cloud environment of the enterprise have been developed.

Field of use – cyber security of the cloud environment of the enterprise.

ENTERPRISE INFORMATION SYSTEM, CLOUD ENVIRONMENT, MODERN THREATS, CLOUD, CYBER SECURITY, CLOUD PROTECTION, DETECTION TOOLS, CLOUD INFRASTRUCTURE, RESPONSE TOOLS.

**ЗМІСТ**

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – Програмне Забезпечення

ЦОД – Центр Обробки Даних

ІТ – Інформаційні Технології

CSP – Постачальник Хмарних Послуг (англ. Cloud Service Provider)

БД – База Даних

API – Програмний Інтерфейс Застосунку (англ. Application Programming Interface)

# ВСТУП

*Актуальність дослідження.* Перехід до хмарних обчислень стрімко прискорився в останні роки, і будь-якого уповільнення не очікується. Підприємства та організації переміщують свою інфраструктуру, включаючи критично важливі системи, з-під свого прямого контролю на платформи, які надаються та підтримуються постачальниками хмарних послуг (CSP). Розглядаючи цінність даних, які обробляються та зберігаються в хмарі, можна сказати, що це крок, який міг би здатися неможливим або дуже малоймовірним ще декілька років тому.

Після десятиліть зведення стін навколо інфраструктури, щоб запобігти НСД до даних та інтелектуальної власності, підприємства та організації «руйнують» їх та масово переносять свої дані у системи, над якими вони практично не мають прямого контролю. Першою причиною тому є надзвичайна гнучкість у структурі та вартості.

Друга причина ярко проявила себе в період, коли працівникам був необхідний доступ до критично важливих систем, поки вони не мали змоги бути в офісі (пандемія COVID-19). Певний час підприємства та організації використовували віртуальні приватні мережі (VPN) для доступу до внутрішніх ресурсів, проте з поширенням хмарних сервісів необхідність в них відпала, адже необхідна інфраструктура розміщується за межами внутрішньої мережі, тому до неї можна отримати доступ з будь-якої точки світу.

*Об'єкт дослідження* – виявлення та реагування на загрози в хмарному середовищі підприємства.

*Предмет дослідження* – технологія виявлення та реагування на загрози в хмарному середовищі підприємства Amazon GuardDuty.

*Мета роботи* – запропонувати технологію виявлення та реагування на загрози в хмарному середовищі підприємства та рекомендації щодо її застосування.

*Завдання магістерської роботи:*

визначити концепцію хмари, її призначення та функції; проаналізувати сучасні загрози в хмарі та підходи щодо їх виявлення та реагування;

проаналізувати ринок рішень хмарних технологій та існуючі рішення щодо виявлення та реагування на сучасні загрози в хмарі;

розглянути основні сервіси AWS та їх призначення;

дослідити сервіс Amazon GuardDuty;

провести експерименти для дослідження можливостей Amazon GuardDuty;

на основі функціональних особливостей Amazon GuardDuty, а також результатів експериментів, розроблено загальні рекомендації щодо виявлення та реагування на загрози в хмарному середовищі підприємства.

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

*Практичне значення одержаних результатів:* рекомендації щодо впровадження та використання сервісу Amazon GuardDuty в хмарному середовищі підприємства.

Результати роботи апробовані на Всеукраїнській науково-практичній конференції «АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ» від 27.10.2022.

# 1 АНАЛІЗ ПРОБЛЕМ ЩОДО ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА СУЧАСНІ ЗАГРОЗИ В ХМАРІ

## 1.1. Визначення, призначення та функції хмари

Що таке хмарна інфраструктура?

Закон України «Про хмарні послуги» [1] визначає цей термін наступним чином:

Хмарна інфраструктура (далі, хмара) – сукупність динамічно розподілюваних та налаштовуваних хмарних ресурсів, що можуть бути оперативно надані користувачу хмарних послуг і вивільнені через глобальну та локальні мережі передачі даних.

При цьому Національний Інститут Стандартів і Технологій (NIST) [2] визначає хмару як технологію, яка забезпечує всюдисущий, зручний мережевий доступ за вимогою до спільного пулу ресурсів, до яких CSP може надати або відняти доступ з мінімальними зусиллями щодо керування. Хмара має 5 основних характеристик (Рис. 1.1.), 3 основні моделі обслуговування (Рис. 1.2.) і 4 моделі розгортання (Рис. 1.3.).

*Основні характеристики:*

Самообслуговування. Користувач може в односторонньому порядку отримати обчислювальні можливості, такі як серверний час і мережеве сховище, автоматично і за потребою, не вимагаючи взаємодії людини постачальником послуг;

Широкий доступ до мережі. Ресурси доступні через мережу та доступ до них здійснюється через стандартні механізми, які сприяють використанню різнорідними тонкими або товстими клієнтськими платформами (наприклад, мобільними телефонами, планшетами, ноутбуками та робочими станціями);

Пул ресурсів. Обчислювальні ресурси постачальника об’єднуються для обслуговування кількох споживачів за допомогою моделі з кількома клієнтами,

причому різні фізичні та віртуальні ресурси динамічно призначаються та перепризначаються відповідно до попиту споживачів. Існує відчуття незалежності розташування, оскільки клієнт зазвичай не контролює чи не знає точного розташування наданих ресурсів, але може вказати розташування на вищому рівні абстракції (наприклад, країна, штат або центр обробки даних). Приклади ресурсів включають зберігання, обробку, пам'ять і пропускну здатність мережі;

Швидка еластичність. Ресурси можна отримувати та звільняти досить вільно, гнучко, у деяких випадках автоматично, для швидкого масштабування назовні та всередину, в залежності від попиту. Для клієнта необхідні ресурси часто здаються без обмежень і можуть бути використані в будь-якій кількості в будь-який час;

Розмірене обслуговування. Хмарні системи автоматично контролюють і оптимізують використання ресурсів, використовуючи можливості вимірювання на певному рівні абстракції, що відповідає типу послуги (наприклад, зберігання, обробка, пропускна здатність і активні облікові записи користувачів). Використання ресурсів можна відстежувати, контролювати та отримувати звіти, забезпечуючи прозорість як для постачальника, так і для споживача використовуваної послуги.

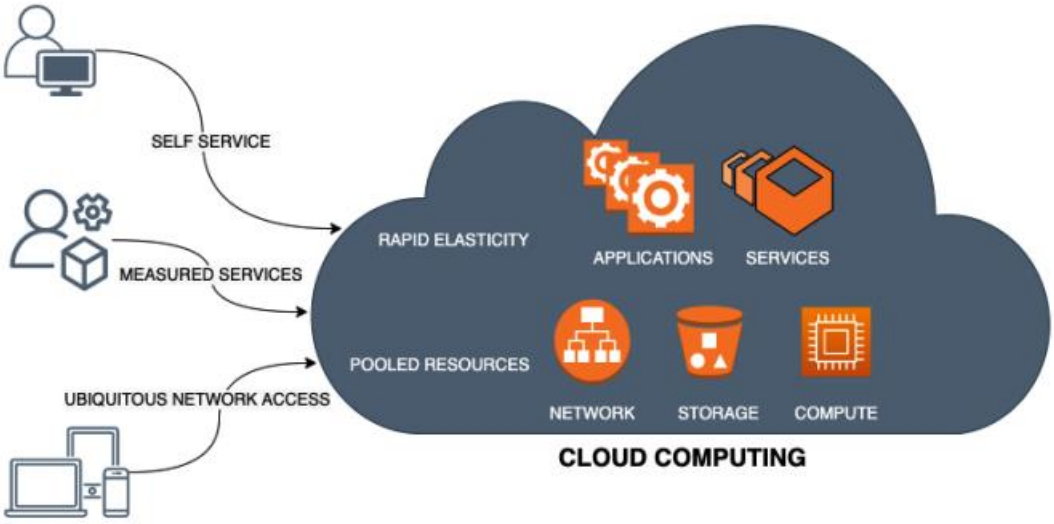



Рис. 1.1. Ключові елементи хмарних обчислень [3]

*Основні моделі обслуговування:*

Програмне Забезпечення як Сервіс (SaaS). Послуга, яка надається користувачу, полягає у використанні застосунків постачальника, які працюють у хмарі. Застосунки доступні з різних клієнтських пристроїв або через клієнтський інтерфейс, наприклад веб-браузер, або інтерфейс застосунку. Користувач не керує хмарною інфраструктурою, яка лежить в основі цього застосунку, включаючи мережу, сервери, операційні системи, сховище або навіть окремі можливості та функції, за винятком обмежених параметрів конфігурації застосунку, призначених для користувача;

Платформа як Сервіс (PaaS). Послуга, яка надається користувачу, полягає в розгортанні в хмарі створених або придбаних клієнтом застосунків, створених за допомогою мов програмування, бібліотек, служб та інструментів, які підтримуються постачальником. Користувач не керує хмарною інфраструктурою, яка лежить в основі цього застосунку, включаючи мережу, сервери, операційні системи та сховище, але контролює розгорнуті застосунки та, можливо, параметрами конфігурації для середовища їх розміщення;

Інфраструктура як Сервіс (IaaS). Послуга, яка надається користувачу, полягає в забезпеченні обробки, зберігання, маршрутизації та інших фундаментальних обчислювальних ресурсів, де клієнт може розгортати та запускати довільне ПЗ, яке може включати операційні системи та застосунки. Споживач не керує та не контролює базу хмарної інфраструктури, але має контроль над операційними системами, сховищами та розгорнутими застосунками; і, можливо, обмежений контроль окремих мережевих компонентів (наприклад, брандмауери хоста).

*Моделі розгортання:*

Приватна хмара. Хмарна інфраструктура надається для ексклюзивного використання одним підприємством чи організацією, що складається з кількох споживачів (наприклад, бізнес-підрозділів). Він може належати, управлятися та експлуатуватися власне організацією, третьою стороною або їх комбінацією, і він може існувати на території підприємства або за її межами.

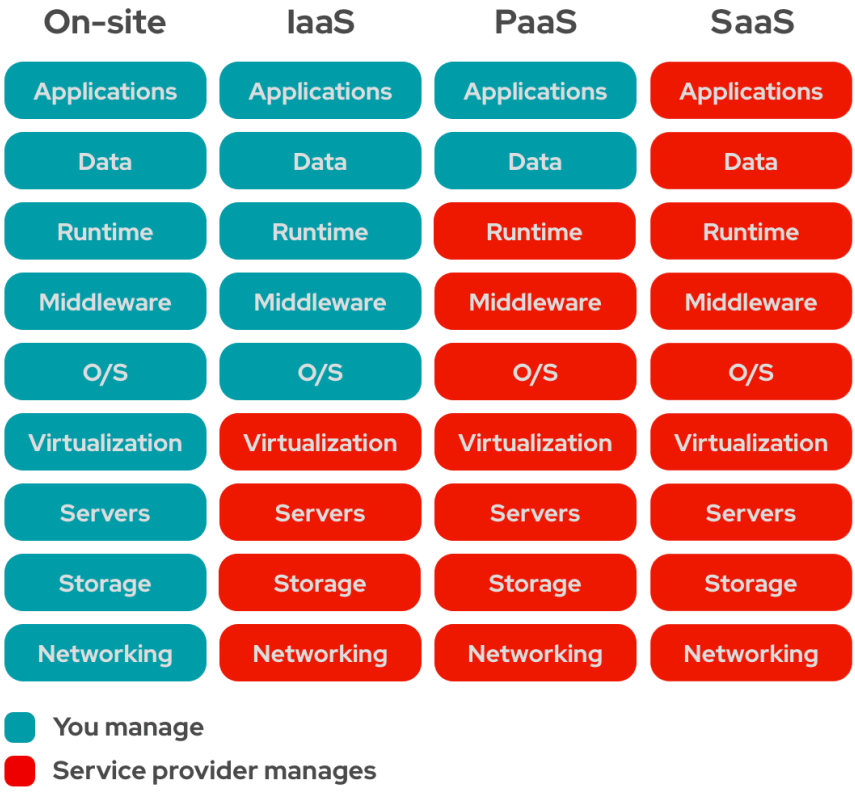



Рис. 1.2. Основні моделі обслуговування хмарних обчислень

Суспільна хмара. Хмарна інфраструктура надається для ексклюзивного використання певною групою споживачів (організацій, підприємств тощо), які мають спільні інтереси (наприклад, місія, вимоги безпеки, політика і т.п.). Вона може належати, управлятися та експлуатуватися однією або декількома організаціями в спільноті, третьою стороною або їх комбінацією, і вона може існувати на території підприємства або за її межами.

Публічна хмара. Хмарна інфраструктура надається для відкритого використання широким загалом користувачів. Вона може належати, управлятися та експлуатуватися компанією (бізнес), навчальним закладом чи державною організацією або деякою їх комбінацією. Вона розташована на території CSP.

Гібридна хмара. Цей тип хмарної інфраструктури – це композиція з двох різних хмарних інфраструктур (приватних і суспільних або публічних), які залишаються унікальними відносно одного об’єктами, але пов’язані між собою стандартизованою або запатентованою технологією, яка забезпечує переносимість даних і застосунків (наприклад, балансування навантаження між хмари).

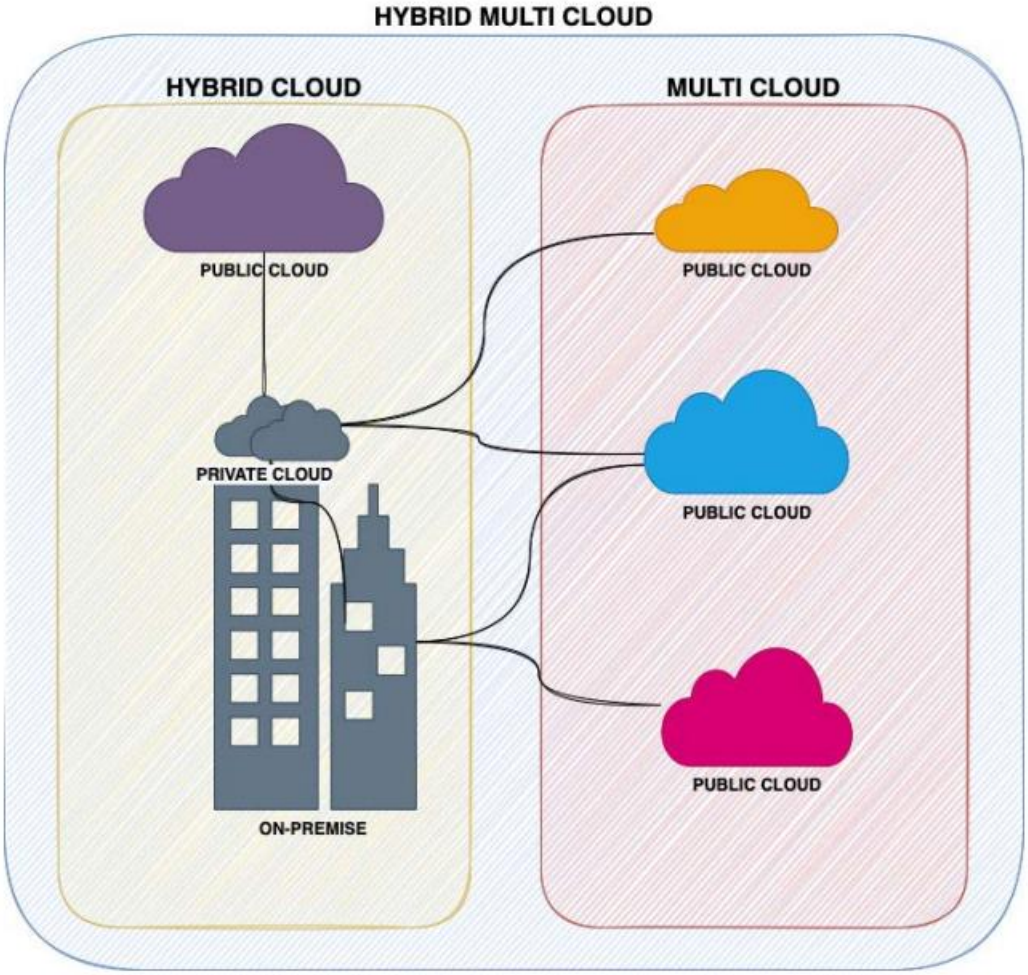



Рис. 1.3. Моделі розгортання хмарних обчислень [3]

Також існують мультихмарна та гібридна мультихмарна моделі, які комбінують в собі основні моделі обслуговування.

## 1.2. Аналіз сучасних загроз в хмарі

На сьогодні, всі підприємства та організації використовують хмарні технології в тому чи іншому вигляді. Але незалежно від того, яку модель надання послуг (SaaS, IaaS або PaaS) використовує підприємство, кіберзагрози є спільним аспектом хмари, до якого приділяється дуже багато уваги.

Не дивлячись на різноманіття сервісів та інструментів, призначенням яких і є боротьба з кіберзагрозами, кількість інцидентів хмарної безпеки тільки росте. За даними цьогорічного звіту від Check Point щодо хмарної безпеки [4] близько 27%

організацій зіштовхнулись з порушеннями безпеки – ріст на 10% у порівнянні з попереднім роком. Найчастішими інцидентами стали: неправильні налаштування (акаунтів, серверів тощо), скомпрометовані (або викрадені) акаунти, використання вразливостей, неналежна передача даних, зараження ресурсів шкідливим програмним забезпеченням (далі ШПЗ), завантаження даних на небезпечний пристрій (Рис. 1.4.). Існують й інші загрози для хмарної інфраструктури [5]: НСД, інсайдери, кібератаки та DDoS атаки, витік даних тощо.

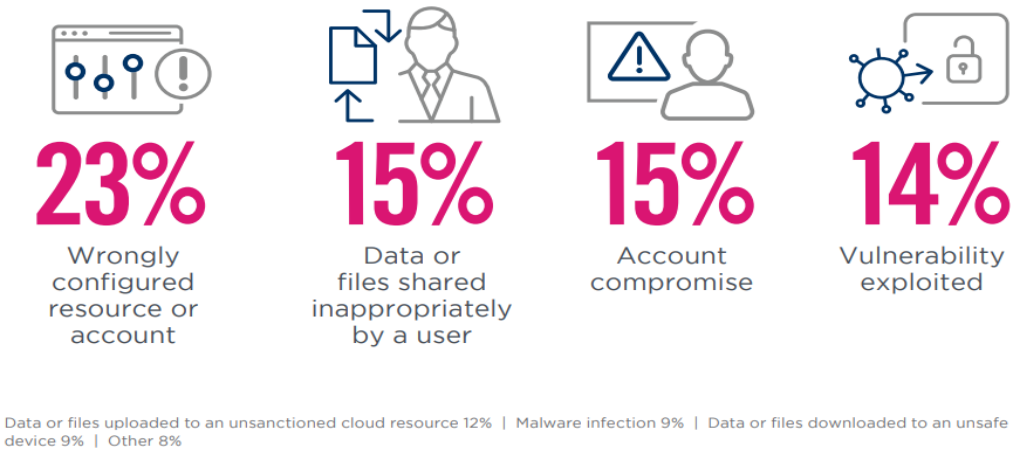



Рис. 1.4. Найчастіші інциденти порушень безпеки в хмарі

Ще одним фактором, який може призвести до реалізації загроз є відсутність видимості та відстеження (visibility and tracking) ресурсів в хмарі. У моделі IaaS хмарні постачальники мають повний контроль над інфраструктурним рівнем і не розкривають його своїм клієнтам. Відсутність видимості та контролю ще більше поширена в PaaS і SaaS. Клієнти часто не можуть ефективно ідентифікувати та кількісно оцінити свої хмарні активи або візуалізувати своє хмарне середовище [6]. Як наслідок, багато традиційних інструментів для досягнення видимості мережі неефективні для хмарних середовищ, а деяким організаціям бракує інструментів безпеки, орієнтованих на хмару. Це обмежує здатність організації відстежувати свої хмарні ресурси та захищати їх від атак.

Сказане вище, а також найбільша популярність саме публічних хмар, призводить до того, що професіонали з кібербезпеки мають серйозні побоювання щодо безпеки даних, що зберігаються та обробляються в хмарі [4]. В 2022 році 95% організацій були стурбовані безпекою в хмарі:

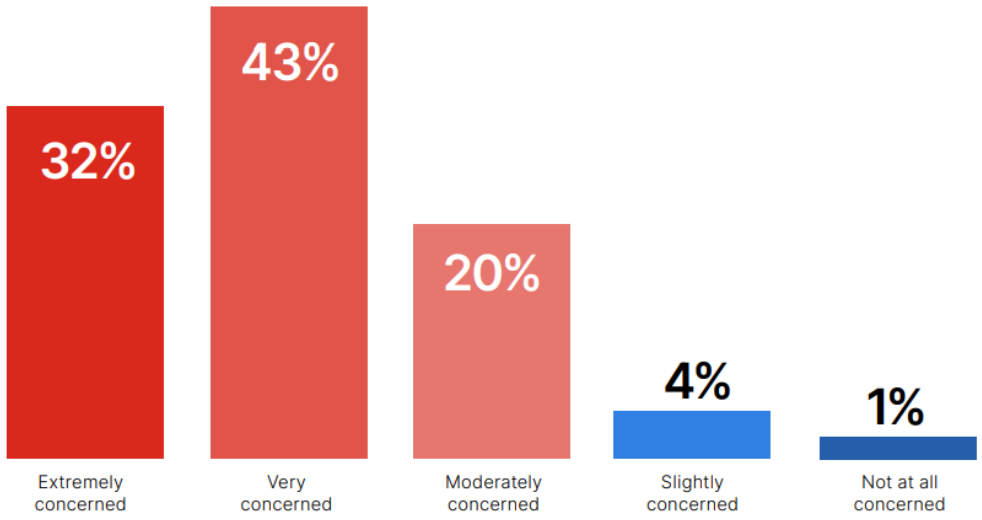



Рис. 1.5. Рівень стурбованості організацій безпекою в публічних хмарах

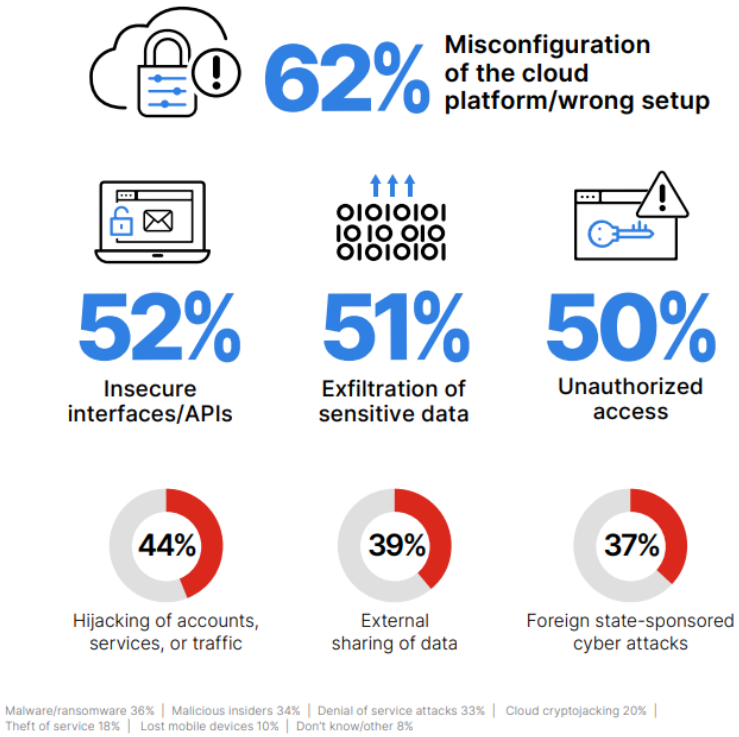



Рис. 1.6. Найбільші загрози в публічній хмарі на думку спеціалістів [4]

На питання «Які, на Вашу думку, найбільші загрози в публічній хмарі?» відповіді були різноманітними, але більшу частину спеціалістів турбує: ризик невірної конфігурації в хмарі, небезпечні/незахищені інтерфейси, витік чутливих даних та НСД (Рис. 1.6.).

## 1.3. Дослідження проблем та аналіз підходів щодо виявлення сучасних загроз в хмарі

Виявлення загроз – це практика аналізу всієї системи для виявлення будь-якої зловмисної діяльності, яка може скомпрометувати мережу або ресурси. Якщо загрозу виявлено, необхідно вжити заходів для її пом'якшення, щоб належним чином нейтралізувати загрозу, перш ніж вона зможе використати будь-яку наявну вразливість.

Порушення безпеки – сценарій, якому більшість організацій мають віддавати пріоритет, залучати розумних людей і технології, щоб працювати як захисний бар'єр проти будь-кого, хто може спробувати створити проблеми. Але безпека – це постійний процес, а не гарантія.

У контексті безпеки хмарної інфраструктури організації поняття «виявлення загрози» є багатогранним. Навіть найкращі сервіси безпеки можуть щось «упустити», працюючи поодинці.

Коли справа доходить до виявлення та подолання загроз, швидкість має вирішальне значення. Служби повинні бути в змозі швидко й ефективно виявляти загрози, щоб зловмисники не мали достатньо часу для пошуку конфіденційних або критично-важливих даних. Зазвичай служби можуть зупинити більшість загроз, оскільки вони були помічені раніше, тож вони знають, як з ними боротися. Ці загрози вважаються «відомими». Однак існують й «невідомі» загрози, які організація прагне виявити. Це ті загрози, які використовують методи та вразливості, з якими ще ніхто не стикався.

Відомі загрози іноді можуть пройти повз навіть найкращі засоби захисту, тому більшість організацій активно шукають як відомі, так і невідомі загрози у своєму середовищі. Отже, як організація може спробувати виявити як відомі, так і невідомі загрози?

В арсеналі захисника є кілька способів, які можуть допомогти [7]:

*Аналіз загроз*

Аналіз загроз – це спосіб перегляду сигнатурних даних раніше помічених

атак і порівняння їх із корпоративними даними для виявлення загроз. Це робить його особливо ефективним у виявленні відомих загроз, але не невідомих. Інтелектуальні дані про загрози часто використовуються з великою ефективністю в технологіях безпеки та керування подіями (SIEM), антивірусі, системі виявлення вторгнень (IDS) і веб-проксі.

*Аналіз поведінки користувачів і зловмисників*

За допомогою аналітики поведінки користувачів організація може отримати базове розуміння того, якою буде нормальна поведінка співробітника: наприклад, до яких даних вони мають доступ, коли вони входять у систему тощо. Таким чином, раптова зміна поведінки, як-от вхід о 2 годині ночі в Шанхаї від людини, яка зазвичай працює з 9 до 5 у Нью-Йорку й не подорожує у справах, виділяється як незвичайна поведінка та те, що необхідно розслідувати якнайшвидше.

З аналітикою поведінки зловмисників складніше: він не має «базової» активності, з якою можна порівняти інформацію; натомість невеликі, здавалося б, непов’язані дії, виявлені в мережі з часом, насправді можуть бути навігаційними крихтами активності, які зловмисник залишає позаду. Щоб поєднати ці частини, потрібні технологія та інтелект, щоб сформувати картину того, що може задумати зловмисник у мережі організації.

*Встановлення пасток для порушників*

Деякі цілі надто спокусливі для зловмисника, щоб їх пропустити. Команди безпеки знають про це, тому вони розставляють пастки в надії, що зловмисник захопить наживку. У контексті мережі організації пастка для зловмисників може включати honeypot, яка, на перший погляд, містить мережеві служби, особливо привабливі для зловмисника, або облікові дані, які мають привілеї користувача, необхідні зловмиснику для отримання доступу до чутливих систем або даних. Коли зловмисник знаходить цю приманку, команді безпеки приходить сповіщення, що в мережі є підозріла активність, яку слід дослідити.

*Виявлення загроз вимагає двостороннього підходу*

Виявлення загроз потребує як людського, так і технічного компонентів. Людський елемент включає аналітиків безпеки, які аналізують тенденції,

закономірності в даних, поведінку та звіти, а також тих, хто може визначити, чи вказують аномальні дані на потенційну загрозу чи на помилкову тривогу.

Але технологія виявлення загроз також відіграє ключову роль у процесі виявлення. У процесі виявлення загроз немає єдиного рішення, який би впорався із завданням. Натомість комбінація інструментів, що діє по всій інфраструктурі організації, від кінця до кінця, намагаючись зафіксувати загрози, багатократно підвищують вірогідність вдалого виявлення.

Надійна система для виявлення загроз повинна використовувати:

- Технологію виявлення загроз безпеки для збирання даних про події в мережі, включаючи автентифікацію, доступ до мережі та журнали з критичних систем;
- Технологію виявлення мережевих загроз для розуміння моделей трафіку в мережі та моніторингу трафіку всередині мереж і між ними, а також до Інтернету;
- Технологію виявлення загроз на віртуальних машинах, в БД тощо для надання детальної інформації про ймовірні зловмисні події, а також будь-якої поведінкової чи криміналістичної інформації для допомоги у розслідуванні загроз.

Застосовуючи комбінацію цих методів захисту, користувач хмарних обчислень збільшує свої шанси на швидке та ефективне виявлення та пом’якшення загрози. Безпека – це безперервний процес, де нічого не гарантовано. Від користувача, ресурсів і процесів, які він використовує, залежатимете, чи буде підприємство «у безпеці».

## 1.4. Аналіз ринку та огляд існуючих рішень хмарних технологій щодо виявлення та реагування на сучасні загрози в хмарі

В жовтні 2022 року Gartner – дослідницька та консалтингова компанія, що спеціалізується на ринках інформаційних технологій, випустила звіт [8] типу «Магічний квадрант» для вендорів хмарної інфраструктури та сервісних платформ.


Рис. 1.7. Магічний квадрант для Хмарної Інфраструктури та Сервісних Платформ

Компанія Gartner визначає ринок Хмарної Інфраструктури та Сервісних Платформ (далі, CIPS) як стандартизовані, високоавтоматизовані пропозиції, у яких хмарні ресурси доповнюються інтегрованими сервісами платформи. До них входять керовані застосунки, бази даних і функції як послуга. Ресурси масштабовані та еластичні в реальному часі та оплачуються лише за фактом

використання. Інтерфейси самообслуговування, включаючи веб-інтерфейс користувача (UI) і API, доступні безпосередньо клієнту. Ресурси можуть розміщуватися постачальником або локально в ЦОД клієнта.

Сфера дії Магічного квадранта для CIPS включає пропозиції IaaS та PaaS. До них відносяться PaaS для додатків (aPaaS), функції як сервіс (FaaS), PaaS для баз даних (dbPaaS), PaaS для розробників додатків (adPaaS) і промислові розподілені хмарні пропозиції, які часто розгортаються в корпоративних ЦОД.

З минулого року Лідери та їх розташування відносно одне одного не змінились: Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP) залишили за собою місця найкращих вендорів на ринку (Рис. 1.7.). Їх частка на ринку хмарних послуг, за даними Synergy Research Group [9], показує такий же результат:

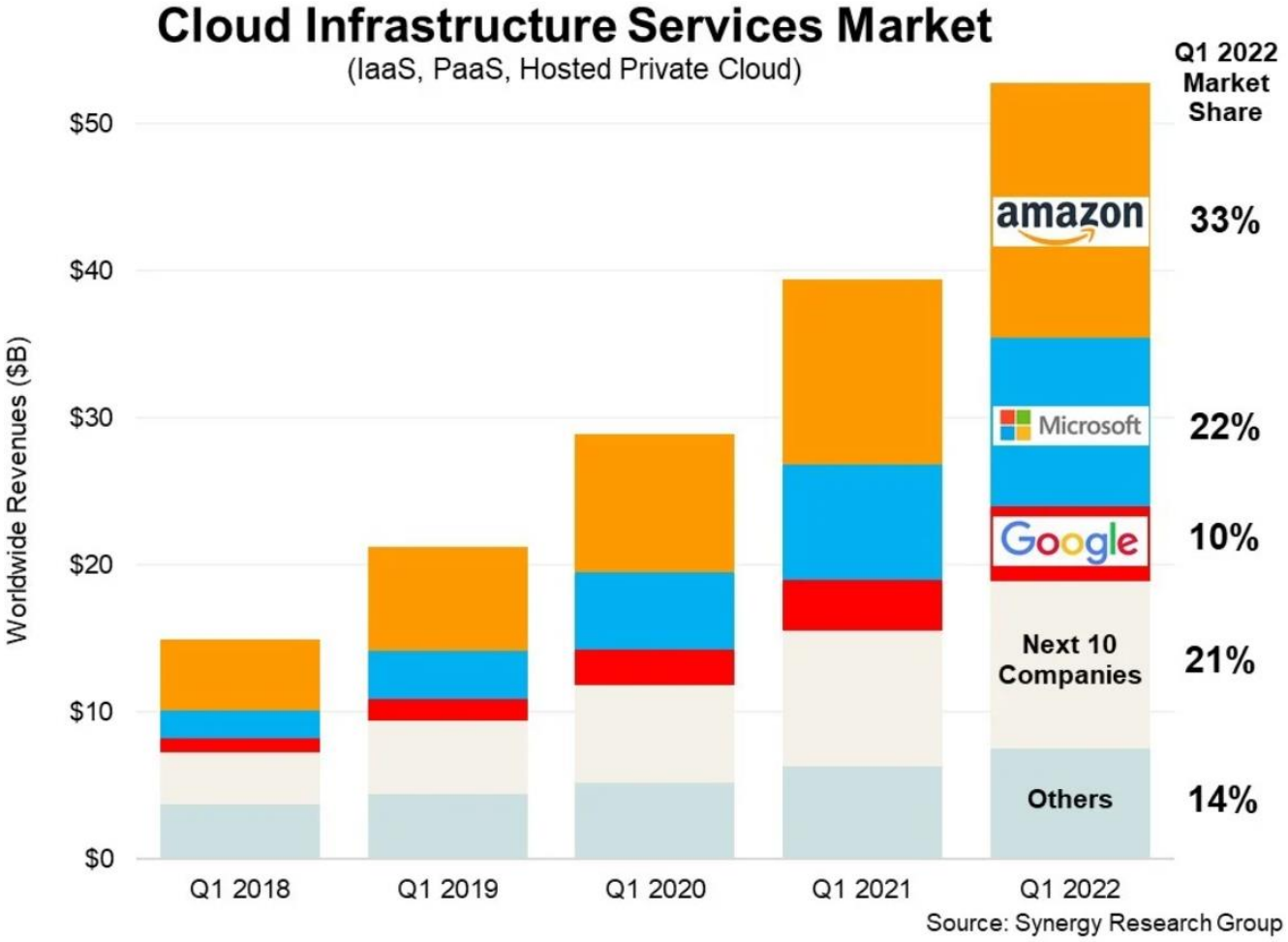



Рис. 1.8. Ринок постачальників хмарних послуг

*AWS*

Amazon Web Services, дочірня компанія Amazon, є абсолютним лідером у цьогорічному Магічному квадранті. AWS зосереджена на тому, щоб бути постачальником широкого спектру IT-послуг, починаючи від хмарних і граничних до ERP і критично важливих обчислень.

AWS планує розширити розміри ринку, який вона займає, через партнерства з телекомунікаційними компаніями, а також розширення доступних послух та служб (наприклад, приватні 5G мережі). Діяльність AWS за характером є глобальною. Його клієнти мають різні профілі, розміри, галузі та регіони.

Сильні сторони:

*Широта функціональних можливостей*: AWS продовжує мати найбільшу широту та глибину можливостей серед усіх вендорів на ринку CIPS. AWS служить рушійною силою на ринку в цілому, встановлюючи прийняті стандарти, розробляючи технології та впроваджуючи методології, які часто повністю копіюються конкуруючими вендорами хмарних послуг. Часто хмарні провайдери намагаються копіювати AWS, проте їм зазвичай не вистачає даних, аргументації та сприйняття клієнтами, які AWS використовує для підтримки своєї пропозиції.

*Поточна лідерська частка ринку:* Доходи AWS робить його поточним лідером за часткою ринку на ринку CIPS, перевищуючи Microsoft Azure, свого найближчого конкурента, майже в два рази. Крім того, AWS є одним із небагатьох вендорів на цьому ринку, який не перебільшує свою бізнес-ефективність для клієнтів на основі продажу пропозицій, які знаходяться далеко за межами того, що розумно вважається хмарним. Прикладами такого стороннього доповнення іншими вендорами включають продаж ліцензій на операційні системи та бази даних інших хмарних провайдерів, а також локально-розгорнуті платформи PaaS, які складають значну частину «хмарного» доходу.

*Жвава та процвітаюча екосистема*: AWS є магнітом для партнерів екосистеми, враховуючи її частку ринку та момент імпульсу. Партнери-незалежні постачальники ПЗ часто мають пріоритет «спочатку AWS» щодо того, яких хмарних постачальників підтримувати спочатку. Прикладами є SAP, Splunk і

VMware.

Застереження:

*Ерозія відносин з клієнтами*: Аналіз запитів клієнтів, що провела Gartner, показує, що AWS часто оптимізує роботу з клієнтами на короткий термін, особливо під час поновлення контракту, що призводить до погіршення відносин із клієнтами. Це, разом зі змінами виконавчого керівництва, зміною пріоритетності клієнтів, привілейованням провайдерів у різних регіонах і сильною конкуренцією, малює складну картину для AWS у майбутньому.

*Мультихмарна і суверенна стратегія*: AWS, провідний вендор на цьому ринку за часткою ринку, має відносно слабку стратегію підтримки клієнтів, які шукають суверенні та мультихмарні рішення. AWS не проявляє зацікавленості в реалізації значущих мультихмарних стратегій для своїх клієнтів, незважаючи на те, що багато клієнтів користуються послугами й інших хмарних провайдерів. Крім того, AWS має досить невпевнений підхід до суверенних хмар у Європі, де її конкуренти проявляють більше ініціативи.

*Регіональні залежності та зв'язок*: Операційний інцидент AWS 7 грудня 2021 року виявив деякі мультирегіональні залежності від внутрішньої мережі AWS, яка розміщена в us-east-1. Оскільки us-east-1 також розміщує службу підтримки для Північної Америки, у клієнтів AWS також виникли труднощі зі зв’язком із технічною підтримкою під час інциденту. Це призвело до того, що AWS не змогла підтримувати зв'язок з клієнтами в адекватних часових рамках, а вражаюче неточні звіти Health Dashboard призвели до відсутності розуміння у клієнтів всієї ситуації щодо збоїв.

Для постійного моніторингу та виявлення загроз AWS пропонує тандем з Amazon GuardDuty та AWS Security Hub.

*Google*

Google одним із лідерів у цьому Магічному квадранті. Google Cloud Platform (GCP) це потужна хмарна платформа майже в усіх випадках використання та досягла значного прогресу в покращенні своїх граничних можливостей. Google

продовжує інвестувати в те, щоб стати постачальником IaaS і PaaS з широким спектром можливостей. Його операції географічно диверсифіковані, а його клієнтами є як стартапи, так і великі підприємства.

Сильні сторони:

*Збільшення доходів і можливостей*: Серед усіх хмарних провайдерів на цьому ринку GCP мав як найвищий відсоток прибутку, так і покращення відносно методу визначення критичних можливостей від Gartner для CIPS. Це, значною мірою, результат збільшення продажів на місцях, спільного продажу з партнерами та прагнення пропонувати конкурентоспроможну платформу з точки зору можливостей.

*Виконання продажів*: Послідовна орієнтація GCP на підприємства та перехід до продажу керівникам компаній (а не технічним командам) дали дуже помітні результати як з точки зору впровадження, так і сприйняття в підприємстві. Це сильно контрастує з ситуацією кількох років тому, коли більшість підприємств навряд чи розглядали б Google як вендора корпоративних IT-рішень.

*Суверенна хмара*: GCP має більш гнучку партнерську позицію за межами своїх основних регіонів. Він готовий співпрацювати з операторами в країні для створення суверенних хмарних альтернатив у ключових регіонах і співпрацювати з постачальниками OBO (оригінальний виробник обладнання) для розгортання Google Anthos у приватних центрах обробки даних і граничних місцях.

Застереження:

*Підвищення цін*: Історично Google приваблювала клієнтів агресивним ціноутворенням у порівнянні з конкурентами, але клієнтам слід приготуватись, що ціни не будуть залишатися низькими вічно. Наприклад, Google нещодавно підвищив ціни на 100% на деякі аспекти своїх послуг хмарного сховища. Хоча Google виконує наявні зобов’язання перед клієнтами, цей випадок став першим значним підвищенням ціни вендором на цьому ринку.

*Стратегічна плутанина*: Хоча Google підтримує програми підтримки клієнтів як для своєї Програми швидкої оцінки та міграції (RAMP), так і для Програми модернізації хмарних додатків (CAMP), Gartner вважає, що RAMP є

більш поширеною на ринку, і ми не часто чуємо про CAMP від клієнтів. Крім того, Google публічно рекламує 39 спеціалізованих партнерів RAMP, але не підтримує еквівалентного публічного списку партнерів CAMP.

Для моніторингу хмарної інфраструктури Google пропонує комбінацію із наступних служб виявлення загроз: Container Threat Detection, Event Threat Detection, Virtual Machine Threat Detection, Rapid Vulnerability Detection. Проте ці служби працюють лише при використанні Security Command Center преміального рівня.

*Microsoft*

Microsoft є одним із лідерів в цьому Магічному квадранті. Microsoft Azure є сильним у всіх варіантах використання, включаючи розширені хмарні та граничні обчислення. Azure особливо добре підходить для організацій, орієнтованих на Microsoft. Корпорація Microsoft зосереджена на інвестиціях у гібридні та мультихмарні технології, а також покращеннях в архітектурі та безпеці платформи Azure. ЇЇ операції географічно диверсифіковані, а її клієнтами, як правило, є середні та великі підприємства.

Сильні сторони:

*Частка ринку*: Microsoft Azure продовжує досягати прогресу з року в рік, скорочуючи розрив у частці ринку з AWS, найсильнішим конкурентом Microsoft. З нинішніми темпами Azure глобальне відставання від AWS значно скоротиться в найближчому майбутньому, і це вже відбувається в Європі.

*Орієнтованість на рішення*: Microsoft Azure має вражаючу орієнтацію на рішення з широким спектром хмарних можливостей Microsoft та екосистему, в якій Майкрософт та її партнери доповнюють одне одного, щоб задовольнити будь-які вимоги своїх клієнтів. Корпорація Майкрософт займає диференційовану позицію в широких сегментах, таких як телекомунікації, охорона здоров’я, виробництво, роздрібна торгівля та фінансові послуги.

*Гібридність та мультихмарність*: Бачення корпорацією Майкрософт щодо цього ринку ґрунтується на вірі в те, що більшість підприємств залишатимуться

гібридними та мультихмарними, і що для безпечної та ефективної роботи таких різноманітних середовищ потрібні спрощені операції та керування. Корпорація Майкрософт пропонує це за допомогою набору технологій, відомих як Azure Arc, які намагаються задовольнити ці потреби, але наразі мають низький рівень впровадження.

Застереження:

*Проблеми безпеки та відсутність інновацій*: Незважаючи на збільшення частки ринку Microsoft Azure, 2021 рік не був знаковим для Microsoft Azure, оскільки він стосується нових інновацій на ринку хмарної інфраструктури та сервісних платформи. Gartner інтерпретує це як час, який Майкрософт витрачає на проблеми надійності та безпеки, з якими стикнулися клієнти Azure після безперервного потоку інцидентів. І звичайно, що конкуренти Microsoft, такі як Google і Oracle, не стоять на місці і, швидше за все, з часом досягнуть і навіть перевищать можливості Azure за деякими параметрами.

*Непрозорі витрати*: Багато клієнтів Gartner повідомляють про розчарування, спостерігаючи, як зростають їхні витрати на Azure з часом, не знаючи причини. Критичні корпоративні функції часто доступні лише в найвищому рівні. Власні можливості Azure з управління витратами відстають від деяких конкурентів у зрілості та повноті, задовольняючи лише половину «обов'язкових» критеріїв, які Gartner використовує для оцінки можливостей керування витратами хмарних провайдерів. Крім того, партнери Microsoft CSP дуже нерівні в своїх знаннях в оптимізації витрат у хмарі і відповідних методів підтримки. Нарешті, складність витрат на ліцензування та підтримку Microsoft поширюється й на Azure: клієнтам важко консолідувати свої витрати та домовитися про приватні знижки простим і передбачуваним способом.

*Каральне ліцензування*: Microsoft планує дотримуватися принципів справедливого ліцензування програмного забезпечення. Однак Microsoft використовує ліцензування для своїх продуктів, таких як Windows і SQL Server, з метою покарання проти конкурентних хмарних провайдерів, роблячи дорожчим розгортання робочих навантажень Windows будь-де, крім Azure. Існують також

обмеження щодо використання ліцензій Microsoft у самому Azure, які часто не повідомляються клієнтам. Наприклад, клієнтам не повідомляють про обмежувальні правила в розділі «Переваги гібридного використання Azure» у багатокористувацьких середовищах Azure.

Azure пропонує вбудовані функції захисту від загроз за допомогою служб Azure Active Directory (Azure AD), Azure Monitor logs, та Microsoft Defender for Cloud.

Отже, ринок CIPS істотно змінюється, що має довгострокові наслідки для майбутнього корпоративних IT. Гіпермасштабовані постачальники хмарних послуг змагаються за колонізацію підприємств, намагаючись стати основним стратегічним постачальником хмарних послуг для вирішення широкого спектру IT-завдань.

Зусилля колонізувати підприємства суперечать прерогативам більшості підприємств «бути мультихмарними» щодо стратегій пошуку. Ще більше ускладнює ситуацію те, що «найкращий у своєму роді» підхід, який історично використовувався локально, є ненадійним у хмарі, враховуючи відмінності систем ідентифікації, характеристики стійкості, затримку мережі та загальне побоювання провідних постачальників працювати разом в інтересах клієнтів. Зрештою, мультихмарні архітектури все ще підходять лише для найдосвідченіших клієнтів, які можуть впоратися з безліччю завдань, які чекають на них.

Коли підприємства перебувають під владою хмарного постачальника, малоймовірно, що хмарний постачальник залишатиметься доброзичливим дуже довго. Кінцева мета хмарних провайдерів полягає в тому, щоб перемістити підприємства далі на рівень PaaS, де прибутки вищі, а можливість вивільняти робочі навантаження та процеси стає складнішою. Але традиційні робочі навантаження також стає важче переносити через їх критично важливий характер.

Негативні наслідки перебування під владою хмарного провайдера вже починають проявлятися. Запит клієнтів Gartner у багатьох регіонах світу виявив недобросовісну поведінку з боку постачальника хмарних послуг після того, як підприємства обрало основного постачальника.

Деякі хмарні постачальники використовують тактику «сильної руки», щоб змусити підприємства погоджуватися на все більш високі рівні витрат. Інші використовують ліцензування програмного забезпечення з укоріненої бази операційної системи та використання системи керування реляційною базою даних, щоб спрямувати більше використання хмари на свої відповідні пропозиції.

Перші ознаки свідчать про те, що деякі підприємства чинять запеклий опір і в результаті будують значні плани щодо диверсифікації постачальників ІТ. Але складність і накладні витрати на керування декількома хмарними постачальниками в поєднанні з нижчими знижками через менші зобов’язання постачальників часто призводять до того, що мультихмарна стратегія збільшує сукупну вартість володіння, а не знижує її за бажанням.

# 2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ В ХМАРНОМУ СЕРЕДОВИЩІ ПІДПРИЄМСТВА НА БАЗІ AMAZON GUARDDUTY

Amazon Web Services вже 12 рік поспіль залишається лідером в категорії CIPS «Магічного квадранту» Gartner. Також AWS займає найбільшу частку на ринку постачальників хмарних послуг. Саме ці два фактори стали вирішальними при виборі провайдера, сервіси якого, зокрема GuardDuty, будуть розглянуті в наступних двох підрозділах.

## 1.1. Основні сервіси AWS та їх призначення

Amazon Web Services (AWS) надає масштабовану платформу хмарних обчислень із високою доступністю та надійністю, надаючи інструменти, які дозволяють клієнтам запускати широкий спектр додатків та застосунків. Допомога у захисті конфіденційності, цілісності та доступності систем і даних клієнтів є пріоритетом для AWS, як і збереження довіри та впевненості клієнтів.

Перш ніж почати огляд сервісів AWS, необхідно пояснити, чим безпека в хмарі дещо відрізняється від безпеки в локальних ЦОД. Коли підприємство переміщує комп’ютерні системи та дані в хмару, відповідальність за безпеку розподіляється між цим підприємством та постачальником хмарних послуг. У цьому випадку AWS відповідає за безпеку базової інфраструктури, яка підтримує хмару, а підприємство несете відповідальність за все, що розміщається в хмарі або підключається до хмари. Ця модель спільної відповідальності за безпеку зменшує операційне навантаження підприємства у багатьох відношеннях, а в деяких випадках може навіть покращити загальний стан безпеки без додаткових дій [10].

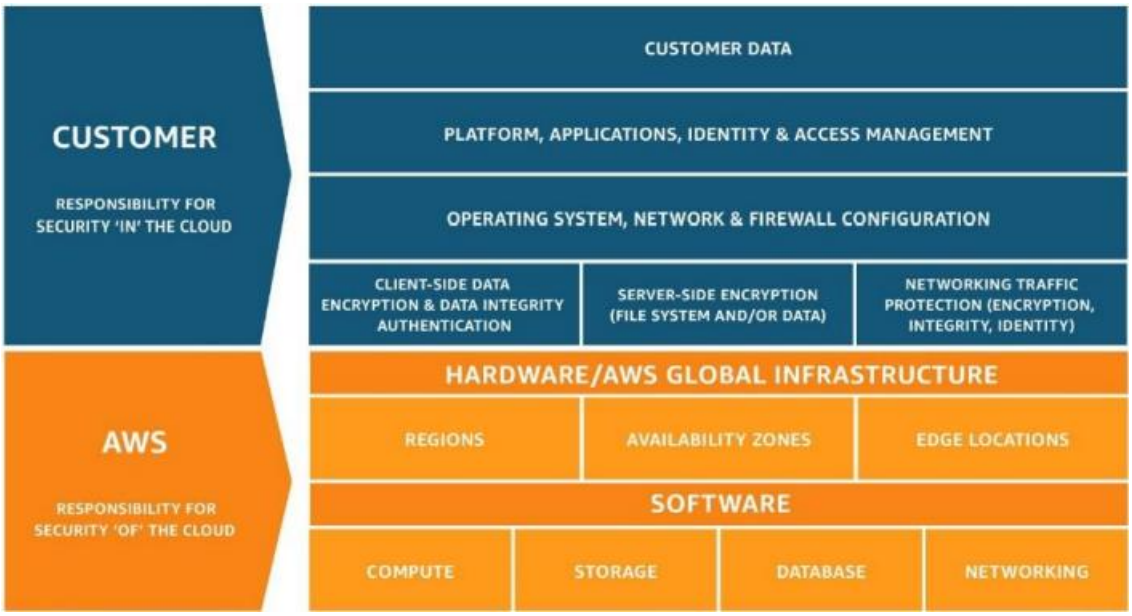



Рис. 2.1. Модель спільної відповідальності за безпеку AWS [10]

*Відповідальність за безпеку зі сторони AWS*

AWS відповідає за захист глобальної інфраструктури, яка керує всіма послугами в хмарі. Ця інфраструктура включає апаратне забезпечення, програмне забезпечення, мережу та засоби, які запускають служби AWS. Захист цієї інфраструктури є пріоритетом номер один для AWS. Незважаючи на те, що клієнти (можливо, за деякими виключеннями) не можуть відвідати ЦОД або офіси AWS, щоб побачити цей захист на власні очі, AWS пропонує звіти від сторонніх аудиторів, які перевірили відповідність різноманітним стандартам і правилам комп'ютерної та кібербезпеки.

Крім захисту глобальної інфраструктури, AWS відповідає за конфігурацію безпеки своїх продуктів, які вважаються керованими службами. Приклади таких типів служб включають Amazon DynamoDB, Amazon RDS, Amazon Redshift, Amazon EMR, Amazon WorkSpaces та інші. Ці служби забезпечують масштабованість і гнучкість хмарних ресурсів із додатковою перевагою керування ними. Для цих служб AWS виконує основні завдання безпеки, такі як гостьова операційна система (ОС) і усунення проблем бази даних, налаштування брандмауера та аварійне відновлення. Для більшості цих керованих сервісів все, що клієнту потрібно зробити, це налаштувати логічні елементи керування

доступом до ресурсів і захистити облікові дані свого облікового запису. Деяким клієнтам можуть знадобитися виконання додаткових задач, як-от налаштування облікових записів користувачів бази даних, але загалом конфігурацію безпеки виконує сервіс [10].

*Відповідальність за безпеку зі сторони клієнта*

За допомогою хмари AWS організація може отримати віртуальні сервери, сховище, бази даних і робочі столи за лічені хвилини замість тижнів. Також клієнт може використовувати хмарну аналітику та інструменти робочого процесу, щоб обробляти свої дані за потреби, а потім зберігати їх у власних ЦОД або в хмарі. Служби AWS, якими користується підприємство, визначають, скільки конфігураційної роботи має виконати це підприємство в рамках його відповідальності щодо безпеки.

Продукти AWS, які належать до категорії IaaS – Amazon EC2, Amazon VPC і Amazon S3, повністю знаходяться під контролем клієнта і вимагають безпосереднього керування та виконання всіх необхідних налаштувань безпеки. Наприклад, для екземплярів EC2 клієнт відповідає за керування гостьовою ОС (включно з оновленнями та виправленнями безпеки), додатками або утилітами, які встановлені на екземплярі, а також конфігурацію брандмауера AWS на кожному екземплярі. Це, в основному, ті самі завдання безпеки, які виконуються незалежно від того, де розташовані сервери.

Сервіси, що керуються AWS, як-от Amazon RDS або Amazon Redshift, надають усі ресурси, необхідні для виконання конкретного завдання, але без додаткової роботи з налаштування. Завдяки керованим службам клієнту не доведеться турбуватися про запуск і підтримку екземплярів, виправлення гостьової ОС або бази даних або реплікацію баз даних – AWS безе це на себе. Але, як і у випадку з усіма службами, клієнту слід захистити облікові дані свого облікового запису AWS і налаштувати індивідуальні облікові записи користувачів за допомогою Amazon Identity and Access Management (IAM), щоб кожен із користувачів мав власні облікові дані для, наприклад, розподілення обов’язків [10].

Основні служби та сервіси AWS:

*Amazon EC2 (Elastic Compute Cloud)*

EC2 – це хмарна платформа від Amazon, яка пропонує безпечну обчислювальну потужність із змінним розміром. Його мета – надати розробникам легкий доступ і зручність використання для хмарних обчислень веб-масштабу, одночасно дозволяючи повністю контролювати обчислювальні ресурси.

*Amazon RDS (Relational Database Services)*

RDS спрощує конфігурацію бази даних, керування та масштабування в хмарі. RDS доступний на різних екземплярах баз даних, які оптимізовані для продуктивності та пам’яті, забезпечуючи шість популярних двигунів баз даних, включаючи Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle і SQL.

*Amazon S3 (Simple Storage Service)*

S3, за своєю суттю, полегшує зберігання об’єктів, забезпечуючи найкращу масштабованість, доступність даних, безпеку та продуктивність. Підприємства величезного розміру можуть використовувати S3 для зберігання та захисту великих обсягів даних для різноманітного призначення, таких як веб-сайти, застосунки, резервне копіювання тощо.

*Amazon GuardDuty*

GuardDuty – це служба виявлення загроз, яка постійно відстежує ваші облікові записи та робочі навантаження AWS на наявність зловмисної активності та надає докладні результати безпеки для видимості та виправлення.

*Amazon Lambda*

Lambda дозволяє запускати код без володіння або керування серверами. Користувачі платять лише за витрачений обчислювальний час.

*Amazon CloudFront*

CloudFront – це мережева платформа доставки вмісту, яка працює з високою швидкістю з безпечним розподілом даних, відео, програм і API у глобальному масштабі з малими затримками. Підключений до глобальної інфраструктури AWS, CloudFront легко інтегрується з такими системами, як Amazon S3, Amazon EC2, AWS Shield і Lambda, щоб керувати спеціальним кодом, персоналізуючи роботу.

*Amazon EBS (Elastic Block Store)*

EBS – це високопродуктивне рішення для блокового зберігання, яке використовується в Amazon EC2 для пропускної здатності та робочих навантажень будь-якого розміру в будь-який час. Він обробляє різноманітні робочі навантаження, такі як реляційні та нереляційні бази даних і корпоративні програми.

*Amazon VPC (Virtual Private Cloud)*

VPC дає змогу налаштувати достатньо ізольовану частину хмари AWS, де можна масштабно розгортати ресурси AWS у віртуальному середовищі. VPC дає клієнту повний контроль над середовищем, що включає можливість вибору власного діапазону IP-адрес, створення підмножин і розташування таблиць маршрутів і точок доступу до мережі.

*Amazon IAM (Identity and Access Management)*

IAM забезпечує безпечний доступ і керування ресурсами безпечним і відповідним чином. Використовуючи IAM, клієнт зможе створювати користувачів і групи та керувати ними, дозволяючи та забороняючи їхні дозволи для окремих ресурсів.

*Amazon Redshift*

Redshift – це служба сховища даних, яка пропонує найкращу в галузі продуктивність і безперебійне надання, яка підтримує економічно ефективний аналіз даних на стандартному SQL.

*Amazon Security Hub*

Security Hub – це служба керування безпекою в хмарі, яка перевіряє передові методи безпеки, збирає сповіщення та забезпечує автоматичне виправлення.

## 2.2. Призначення та основні функції рішення GuardDuty

Amazon GuardDuty – служба моніторингу, яка аналізує та обробляє джерела даних, як-от дані про події AWS CloudTrail для Amazon S3, журнали подій керування CloudTrail, журнали DNS, дані томів Amazon EBS, журнали аудиту Kubernetes, журнали потоків Amazon VPC і вхід RDS діяльність. Вона

використовує канали аналізу загроз, наприклад списки зловмисних IP-адрес і доменів, а також машинне навчання для виявлення неочікуваної, потенційно неавторизованої та зловмисної активності в середовищі AWS. Це може включати такі проблеми, як ескалація привілеїв, використання скомпрометованих облікових даних або зв’язок зі зловмисними IP-адресами, доменами, наявність зловмисного ПЗ в екземплярах Amazon EC2 і робочих навантаженнях контейнерів або виявлення незвичайної поведінки під час отримання доступу до бази даних тощо. Наприклад, GuardDuty може виявляти скомпрометовані екземпляри EC2 і робочі навантаження контейнерів, які обслуговують зловмисне ПЗ або майнінг біткойнів. Він також відстежує поведінку доступу до облікового запису AWS на наявність ознак компрометації, як-от несанкціоноване розгортання інфраструктури, екземпляри, що були розгорнуті в незвичному регіоні, який раніше не використовувався, або незвичні виклики API, як-от зміна політики паролів для зниження надійності пароля [11].

Особливістю GuardDuty є те, що моніторинг відбувається з залученням машинного навчання. Модель, що використовується, заснована на Variational Autoencoders (VAEs), яка останнім часом стала одним із найуспішніших підходів до моделювання складних розподілів даних. Це дозволяє GuardDuty оцінити ймовірнісний розподіл викликів API, що виконуються користувачами на обліковому записі AWS. Навіть якщо користувач в обліковому записі здійснює певні дії вперше, модель передбачатиме, чи є вони частиною його нормальної, очікуваної роботи. Саме ця додана ймовірна складова допомагає проводити точні виявлення підозрілої поведінки облікового запису [12].

GuardDuty використовує цю нову модель машинного навчання, щоб ідентифікувати незвичайну активність в облікових записах, аналізувати відповідність активності безпеці, враховуючи контекст, у якому вона була викликана, і застосовувати прогнозну ймовірність для винесення остаточного висновку про те, чи є ця активність достатньо аномальною для розслідування. Нове виявлення загроз на основі моделі, додане до GuardDuty, також допомагає визначити тактику атаки, пов’язану з аномальними викликами API, включаючи

виявлення, початковий доступ, постійність, ескалація привілеїв, обхід захисту, доступ до облікових даних, вплив і викрадання даних.

Нові поведінкові виявлення машинного навчання в GuardDuty надає багаті контекстні дані як частину висновків GuardDuty. Ці висновки GuardDuty дозволяють швидко приймати рішення про те, чи потрібно запускати процес реагування на інцидент.

У нових висновках тепер можна побачити детальний список усіх аномальних API, які були викликані одним і тим же користувачем протягом кількох хвилин. Наприклад, замість того, щоб повідомити, що користувач IAM Admin-1 аномально викликав S3 ListBuckets API, GuardDuty повідомить, що поруч із цією операцією користувач також аномально викликав API GetBucketACL, GetBucketPublicAccessBlock і PutBucketPublicAccessBlock. Усі API у списку буде згруповано за пов’язаною службою AWS, щоб було ще простіше швидко зрозуміти, до яких служб був отриманий доступ в рамках аномальної активності. Подія також містить детальну інформацію про те, які з аномально викликаних API були викликані успішно, а які з помилкою, включаючи отриману відповідь про помилку. Цей контекст може бути важливим, коли сортуються результати. Наприклад, успішні виклики API вказують на те, що користувач зміг виконати певні операції та представляють інцидент вищої серйозності. З іншого боку, якщо користувачеві було заборонено доступ, це може свідчити про скомпрометовані облікові дані, які зловмисник намагався використати для визначення доступних дозволів до тих чи інших ресурсів.

Кожна подія чітко визначає, які атрибути активності були аномальними для конкретного користувача, а також для всіх інших користувачів, які працюють у тому самому обліковому записі AWS, щоб допомогти визначити, чому поведінку було позначено як дуже підозрілу. Нарешті, деталі події також включають інформацію про очікувану поведінку користувача та всіх інших користувачів, які працюють у тому самому обліковому записі AWS. Очікувана поведінка буде згрупована на основі її частоти протягом періоду профілювання. Наприклад, часті (щодня або щотижня), нечасті (кілька разів на місяць) або рідкісні (рідше одного

разу на місяць).

Фактично, GuardDuty є просунутою мережевою IDS з машинним навчанням, яку доповнюють функції антивірусного захисту та контролю доступу. Тому компанія Foregenix провела порівняння GuardDuty з іншими «IDS-like» рішеннями для визначення лідера у сфері систем виявлення вторгнень в хмару. Після тестування ряду рішень, доступних на ринку AWS, з використанням різних посібників із вторгнень і технічних інструментів, Foregenix виявив [13], що жодне рішення не забезпечує повного «готового» покриття всіх можливих типів вторгнень. Однак, будучи мережевим або «нехостовим» IDS, Amazon GuardDuty успішно виявляв і сповіщав про всі спроби вторгнення без необхідності попереднього налаштування. У цьому відношенні GuardDuty отримав набагато вищу оцінку, ніж усі інші конкуруючі рішення, і, безумовно, був найуспішнішим варіантом з точки зору виявлення специфічних загроз AWS.

Щоб виявити несанкціоновану та неочікувану активність в середовищі AWS, GuardDuty аналізує та обробляє дані з джерел. GuardDuty використовує ці джерела даних для виявлення аномалій, пов’язаних із такими типами ресурсів AWS: ключі доступу IAM, екземпляри EC2, контейнери S3 та ресурси Amazon EKS (Рис. 2.2). Під час передачі від цих джерел даних до GuardDuty усі логи шифруються. GuardDuty витягує різні поля з цих логів для профілювання та виявлення аномалій, а потім видаляє їх [11].

*Журнали подій AWS CloudTrail*

AWS CloudTrail надає історію викликів API AWS для облікового запису, включаючи виклики API, здійснені за допомогою консолі керування AWS, пакетів SDK AWS, інструментів командного рядка та певних служб AWS. CloudTrail також дозволяє визначити, які користувачі та облікові записи викликали AWS API для служб, які підтримують CloudTrail, IP-адресу, з якої здійснювалися виклики, і коли виклики відбувалися. GuardDuty може відстежувати як події керування CloudTrail, так і, за бажанням, події даних CloudTrail для S3.

Коли вмикається GuardDuty, він негайно починає аналізувати журнали подій CloudTrail. Він поглинає дані про події від CloudTrail Management і S3

безпосередньо з CloudTrail через незалежний і дубльований потік подій. При цьому, GuardDuty не керує подіями CloudTrail і жодним чином не впливає на наявні конфігурації CloudTrail.

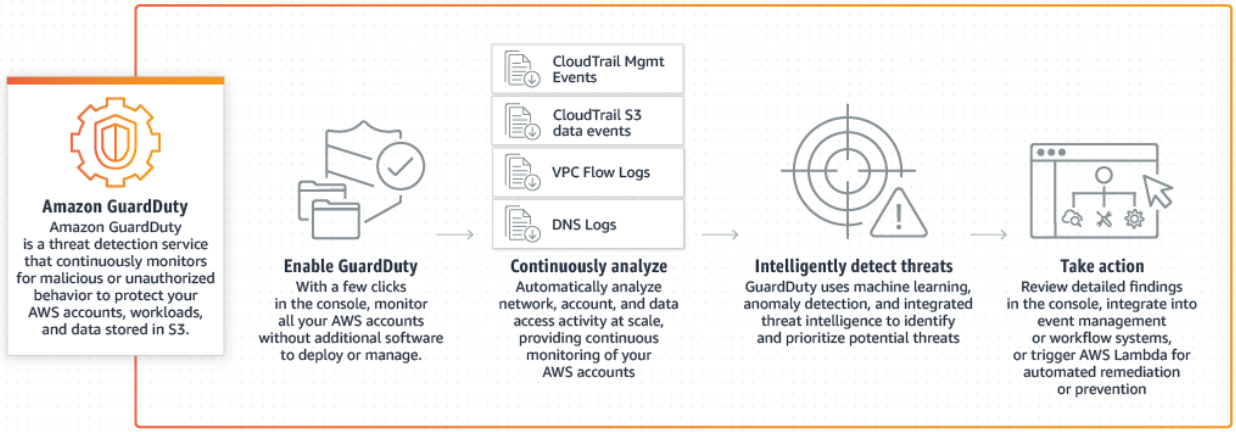



Рис. 2.2 Процес роботи GuardDuty

Ще одна важлива деталь про те, як GuardDuty використовує CloudTrail як джерело даних, – це обробка глобальних подій CloudTrail. Для більшості послуг події записуються в Регіоні, де відбулася дія. Для глобальних служб, таких як IAM, AWS Security Token Service, Amazon S3, Amazon CloudFront і Route 53, події доставляються в будь-який трейл, який включає глобальні служби, і реєструються як такі, що відбуваються у Східному регіоні США (Північна Вірджинія).

GuardDuty обробляє всі події, які надходять до Регіону, включаючи глобальні події, які CloudTrail надсилає в усі Регіони. Це дозволяє GuardDuty підтримувати профілі користувачів і ролей у кожному Регіоні, а також дозволяє точно виявляти облікові дані, які зловмисно використовуються в Регіонах.

Увімкнення GuardDuty у всіх підтримуваних регіонах AWS дозволяє GuardDuty генерувати висновки про несанкціоновану або незвичайну діяльність навіть у Регіонах, які активно не використовуються. Це також дозволяє GuardDuty відстежувати події CloudTrail для глобальних служб AWS. Якщо GuardDuty не увімкнено в усіх підтримуваних регіонах, його здатність виявляти дії, які включають глобальні служби, зменшується.

*Дані про події AWS CloudTrail для S3*

Дані про події, також відомі як операції площини даних, дають уявлення про

операції з ресурсами, які виконуються на ресурсі або всередині нього. Вони часто займають великий обсяг.

Нижче наведено приклади даних про події CloudTrail для S3, які GuardDuty може відслідковувати:

*GetObject* API operations

*PutObject* API operations

*ListObjects* API operations

*DeleteObject* API operations

*Журнал аудиту Kubernetes*

Сервіс Amazon Elastic Kubernetes (Amazon EKS) [14] – служба для запуску Kubernetes на AWS без необхідності встановлювати, керувати та підтримувати власну площину керування або вузли Kubernetes. Kubernetes – це система з відкритим кодом для автоматизації розгортання, масштабування та керування контейнеризованими додатками.

Журнал аудиту Kubernetes фіксує послідовні дії в кластері Amazon EKS, зокрема дії користувачів, додатків, які використовують Kubernetes API, і площі керування. Журнал аудиту є компонентом усіх кластерів Kubernetes.

Amazon EKS дозволяє завантажувати журнал аудиту Kubernetes як журнал Amazon CloudWatch за допомогою функції збору даних з площі керування EKS. Коли вмикається EKS Protection в GuardDuty, GuardDuty негайно починає аналізувати журнали аудиту Kubernetes для ресурсів Amazon EKS. Він отримує доступ до журналу аудиту безпосередньо з функції збору даних з площі керування Amazon EKS через незалежний і дублюючий потік журналів потоку.

*VPC Flow Logs*

VPC Flow Logs сервісу Amazon VPC фіксує інформацію про IP-трафік, що надходить до та з мережевих інтерфейсів середовища.

Коли вмикається GuardDuty, він негайно починає аналізувати дані VPC Flow Logs. Він отримує доступ до зібраних даних безпосередньо з функції VPC Flow Logs через незалежний дублюючий потік журналів потоку.

*Логи DNS*

Якщо для екземплярів Amazon EC2 використовуються DNS-резолвери AWS (налаштування за замовчуванням), тоді GuardDuty зможе отримати доступ і обробити зібрані дані з DNS через внутрішні резолвери AWS DNS. Якщо використовується інший DNS-резолвер, наприклад OpenDNS або GoogleDNS, або якщо налаштовані власні DNS-резолвери підприємства, тоді GuardDuty не зможе отримати доступ і обробити дані з цього джерела даних.

Коли вмикається GuardDuty, він негайно починає аналізувати логи DNS із незалежного потоку даних.

*Томи Elastic Block Storage (EBS)*

GuardDuty Malware Protection сканує та виявляє зловмисне ПЗ на томах Amazon EBS, підключених до екземплярів Amazon EC2.

Коли GuardDuty генерує подію про виявлення зловмисного ПЗ в екземплярі EC2 або робочому навантаженні контейнера, GuardDuty створить знімки томів EBS, прикріплених до потенційно враженого екземпляра EC2 або робочого навантаження контейнера в обліковому записі. Використовуючи дозволи, надані GuardDuty через пов’язані з сервісом дозволи ролі для GuardDuty Malware Protection, GuardDuty створить зашифровані копії томів EBS із цього знімка в обліковому записі служби GuardDuty. Після цього GuardDuty виконає сканування копії томів EBS на наявність шкідливих програм (Рис. 2.3).

Після завершення сканування GuardDuty видаляє зашифровані копії томів EBS і знімки томів EBS. Якщо виявлено зловмисне ПЗ та ввімкнутий параметр збереження миттєвих знімків, миттєві знімки томів EBS не буде видалено й вони автоматично збережуться в обліковому записі AWS. Якщо зловмисне ПЗ не знайдено, знімки томів EBS не зберігатимуться, незалежно від налаштувань.

GuardDuty зберігатиме кожну копію тому EBS, яку сканує, протягом одного дня, якщо тільки не станеться збій у службі або збій у роботі тому EBS із копією та його перевіркою шкідливого ПЗ, після чого GuardDuty зберігатиме такий том EBS не більше семи днів. Розширений період зберігання призначений для сортування та усунення збою або збою. Захист від зловмисного ПЗ GuardDuty видалить репліку

тому EBS після усунення збою чи після закінчення тривалого періоду зберігання.

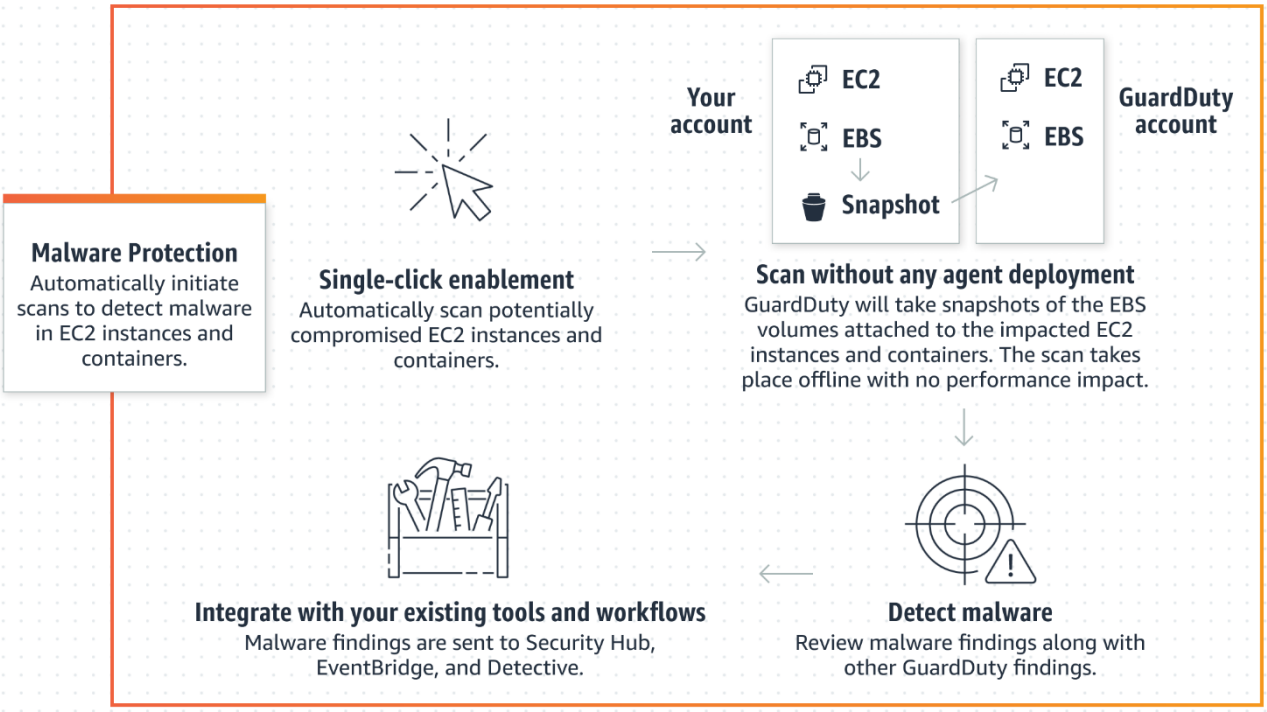



Рис. 2.3 Процес роботи Malware Protection в GuardDuty

*Моніторинг активності входу RDS*

Активність входу RDS фіксує як успішні, так і невдалі спроби входу до підтримуваних баз даних Amazon Aurora в середовищі AWS. Щоб допомогти клієнтам захистити їх бази даних, GuardDuty RDS Protection постійно відстежує активність входу на предмет потенційно підозрілих спроб входу. Наприклад, зловмисник може спробувати отримати доступ способом перебору паролів (метод «Грубої сили») до бази даних Amazon Aurora, вгадавши пароль бази даних.

Коли вмикається функцію захисту RDS, GuardDuty автоматично починає відстежувати активність входу RDS для ваших баз даних безпосередньо зі служби Aurora. Якщо є вказівки на аномальну поведінку під час входу, GuardDuty генерує подію про потенційно скомпрометовану базу даних.

## 1.2. Місце GuardDuty в архітектурі безпеки AWS

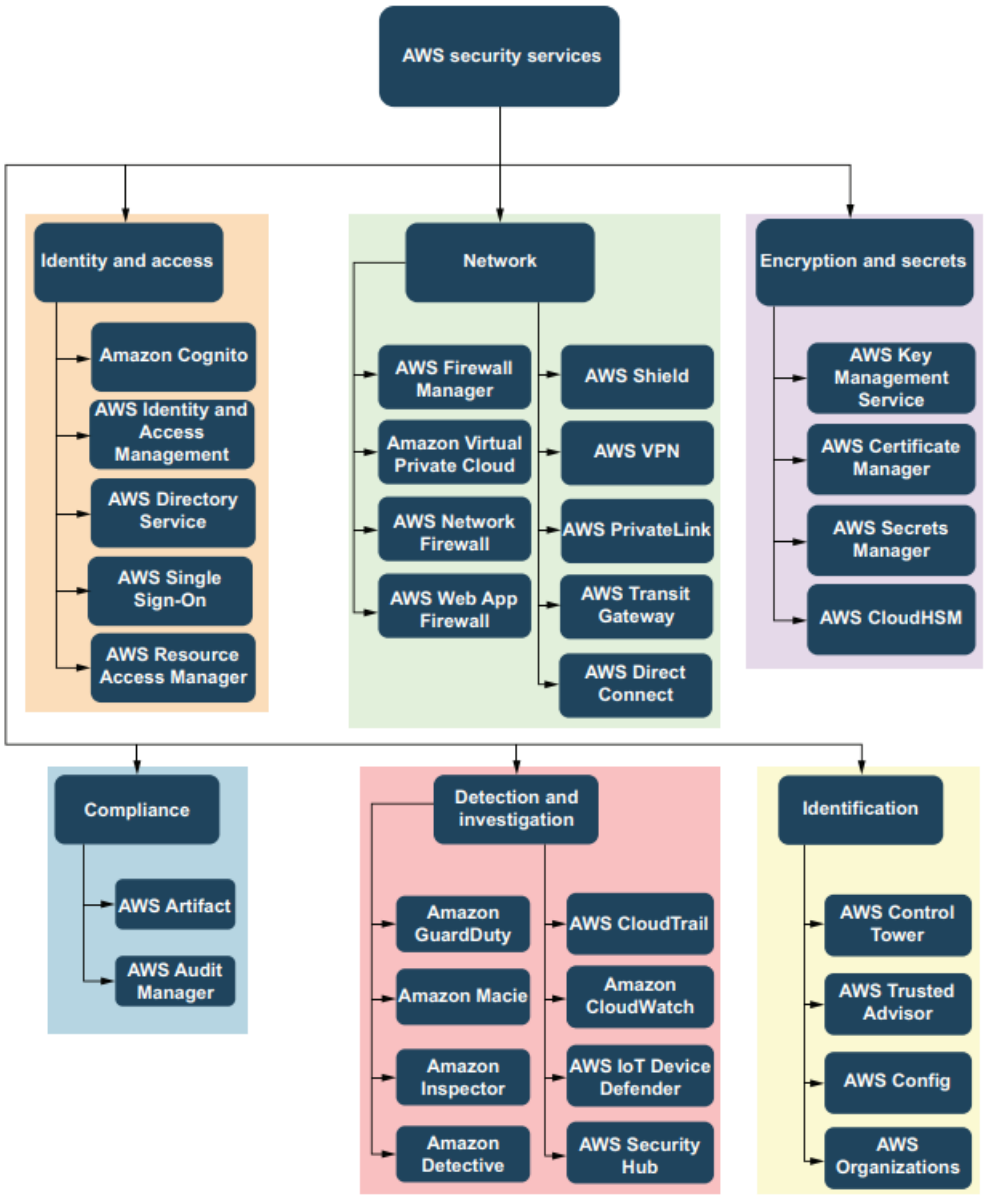



Рис. 2.4. Сервіси безпеки AWS

GuardDuty разом з іншими сервісами безпеки (рис. 2.4) постійно захищає ресурси клієнта від реалізації ризиків та нівелює загрози. Функціонал GuardDuty дозволяє службі займати багато ніш в архітектурі безпеки AWS. Краще всього це видно, якщо використовувати Cybersecurity Framework (Рис.2.5.) від NIST [15].


Рис.2.5. Cybersecurity Framework

Архітектура безпеки AWS за Cybersecurity Framework виглядає наступним чином:

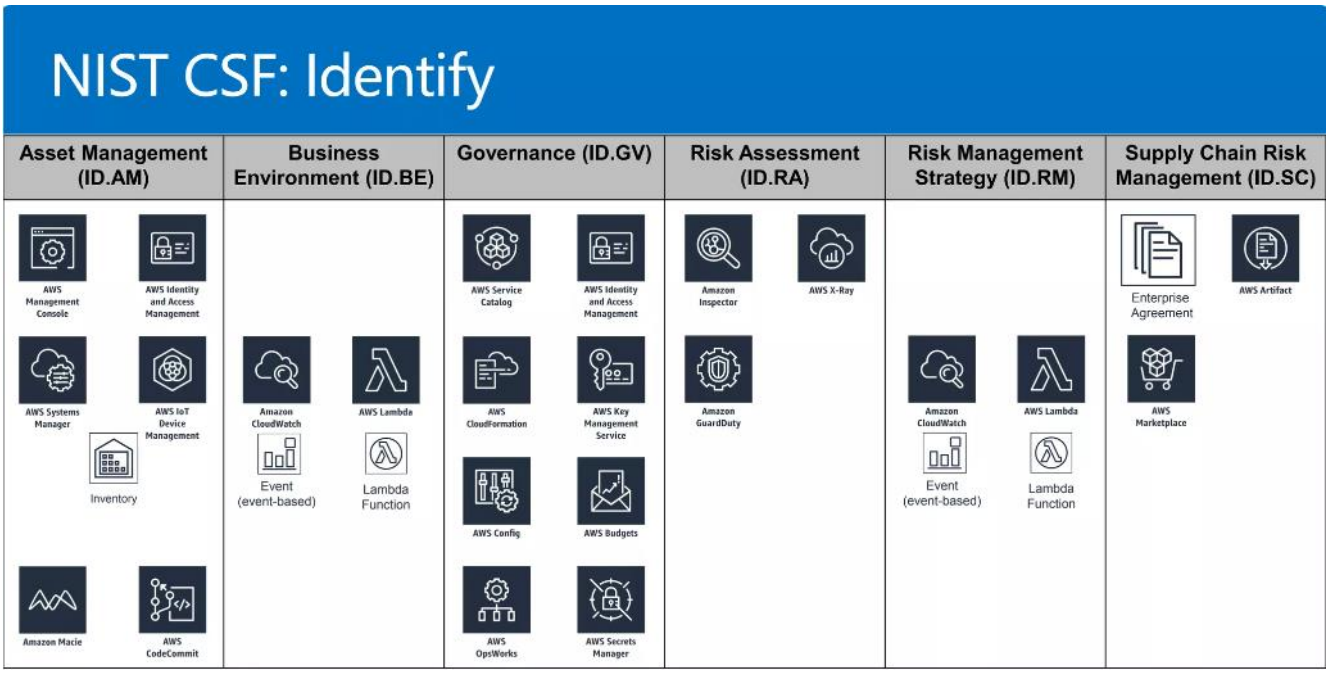



Рис.2.6. Функція ідентифікації ризиків

GuardDuty використовує загрози, вразливості та можливі наслідки для оцінки ризику. А ризик оцінюється за рівнем «тяжкості» події. Чим вище рівень, тим серйозніша загроза хмарному середовищу.

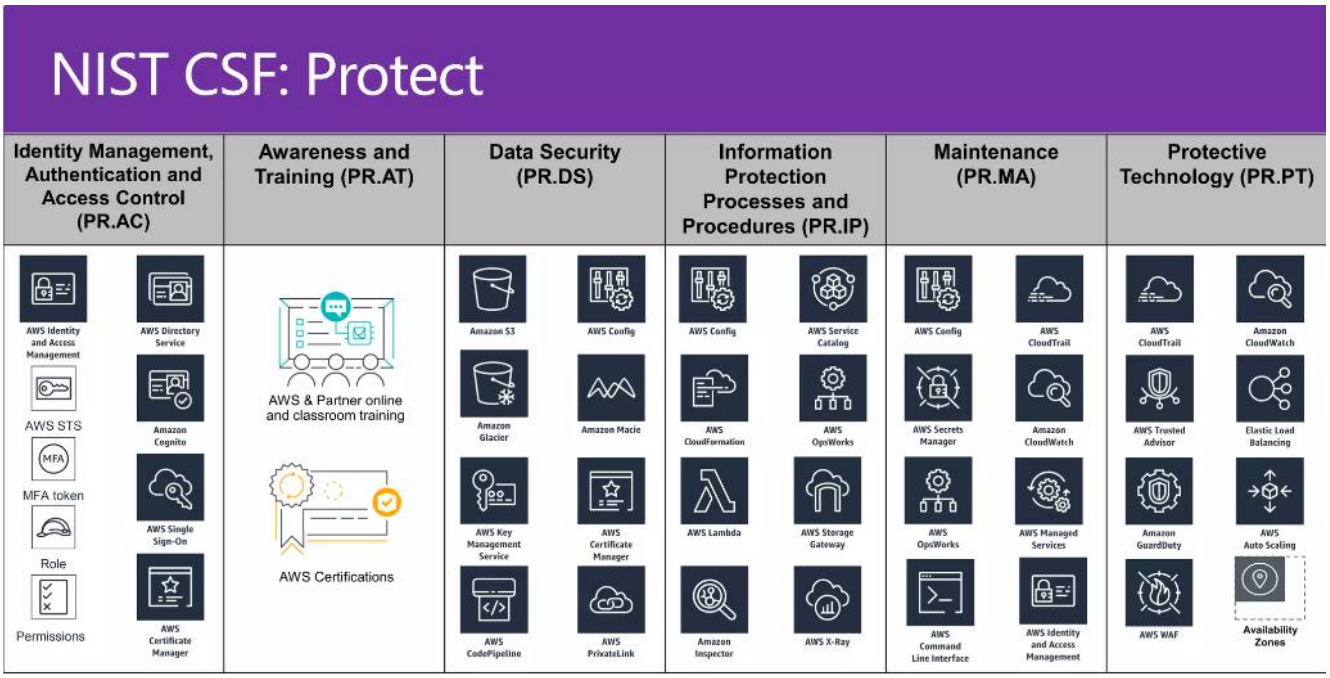



Рис. 2.7. Функція захисту

GuardDuty може (і повинен) використовуватись в режимі «найменшої функціональності», тобто адміністратор отримує лише ті права, які необхідні для виконання посадових обов’язків.

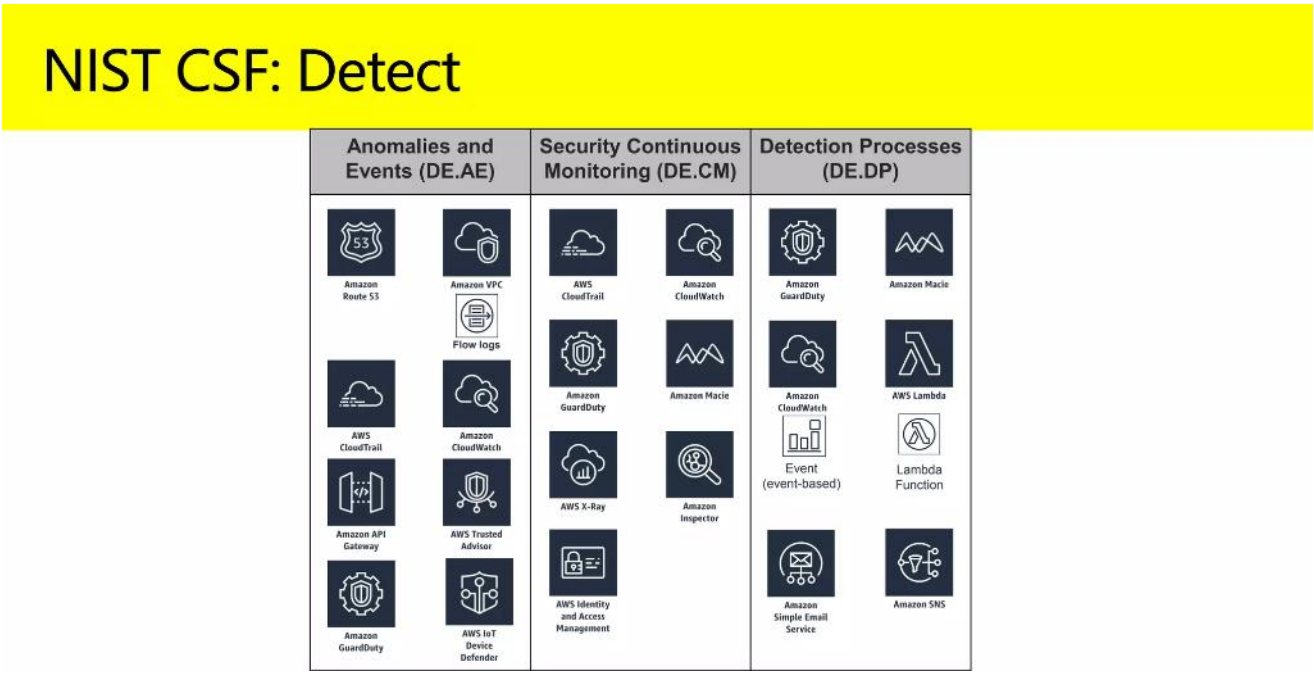



Рис. 2.8. Функція виявлення

Виявлені події аналізуються, щоб зрозуміти цілі та методи атаки. Визначається рівень тяжкості події. Отримані дані збираються та співвідносяться з даними з інших джерел та датчиків.

Активність хмарних ресурсів під постійним моніторингом. Також GuardDuty відслідковує активність персоналу, який може виконувати потенційно-небезпечні функції. Додатково здійснюється аналіз ресурсів на наявність шкідливого коду або ПЗ.

GuardDuty не тільки отримує, а й надсилає інформацію про події іншим сервісам безпеки. Сам процес виявлення постійно вдосконалюється завдяки машинному навчанню.

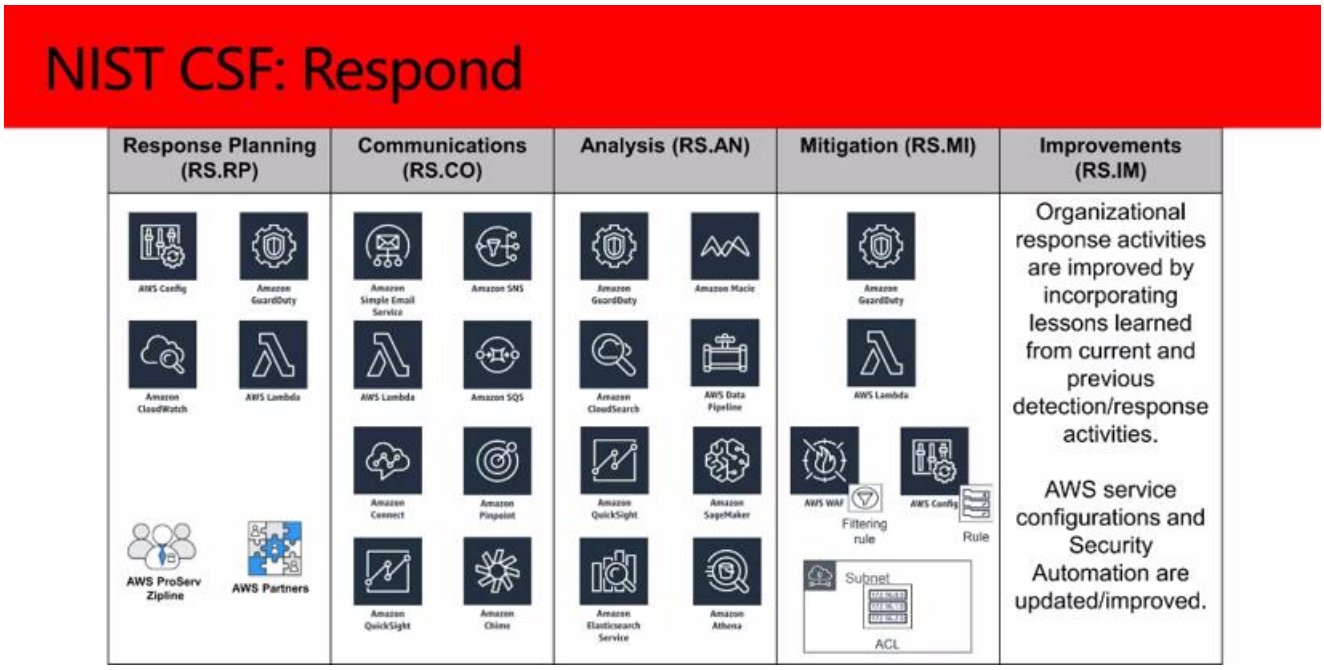



Рис. 2.9. Функція реагування

Інформації про подію достатньо, щоб виконати план із запобігання або подолання наслідків.

GuardDuty не бере участь у відновленні інфраструктури.

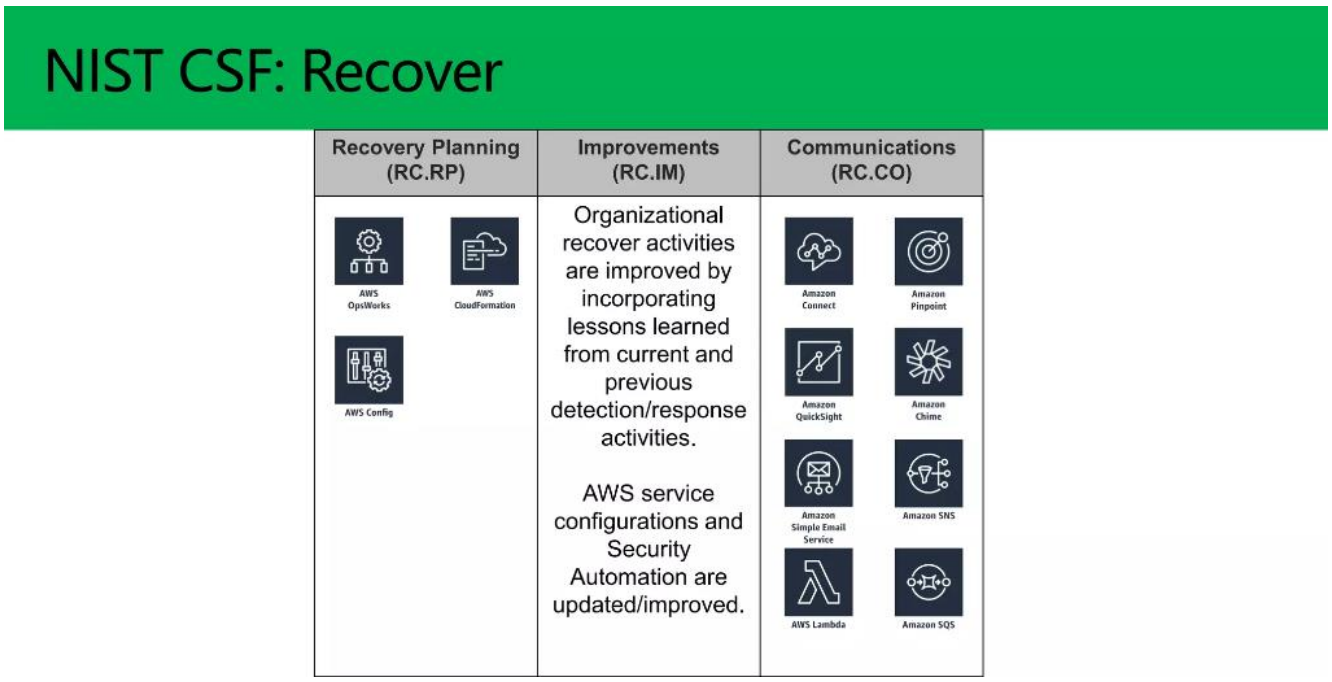



Рис. 2.10. Функція відновлення

# 3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ В ХМАРНОМУ СЕРЕДОВИЩІ ПІДПРИЄМСТВА

## 3.1. Активація та налаштування адміністратора сервісу Amazon GuardDuty та інтеграція з іншими сервісами безпеки

Для активації Amazon GuardDuty в хмарному середовищі підприємства на базі AWS необхідно ввійти як **root** або як користувач з повним доступом до середовища AWS

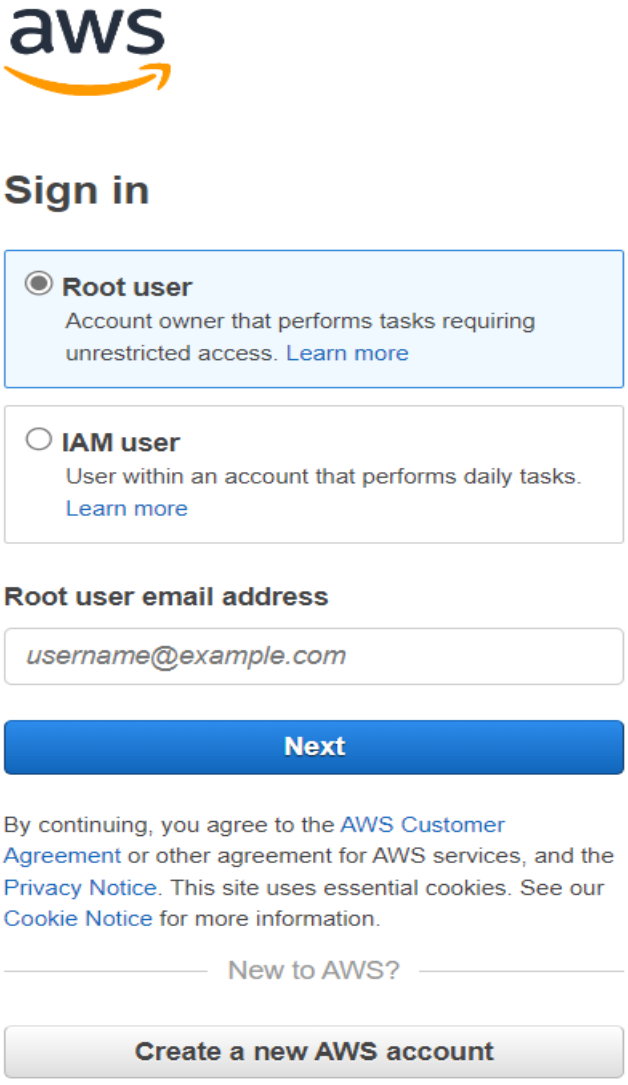



Рис. 3.1. Авторизація в AWS

*Експерименти з застосування сервісу GuardDuty будуть виконуватись від імені Адміністратора *Maxon_B*.

Перед початком застосування необхідно ввімкнути службу та синхронізувати з іншими службами безпеки. Для цього користувач **root**, який має повний контроль над всією інфраструктурою облікового запису підприємства, має авторизуватись.

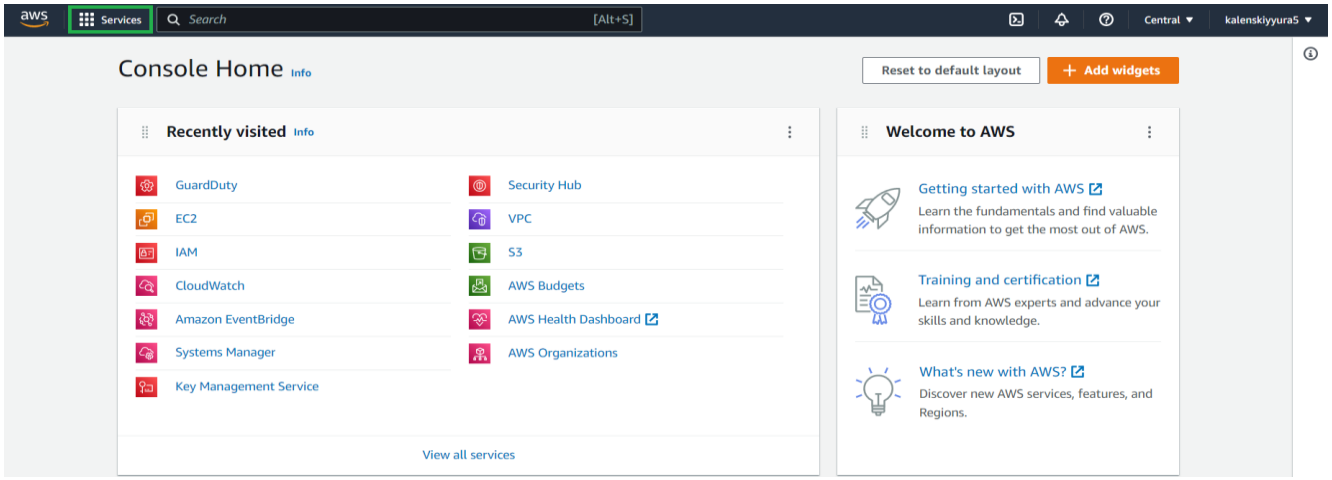



Рис. 3.2. Головна консоль

Після авторизації, користувач потрапляє до Головної Консолі (Рис. 3.2.), де відображаються віджети з важливою інформацією про середовище AWS.

У вкладці «Services», в категорії «Security, Identity, & Compliance», необхідно перейти до служби GuardDuty та активувати її:

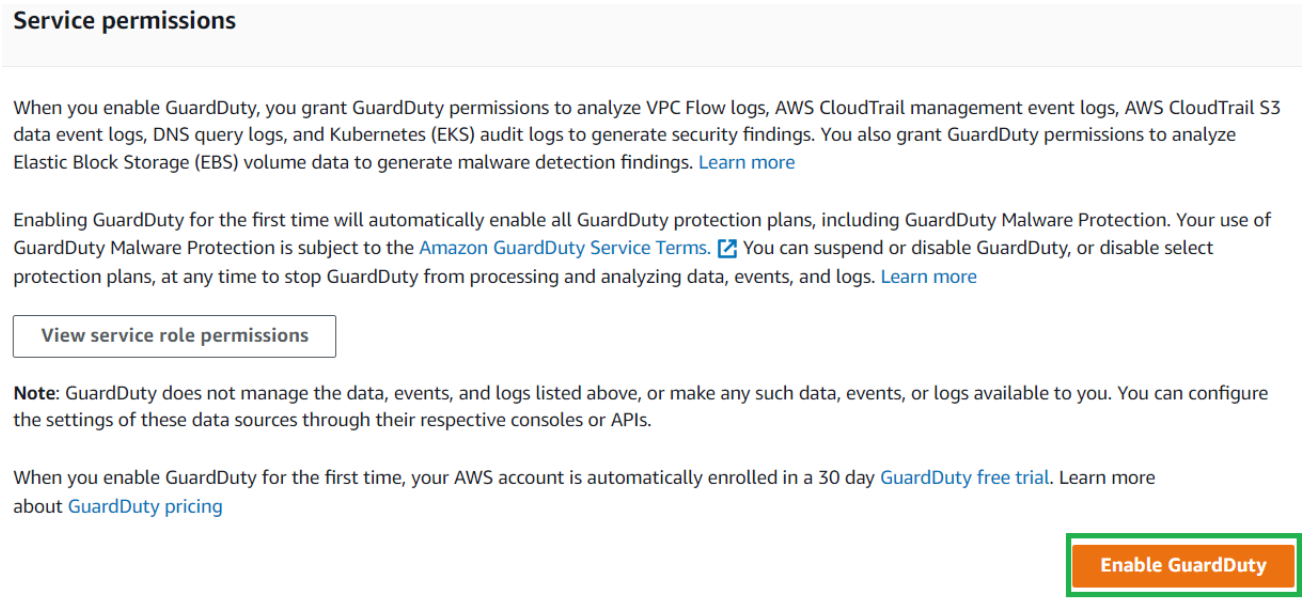



Рис. 3.3. Сторінка активації GuardDuty

Після активації користувач потрапляє до консолі GuardDuty:

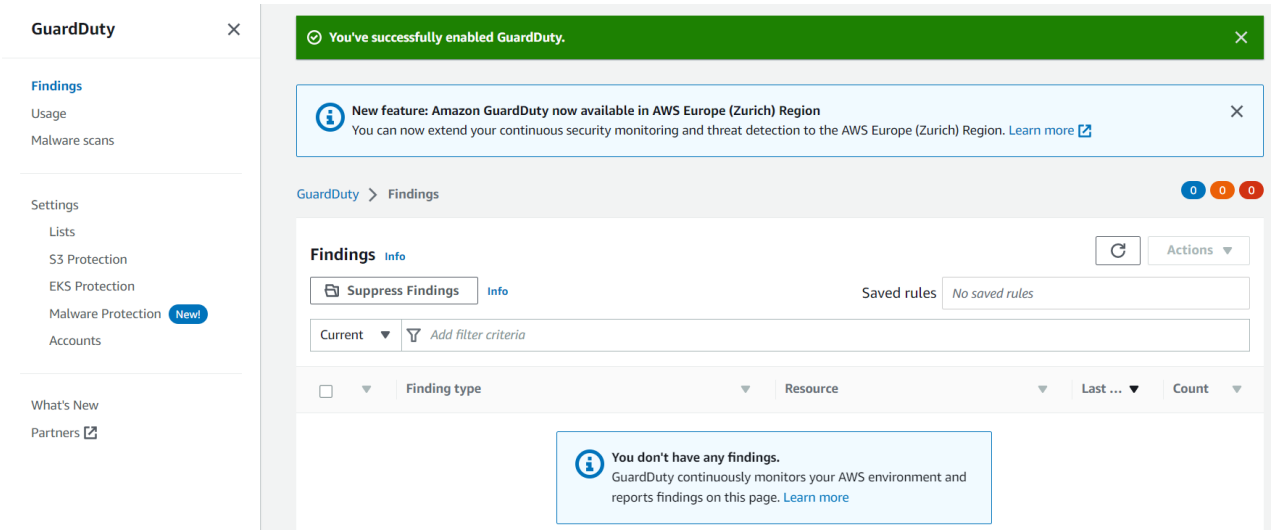



Рис. 3.4. Консоль GuardDuty

Звідси, у вкладці «Services», в категорії «Security, Identity, & Compliance», треба перейти до служби Security Hub і в меню «Integration» активувати GuardDuty:

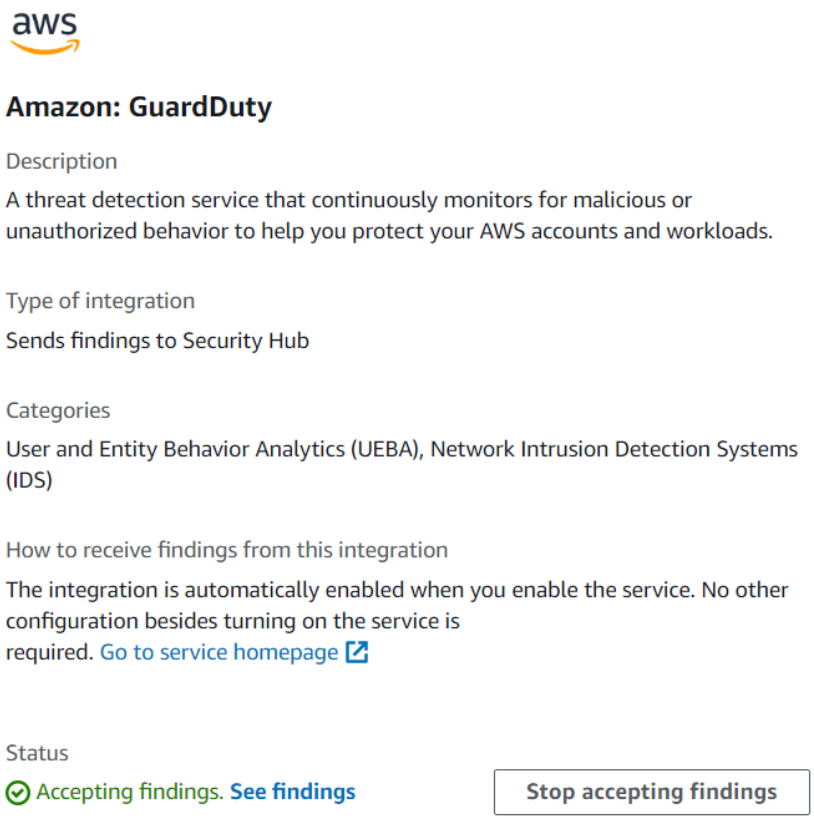



Рис. 3.5. Інтеграція GuardDuty з Security Hub

Далі необхідно створити користувача, який буде виконувати роль

Адміністратора GuardDuty.

В сервісі IAM у вкладці «Users» обрати «Add users»:

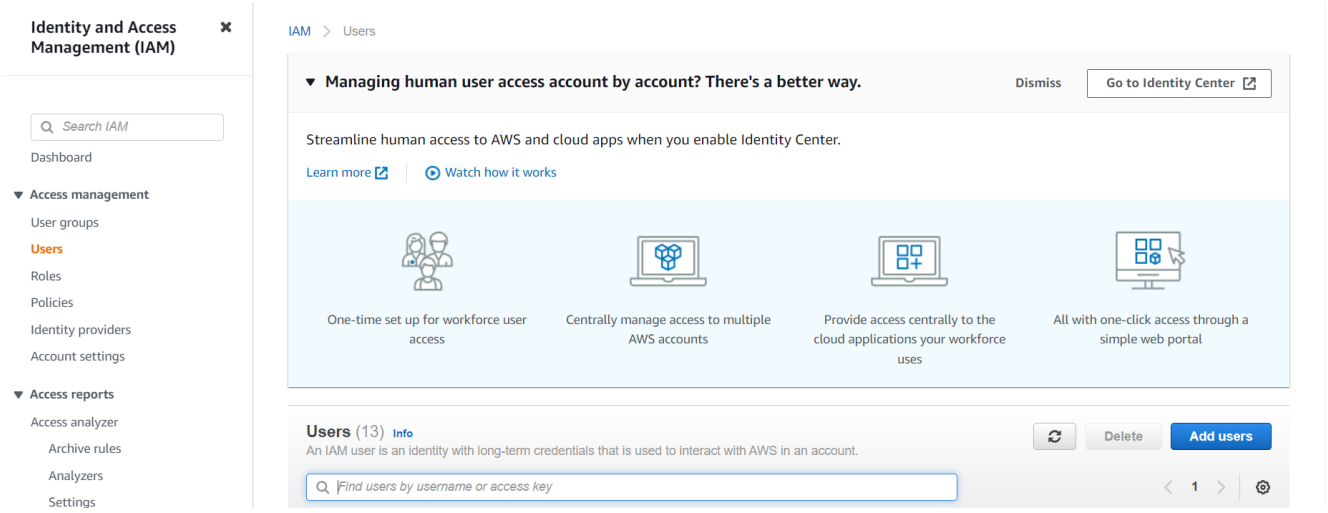



Рис. 3.6. Створення Адміністратора GuardDuty

Призначити ім’я, обрати тип допуску:

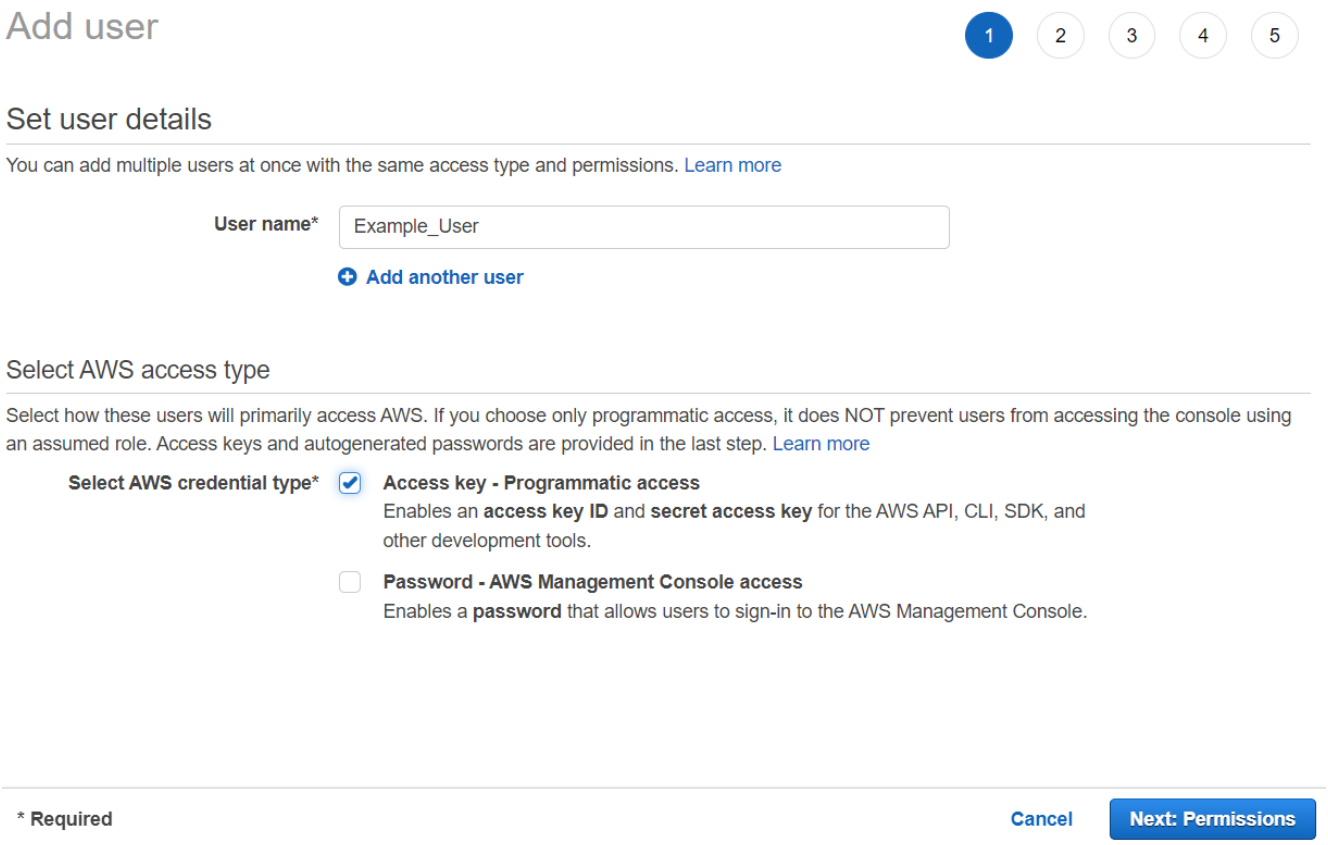



Рис. 3.7. Створення Адміністратора GuardDuty

Далі необхідно надати новому користувачі необхідні права для виконання

обов’язків Адміністратора GuardDuty. Можна додати його до вже існуючої групи Адміністраторів GuardDuty (Рис. 3.8.), скопіювати дозволи з іншого користувача (Рис. 3.9.) або обрати окремо дозволи з повного списку політик доступу (Рис. 3.10.).

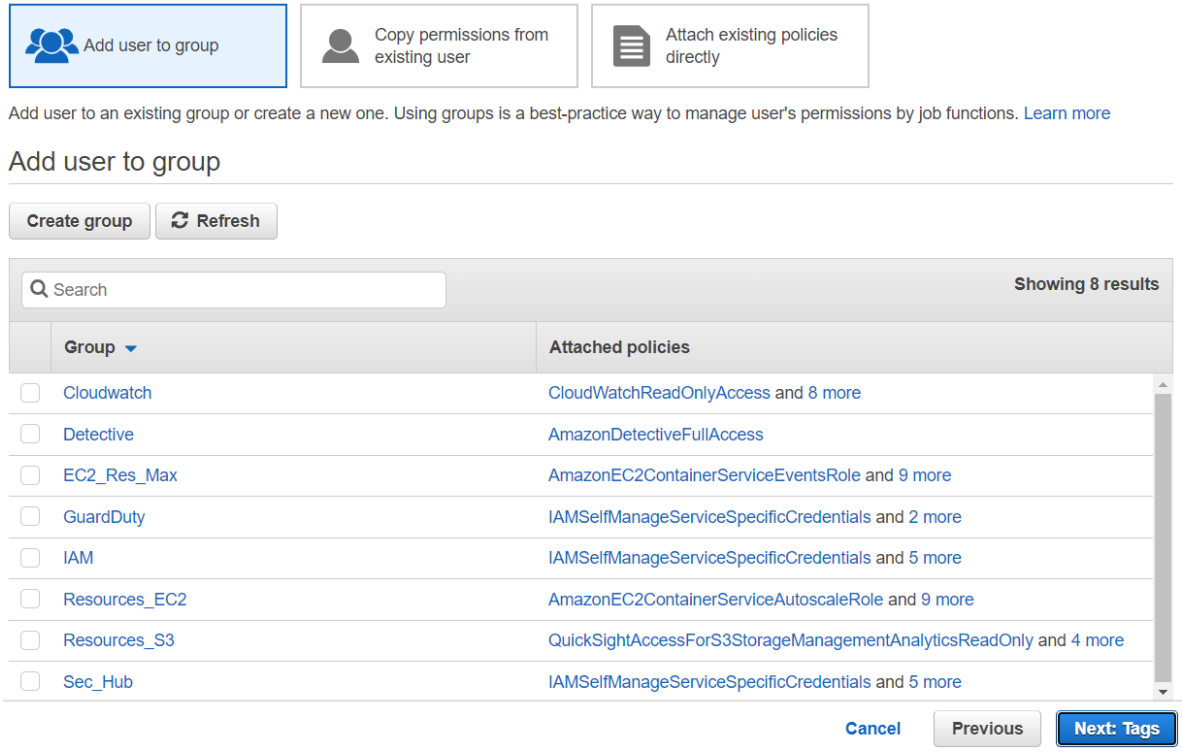



Рис. 3.8. Групи з політиками доступу

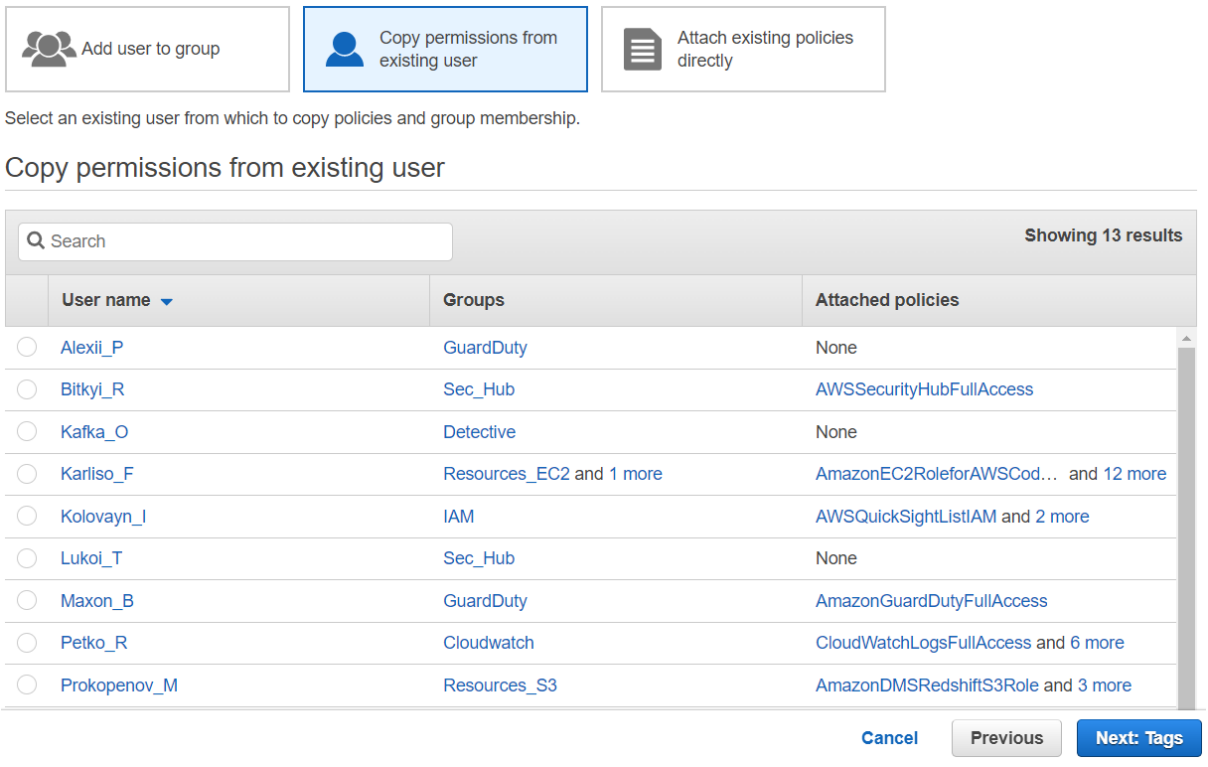



Рис. 3.9. Користувачі, з яких можна скопіювати політики доступу

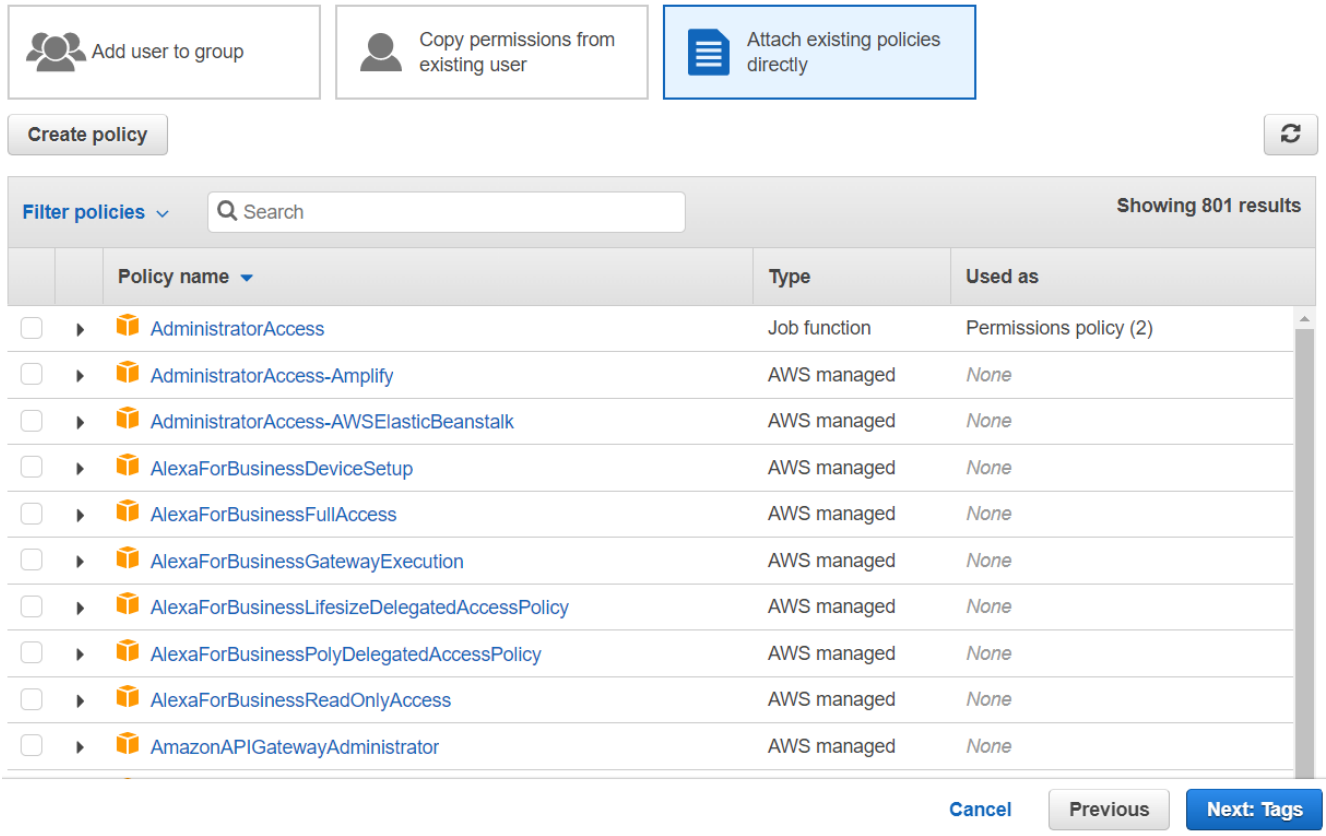



Рис. 3.10. Повний список політик доступу AWS

В останньому вікні перевіряється правильність налаштувань:

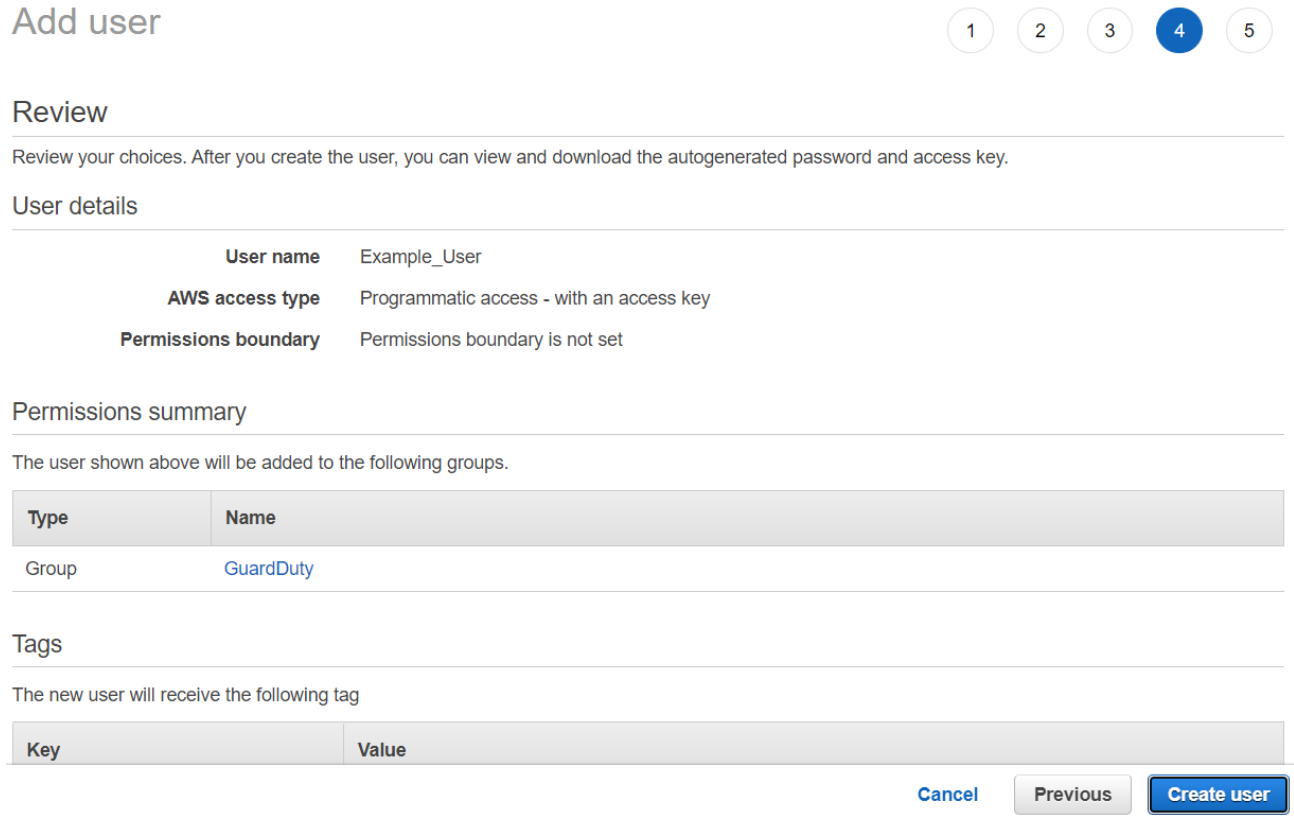



Рис. 3.11. Вікно огляду налаштувань нового користувача

Після створення з’явиться вікно успішного створення, а також ID ключ доступу та секретний ключ доступу:

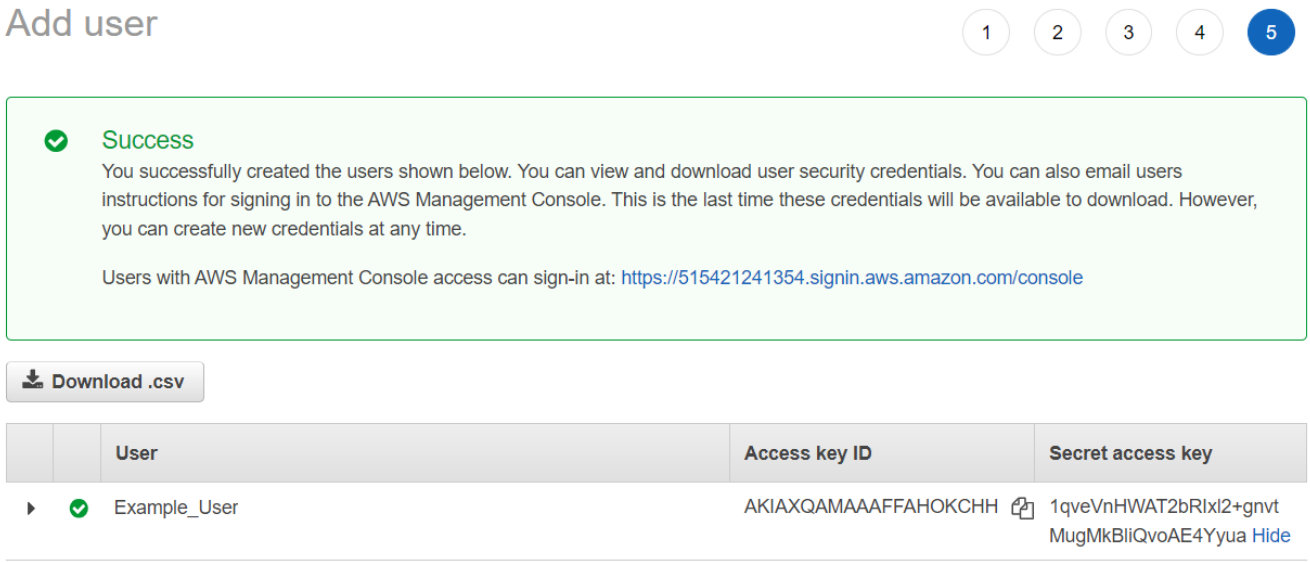



Рис. 3.12. Вікно успішного створення

В налаштуваннях «Security credentials» можна підключити пристрій для багатофакторної автентифікації, а також, за необхідності, скасувати відкритий і, відповідний ньому, закритий ключ доступу користувача:

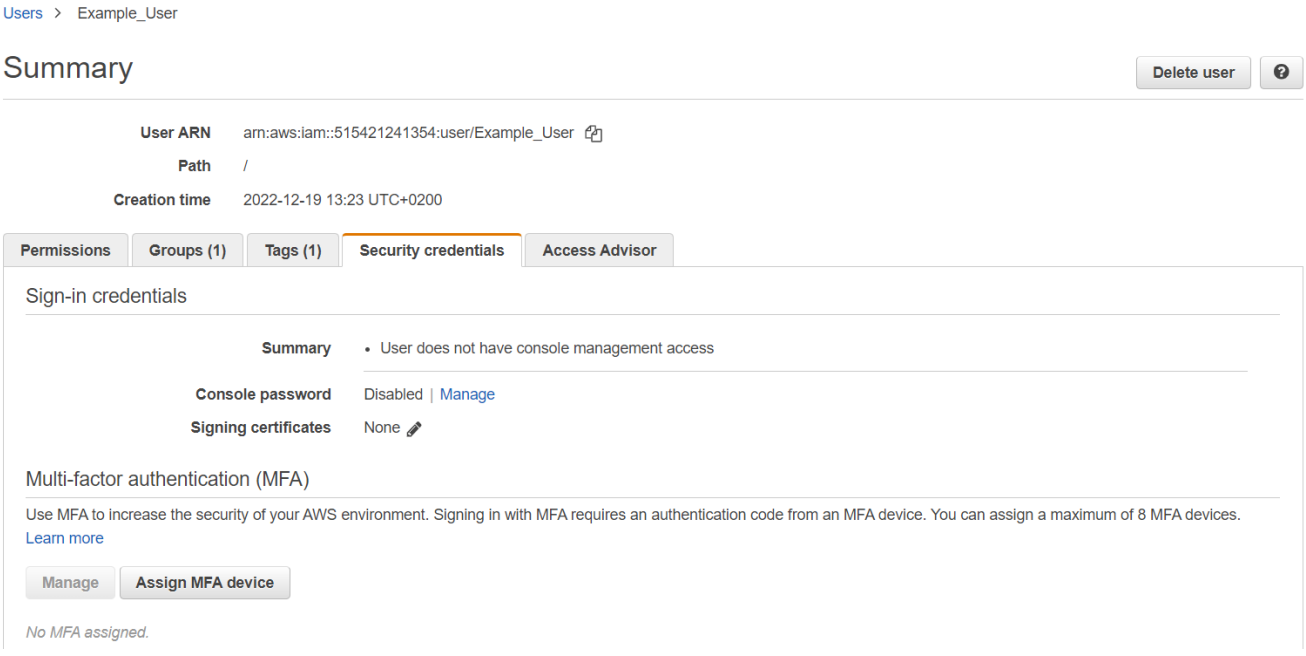



Рис. 3.13. Створення Адміністратора GuardDuty

### 3.2. Експеримент №1: Виявлення та усунення загрози компрометації облікових даних за допомогою GuardDuty

*Сценарій:* Адміністратор безпеки отримав сповіщення про подію в GuardDuty - *UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom* і *Recon:IAMUser/MaliciousIPCaller.Custom*:

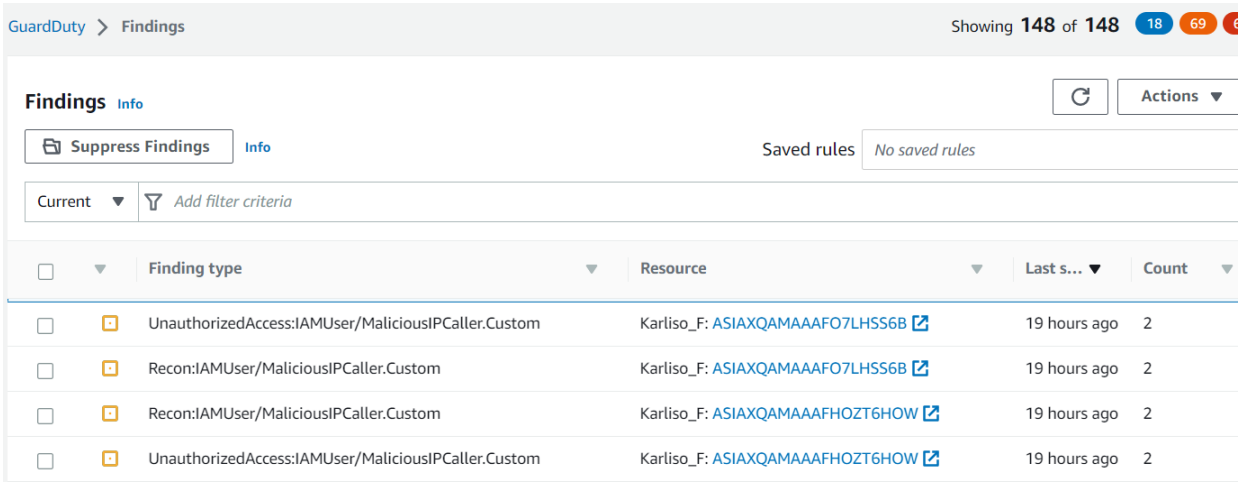



Рис. 3.14. Події GuardDuty

*Етап 1: розслідування*

Ці події інформують адміністратора про те, що операція API (наприклад, спроба запустити екземпляр EC2, створення нового користувача IAM, зміна привілеїв AWS) була викликана з IP-адреси, включеної до списку загроз GuardDuty. Список загроз складається з відомих шкідливих IP-адрес. Це може свідчити про неавторизований доступ до ресурсів середовищі AWS або про спробу провести розвідку наявних ресурсів організації.

Наступні рисунки демонструють детальний опис події:

**UnauthorizedAccess:IAMUser/MaliciousIPCaller.Custom**

Finding ID: aec28774acbc9f603213ba4a25e66158 Feedback

Medium API SendSSHPublicKey was invoked from an IP address 154.28.188.204 on the custom threat list sus2. Info

Investigate with Detective

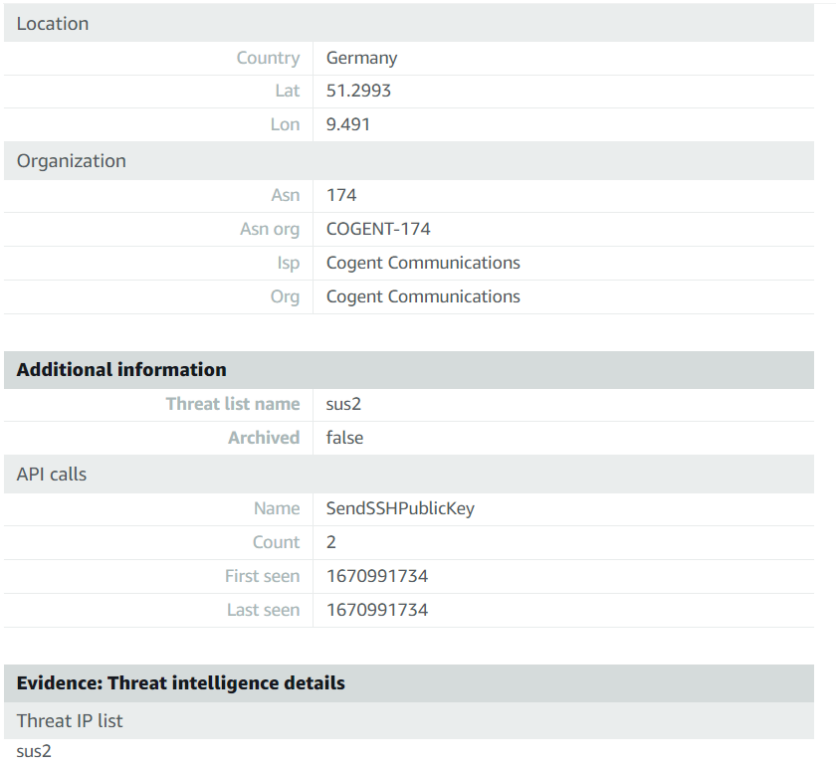
| Overview | |
|---|---|
| Severity | MEDIUM |
| Region | eu-west-1 |
| Count | 2 |
| Account ID | 515421241354 |
| Resource ID | No information available |
| Created at | 12-14-2022 06:34:11 (19 hours ago) |
| Updated at | 12-14-2022 06:34:11 (19 hours ago) |

| Resource affected | |
|---|---|
| Resource role | TARGET |
| Resource type | AccessKey |

Рис. 3.15. Опис події

| | |
|---|---|
| Access key ID | AKIAXQAMAAAFNFV6O677 |
| Principal ID | AIDAXQAMAAAFKGM622ARM |
| User type | IAMUser |
| User name | Karliso_F |
| Affected resources | |
| Instance ID | i-0b2063ba6215006f7 |
| **Action** | |
| Action type | AWS_API_CALL |
| API | SendSSHPublicKey |
| Service name | ec2-instance-connect.amazonaws.com |
| First seen | 12-14-2022 06:22:14 (19 hours ago) |
| Last seen | 12-14-2022 06:22:14 (19 hours ago) |
| **Actor** | |
| Caller type | Remote IP |
| IP address | 154.28.188.204 |
| Location | |
| Country | Germany |

Рис. 3.16. Опис події



| Location | |
|---|---|
| Country | Germany |
| Lat | 51.2993 |
| Lon | 9.491 |
| **Organization** | |
| Asn | 174 |
| Asn org | COGENT-174 |
| Isp | Cogent Communications |
| Org | Cogent Communications |

| **Additional information** | |
|---|---|
| Threat list name | sus2 |
| Archived | false |
| API calls | |
| Name | SendSSHPublicKey |
| Count | 2 |
| First seen | 1670991734 |
| Last seen | 1670991734 |

| **Evidence: Threat intelligence details** |
|---|
| Threat IP list |
| sus2 |

Рис. 3.17. Опис події

Судячи з розділу «Resources affected» адміністратор Karliso_F отримав віддалений доступ до екземпляру i-0b2063ba6215006f7 з використанням відкритих ключів SSH. Також в тому ж розділі вказаний номер його ключів доступу (Access Key ID).

Для подальшого розслідування можна створити фільтр по цьому номеру ключів доступу і переглянути всі інші порушення, пов’язані з цим користувачем. Також необхідно зв’язатись з користувачем для отримання деталей.

*Етап 2: реакція*

В процесі розслідування, після розмови з користувачем Karliso_F, було виявлено, що обліковий запис адміністратора попав руки зловмисника, тому необхідно відкликати ключі доступу для унеможливлювання подальшої компрометації системи. Для цього у вкладці «Services», в категорії «Security, Identity, & Compliance», потрібно перейти до служби AWS Identity and Access Management (IAM).

В розділі «Users» в полі пошуку ввести ключ доступу, який був в вказаний в

події та знайти необхідного користувача:

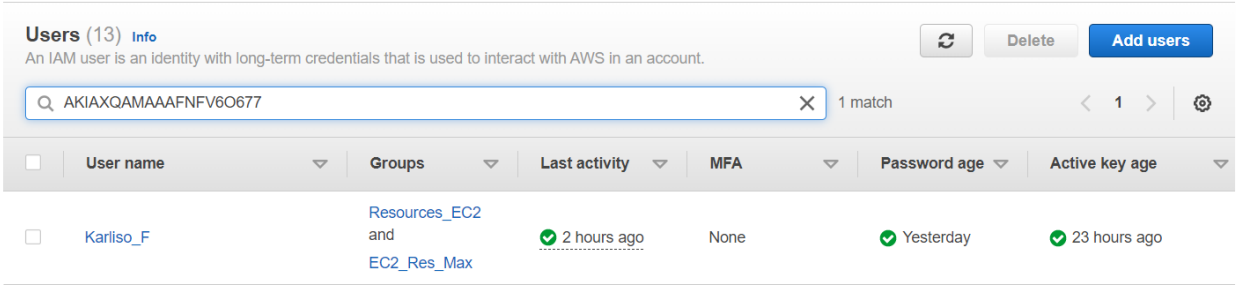



Рис. 3.18. Пошук скомпрометованого користувача

В меню «Security Credentials» і деактивувати ключ доступу:

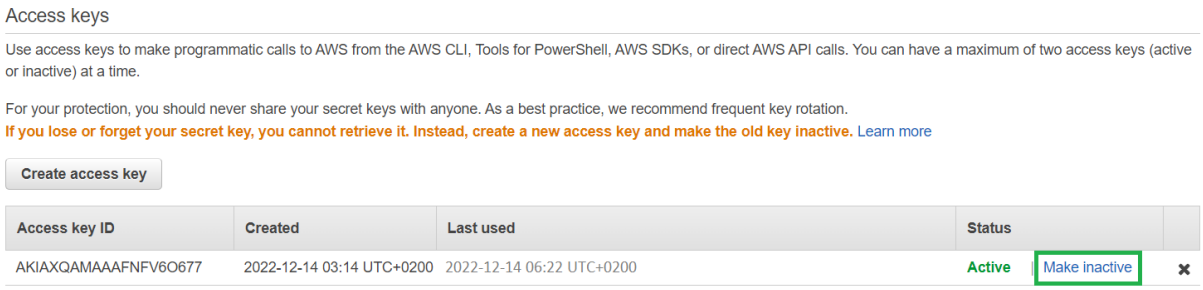



Рис. 3.19. Пошук скомпрометованого користувача


Рис. 3.20. Вікно підтвердження успішної деактивації

*Етап 3: перегенерація ключів доступу*

Після скасування ключів доступу вдалось захистити систему в цілому від подальшої компрометації. Проте, для виконання посадових обов'язків, Karliso_F необхідно в найближчий час отримати нові ключі та замінити їх на екземплярі.

В меню «Security Credentials» (Рис. 3.19.) треба перейти в «Create access key»:

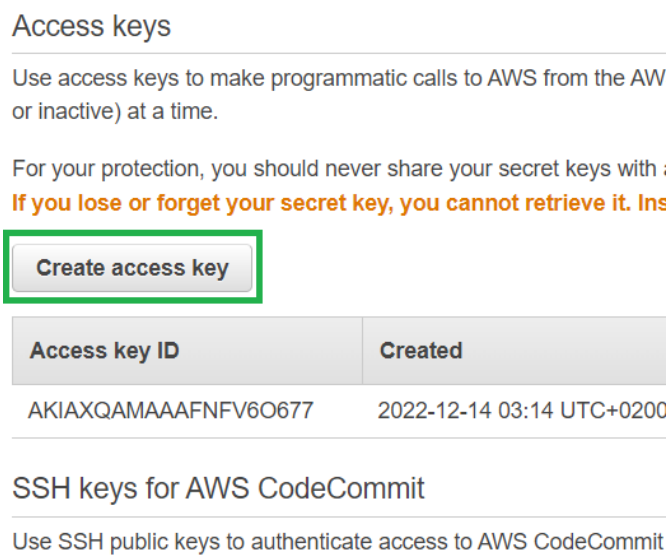



Рис. 3.21. Створення ключа доступу

Новий ключ сформовано:

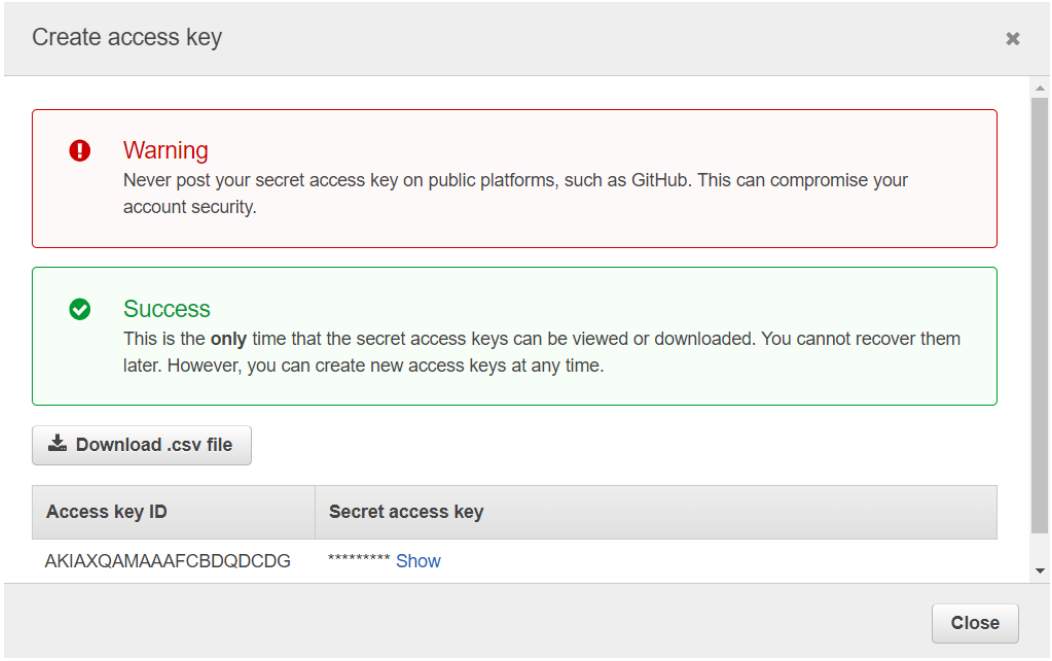



Рис. 3.22. Результат генерації

*Етап 4: ротація ключів на екземплярі EC2*

У вкладці «Services», в категорії «Compute», потрібно перейти до служби EC2:

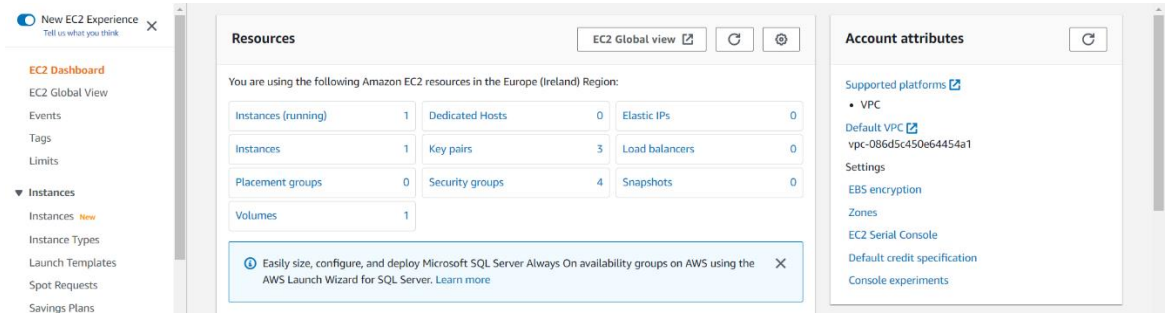



Рис. 3.23. Консоль EC2

Перейти в меню з екземплярами, там обрати скомпрометовану віртуальну машину, зупинити її та запустити знову:

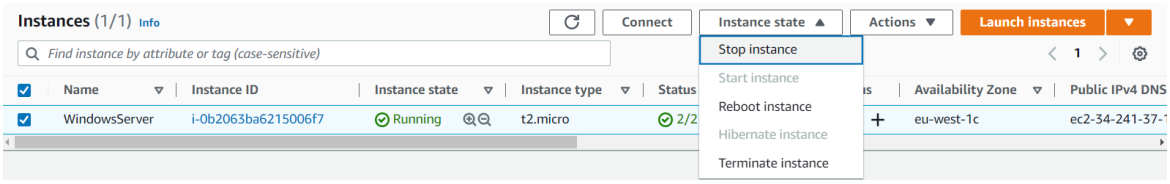



Рис. 3.24. Зупинка екземпляру

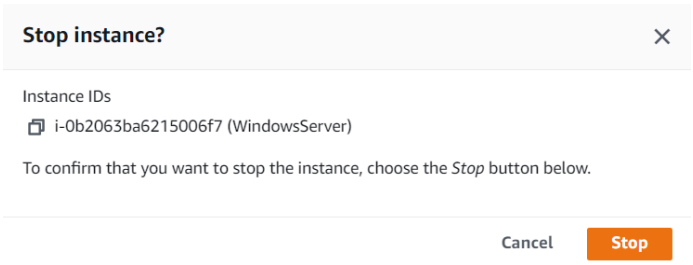



Рис. 3.25. Підтвердження зупинки

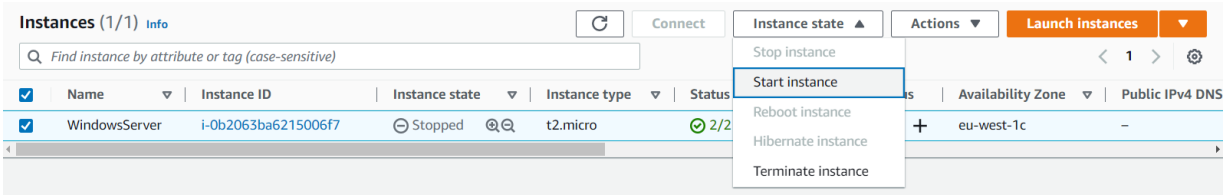



Рис. 3.26. Запуск екземпляру

### 3.3. Експеримент №2: Виявлення та усунення загрози компрометації контейнеру S3 за допомогою GuardDuty

*Сценарій*: Адміністратор безпеки отримав сповіщення про події в GuardDuty - *Stealth:S3/ServerAccessLoggingDisabled* і *Policy:S3/BucketBlockPublicAccessDisabled* (Рис. 3.27).

*Етап 1: розслідування*

Перша подія інформує адміністратора про те, що ведення журналу доступу до сервера S3 вимкнено для контейнеру (Рис. 3.28.). Якщо він вимкнений, не буде вестись запис всіх дій до журналу, виконаних у контейнері S3 або об'єктах в контейнері, якщо не увімкнено запис всіх дій до журналу на рівні об'єкта S3. Незважаючи на те, що це подія незначної серйозності, важливо дослідити, чому були виконані ці дії. Вимкнення запису подій може бути використане для приховування несанкціонованих змін.

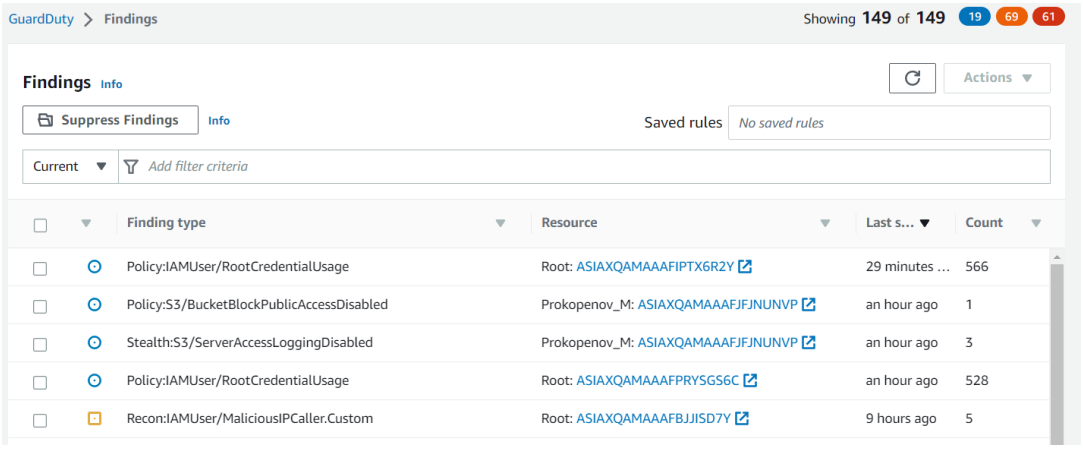



Рис. 3.27. Список подій

Друга (Рис. 3.31.) ж подія інформує, що блокування публічного доступу до контейнеру було вимкнено, що також може сигналізувати про несанкціоновані зміни налаштувань.

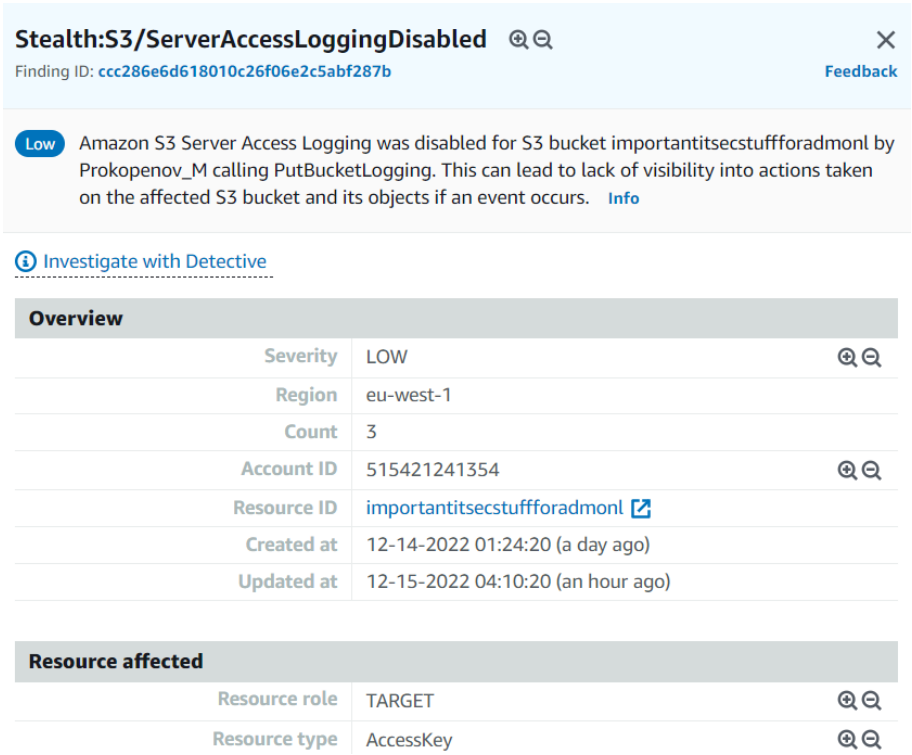



Рис. 3.28. Подія щодо виключення запису подій на доступ до контейнеру

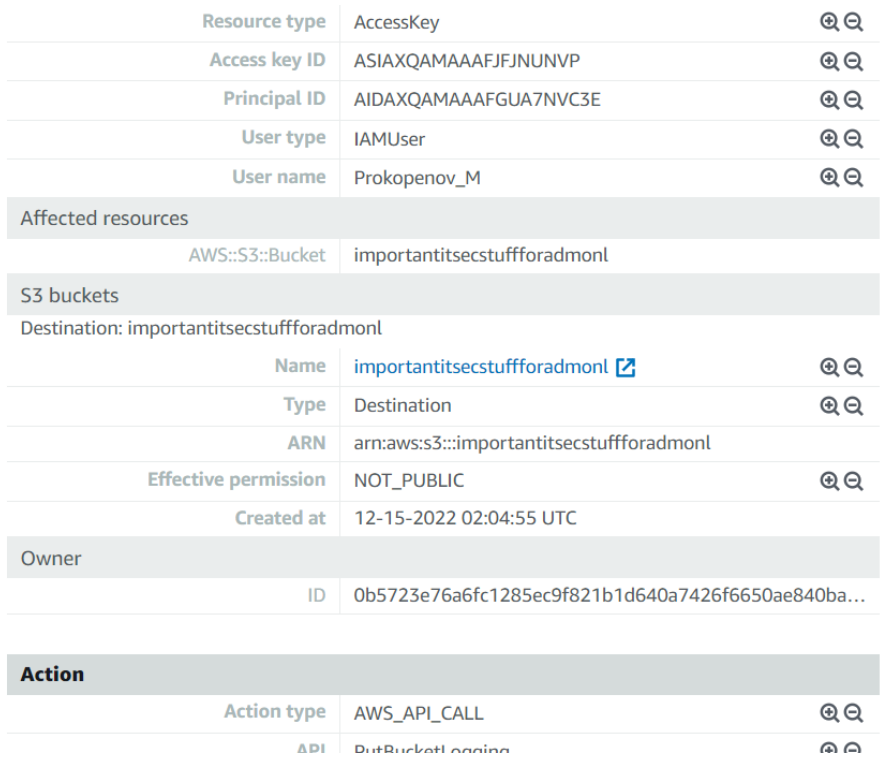



Рис. 3.29. Подія щодо виключення запису подій на доступ до контейнеру

| | |
|---|---|
| Action type | AWS_API_CALL |
| API | PutBucketLogging |
| Service name | s3.amazonaws.com |
| First seen | 12-14-2022 01:18:37 (a day ago) |
| Last seen | 12-15-2022 04:04:29 (an hour ago) |

| **Actor** | |
|---|---|
| Caller type | Remote IP |
| IP address | 93.72.247.84 |
| Location | |
| City | Kyiv |
| Country | Ukraine |
| Lat | 50.458 |
| Lon | 30.5303 |
| Organization | |
| Asn | 25229 |
| Asn org | Volia |
| Isp | Volia |
| Org | Volia |

| **Additional information** | |
|---|---|
| Archived | false |

Рис. 3.30. Подія щодо виключення запису подій на доступ до контейнеру

**Policy:S3/BucketBlockPublicAccessDisabled**

Finding ID: dac289c5ffdb53db142b35930499e510 Feedback

Low Amazon S3 Block Public Access was disabled for S3 bucket importantitsecstuffforadmonl by Prokopenov_M calling PutBucketPublicAccessBlock. If this behavior is not expected, it may indicate a configuration mistake or that your credentials are compromised. Info

Investigate with Detective

| **Overview** | |
|---|---|
| Severity | LOW |
| Region | eu-west-1 |
| Count | 1 |
| Account ID | 515421241354 |
| Resource ID | importantitsecstuffforadmonl |
| Created at | 12-15-2022 04:10:20 (3 hours ago) |
| Updated at | 12-15-2022 04:10:20 (3 hours ago) |

| **Resource affected** | |
|---|---|
| Resource role | TARGET |
| Resource type | AccessKey |

Рис. 3.31. Подія щодо блокування публічного доступу до контейнеру

*Етап 2: реакція*

У вкладці «Services», в категорії «Storage», потрібно перейти до служби S3:

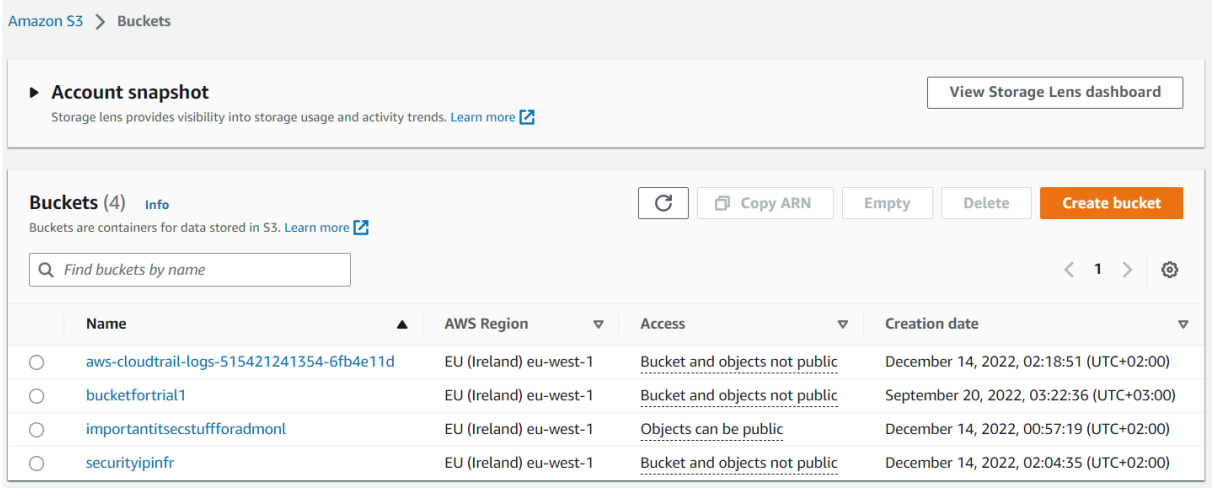



Рис. 3.32. Список контейнерів

В меню «Permission» заблокувати публічний доступ до контейнера:

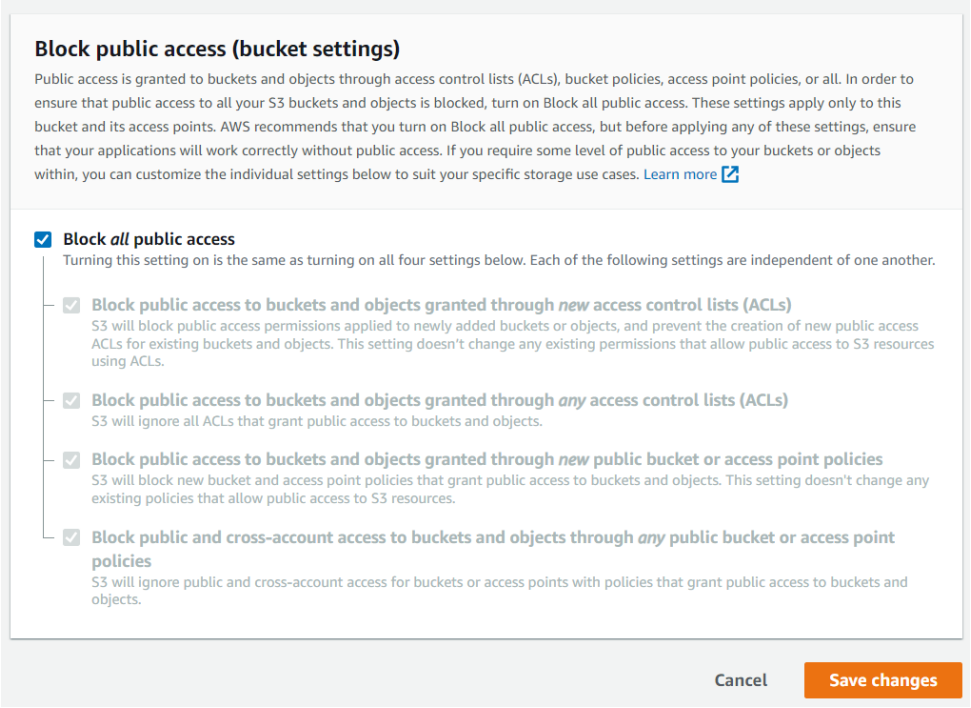



Рис. 3.33. Налаштування публічного доступу

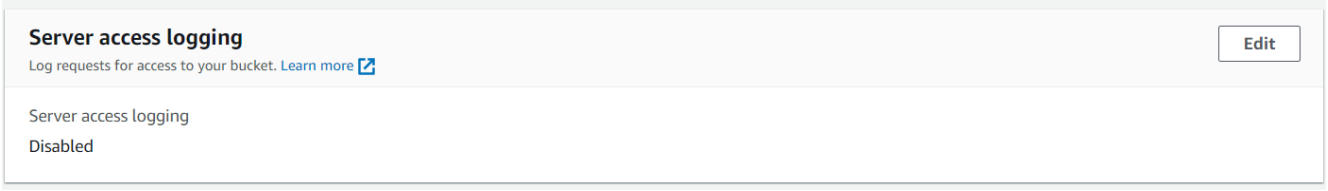



Рис. 3.34. Стан журналу запису подій на доступ

В меню «Properties» необхідно змінити налаштування журналу запису подій на доступ:

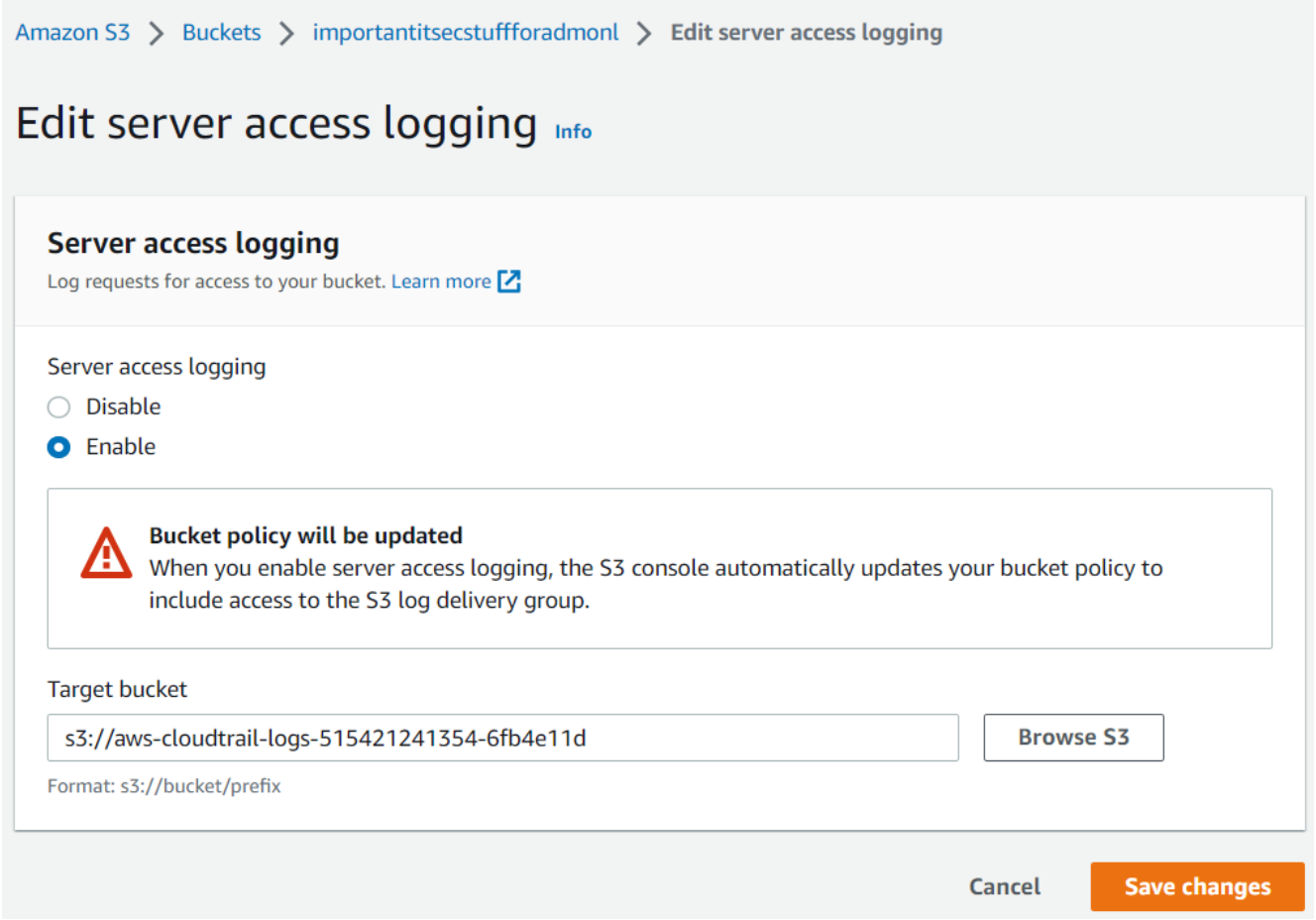



Рис. 3.35. Стан журналу запису подій на доступ

*Етап 3: скасування ключів доступу*

Так як вирішити інцидент необхідно швидко, необхідно прийняти рішення щодо скасування ключа доступу, а після у вкладці «Services», в категорії «Security, Identity, & Compliance», перейти до служби AWS Identity and Access Management (IAM).

Знайти серед користувачів (Рис. 3.36.) потенційно скомпрометований обліковий запис Prokopenov_M та відкрити його властивості. У розділі «Security Credentials» (Рис. 3.37.) деактивувати ключ доступу (Рис. 3.38.).

**Users** (13) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Delete | Add users

Find users by username or access key

1

| User name | Groups | Last activity | MFA | Password age | Active key age |
|---|---|---|---|---|---|
| Alexii_P | GuardDuty | Yesterday | None | Yesterday | Yesterday |
| Bitkyi_R | Sec_Hub | Never | None | Yesterday | Yesterday |
| Kafka_O | Detective | Never | None | Yesterday | Yesterday |
| Karliso_F | Resources_EC2 and EC2_Res_Max | 7 hours ago | None | Yesterday | 4 hours ago |
| Kolovayn_I | IAM | Never | None | Yesterday | Yesterday |
| Lukoi_T | Sec_Hub | Never | None | Yesterday | Yesterday |
| Maxon_B | GuardDuty | Yesterday | None | Yesterday | Yesterday |
| Petko_R | Cloudwatch | Never | None | Yesterday | Yesterday |
| Prokopenov_M | Resources_S3 | 3 hours ago | None | Yesterday | - |

Рис. 3.36. Список користувачів хмарного середовища підприємства

Access keys

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation.
**If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.** Learn more

Create access key

| Access key ID | Created | Last used | Status |
|---|---|---|---|
| AKIAXQAMAAAFGAG43SMC | 2022-12-14 02:49 UTC+0200 | 2022-12-14 06:22 UTC+0200 | Active \| Make inactive |

Рис. 3.37. Список користувачів хмарного середовища підприємства

Deactivate AKIAXQAMAAAFGAG43SMC?

Deactivate access key **AKIAXQAMAAAFGAG43SMC**? You can't use a disabled key to make AWS API calls but you can activate it again later.

Access key last used

2022-12-14 06:22 UTC+0200

IAM user

Prokopenov_M

Account

515421241354

Cancel | Deactivate

Рис. 3.38. Вікно деактивації ключа доступу

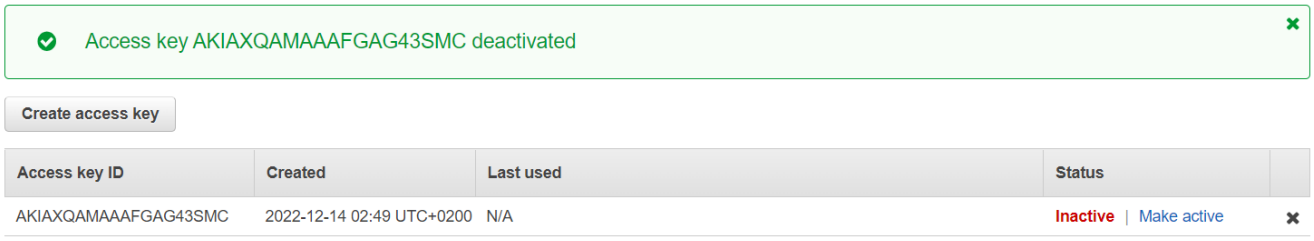



Рис. 3.39. Підтвердження скасованого ключа

## 3.4. Загальні рекомендації щодо виявлення та реагування на загрози в хмарному середовищі підприємства

Дослідивши відгуки, функціональні особливості та результати експериментів, можна запропонувати наступні рекомендації:

Необхідно надавати користувачі лише ті дозволи, які необхідні для його функціональних обов’язків;

Всі користувачі мають використовувати багатофакторну автентифікацію;

На рівні організації включити захист контейнерів S3, що містять чутливу інформацію, щоб GuardDuty та інші сервіси захисту мали можливість відслідковувати будь-яку підозрілу активність відносно цих контейнерів;

Для більшої зручності варто використовувати CloudWatch Events та AWS CloudTrail, щоб отримувати повідомлення щодо подій GuardDuty;

для найефективнішої роботи та захисту хмарного середовища потрібно інтегрувати GuardDuty, Security Hub та Detective.

# ВИСНОВКИ

Підприємства та організації усвідомлюють бізнес-цінність хмари та те, як хмарний (аж до гібридного мультихмарного) підхід стає ключовим компонентом успішної цифрової трансформації, пришвидшення процесів самого бізнесу та миттєвого доступу до інформації. Хоча й існують помітні зміни в тому, як створюються програми та застосунки, як дані керуються, інтегруються та працюють у масштабі – безпека є наскрізною проблемою в усіх цих сферах.

Особливо дані, часто конфіденційні чи секретні, потребують найвищого захисту. Постачальники хмарних послуг розуміють це та намагаються захистити інформацію своїх клієнтів. Для цього використовуються сервіси безпеки, кожен з яких призваний виконувати певну частину роботи по захисту інформації.

Розглянутий у цій роботі сервіс GuardDuty від Amazon є потужним рішенням для захисту хмарної інфраструктури, що легко інтегрується з іншими сервісами захисту для ще вищого рівня захисту.

Позитивними сторонами цієї технології є:

Широкий функціонал;

Зрозумілий інтерфейс;

Можливість початку роботи «з коробки»;

Високий рівень інтеграції з іншими сервісами.

Негативними сторонами цієї технології є:

Взаємозалежність сервісів – без GuardDuty сервіси не будуть отримувати важливу інформацію про виявлені загрози, а без «активних» сервісів GuardDuty це система виявлення;

Відсутність інтеграції зі сторонніми сервісами.

Загалом, в роботі були:

визначена концепція хмари, її призначення та функції; проаналізовані сучасні загрози в хмарі та підходи щодо їх виявлення та реагування;

проаналізуваний ринок рішень хмарних технологій та існуючі рішення щодо виявлення та реагування на сучасні загрози в хмарі;

розглянуті основні сервіси AWS та їх призначення;

досліджено сервіс Amazon GuardDuty;

проведені експерименти для дослідження можливостей Amazon GuardDuty;

на основі функціональних особливостей Amazon GuardDuty, а також результатів експериментів, розроблено загальні рекомендації щодо виявлення та реагування на загрози в хмарному середовищі підприємства.

Рекомендації доцільно використовувати адміністраторам безпеки та іншому персоналу, що займається безпосередньо захистом хмарної інфраструктури, для вибору постачальника основного хмарних послуг та прийняття рішення щодо доцільності використання Amazon GuardDuty.

# ПЕРЕЛІК ПОСИЛАНЬ


1. Про хмарні послуги [Текст]: Закон України № **2075-IX** від 17 лютого 2022 р. / Верховна Рада України / Відомості Верховної Ради України. 2022. Ст. 2.
2. NIST Special Publication 800-145. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology [Електронний ресурс]. Режим доступу: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf
3. Sreekanth Iyer. Hybrid Cloud Security Patterns. Birmingham: Packt Publishing Ltd. 2022. 233 p.
4. CLOUD SECURITY REPORT, 2022 [Електронний ресурс]. Режим доступу: https://www.checkpoint.com/downloads/resources/cloud-security-report-2022.pdf?mkt_tok=NzUwLURRSC01MjgAAAGHxAKdGtY_Va--zTl3n29KzOLQqTWdYsYYpUOvy5VX12A4UQ2nzFCJ2KLWQg6OhTgZxTMZjPmxg5exw79u-sAKAG2Z5HT4H2a5GZREP4wJ9ZYmg8v-
5. Top 15 Cloud Security Issues, Threats and Concerns [Електронний ресурс]. Режим доступу: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/top-cloud-security-issues-threats-and-concerns/
6. What is Cloud Security? [Електронний ресурс]. Режим доступу: https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cloud-security/
7. Threat Detection [Електронний ресурс]. Режим доступу: https://www.rapid7.com/fundamentals/threat-detection/
8. Magic Quadrant for Cloud Infrastructure and Platform Services by Gartner [Електронний ресурс]. Режим доступу: https://www.gartner.com/doc/reprints?id=1-2AOZQAQL&ct=220728&st=sb
9. Huge Cloud Market Still Growing at 34% Per Year [Електронний ресурс]. Режим доступу: https://www.srgresearch.com/articles/huge-cloud-market-is-still-growing-at-34-per-year-amazon-microsoft-and-google-now-account-for-65-of-all-cloud-revenues

10. Amazon Web Services: Overview of Security Processes [Електронний ресурс]. Режим доступу: https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

11. Amazon GuardDuty User Guide [Електронний ресурс]. Режим доступу: https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html

12. AWS Security Blog: How you can use Amazon GuardDuty to detect suspicious activity within your AWS account [Електронний ресурс]. Режим доступу: https://aws.amazon.com/ru/blogs/security/how-you-can-use-amazon-guardduty-to-detect-suspicious-activity-within-your-aws-account/

13. Amazon GuardDuty Security Review [Електронний ресурс]. Режим доступу: https://d1.awsstatic.com/certifications/foregenix_amazon_guardduty_security_review_07-2020.pdf

14. Amazon EKS User Guide [Електронний ресурс]. Режим доступу: https://docs.aws.amazon.com/pdfs/eks/latest/userguide/eks-ug.pdf

15. Aligning to the NIST Cybersecurity Framework in the AWS [Електронний ресурс]. Режим доступу: https://www.slideshare.net/AmazonWebServices/aligning-to-the-nist-cybersecurity-framework-in-the-aws