УДК 004.056

ФРЕЙМВОРК ГОТОВНОСТІ ДО КРИМІНОЛОГІЧНОГО АНАЛІЗУ ІНФРАСТРУКТУРИ В AMAZON WEB SERVICES

Л. С. Курганський[1,a], О. М. Барановський[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

«Фреймворк готовності до кримінологічного аналізу інфраструктури в Amazon Web Services» -— це посібник для організацій щодо підготовки до судових розслідувань у разі інциденту безпеки в їхньому середовищі AWS. Структура окреслює низку кроків для організацій, включаючи визначення критичних активів і потенційних загроз, впровадження належного журналювання та моніторингу, встановлення процедур реагування на інциденти та проведення регулярного тестування та оцінювання. Мета інфраструктури полягає в тому, щоб допомогти організаціям підвищити готовність до криміналістичної експертизи та скоротити час і витрати, пов'язані з реагуванням на інциденти безпеки в середовищі AWS. .

Ключові слова: AWS, хмарні технології, криміналістика

Вступ

Нещодавня революція в галузі хмарних обчислень стала не лише новою парадигмою в інформаційних технологіях, але й викликала великий інтерес до неї як до однієї з найбільш швидкозростаючих і найбільш трансформаційних технологій в історії обчислювальної техніки [1]. Це, у свою чергу, призвело до великої кількості атак, які впливають на хмарні обчислення. Внаслідок чого, виникло багато проблем щодо того, як провести належне цифрове розслідування в хмарних середовищах [1].

1. Причини, проблеми і потреби

Зазвичай, якщо відбувається напад, слід проводити розслідування без необхідності залежати від третьої сторони. Однак у хмарних середовищах цей процес залишається складним, оскільки хмарні провайдери, які мають повну владу над середовищем, контролюють джерела доказів, а споживачі ще не здатні власноруч збирати та зберігати дані до того, як станеться інцидент.

Причини

Головна причина необхідності цифрової криміналістики в хмарі – це стрімкий ріст хмарних сервісів. Даний ріст вагомо збільшив популярність хмарних провайдерів, що сприяло широкому поширенні технології, внаслідок чого, обсяги даних та конфіденційної інформації також значно зросли. І це стало підставою для появи нових злочинів та порушень, які пов'язані з хмарними сервісами.

Сучасні проблеми

Через свої головні властивості -– фізична недостяжність і залежність від провайдера хмарні сервіси влаштовують чимало проблем цифровим криміналістам. Так, перша проблема стосується географічного розташування даних, адже компоненти системи можуть бути розташовані в різних країнах, це унеможливлює фізичний доступ до повної системи.[2] Також, є труднощі з обсягами даними, які постійно зростають, і обробка яких може бути дуже складною та часоємною.[2] З іншого боку, також багато часу може бути витрачено на отримання доступу до компонент систем, що негативно впливає на актуальність даних.[2]

Потреби

Отже, велике збільшення кількості порушень безпеки в хмарних середовищах довело, наскільки гострою є потреба в готовності цифрової криміналістики в хмарних сервісах. Опитування криміналістів показало, що більше 80 відсотків респондентів, висловили необхідність у «процедурі та наборі інструментів для проактивного збору даних, пов'язаних з криміналістикою».[3]

2. Запропоновані рішення

Хоча уже є чимало досліджень про цифрову криміналістику, тематика готовності цифрової криміналістики саме в хмарних середовищах залишається ще мало вивченою. Тому, дане дослідження спрямоване на розробку спеціалізованого інтерфейсу програмного забезпечення (API), щоб допомогти дослідити та покращити технічні фактори, які впливають на

[a]lkurgan55@mail.com

готовність користувачів хмарних технологій до цифрової криміналістики.

Технічні фактори

Технічні фактори описують технологічні аспекти, які впливають на готовність судової експертизи в хмарних середовищах.

• Хмарна інфраструктура:
Підготовка інфраструктури для підтримки цифрової криміналістики розслідування, яка включає мережі, системи та лабораторії.

• Хмарна архітектура:
Архітектура системи має бути розроблено особливим чином, щоб збільшити криміналістичні можливості, результатом яких є отримання цифрових доказів.

• Криміналістичні технології:
Спеціалізоване криміналістичне програмне забезпечення та інструменти, які є життєво важливими, коли доходить до збору доказів.

• Хмарна безпека:
Програми безпеки використовуються в цифрової криміналістики як сигнал тривоги. Таким чином, щоб провести цифрове розслідування, інциденти спочатку повинні бути вчасно виявлені системою моніторингу.

Спеціалізований інтерфейс програмного забезпечення

Спеціалізоване API для цифрової криміналістики на платформі AWS може бути надзвичайно корисним для розробників програмного забезпечення та фахівців з цифрової криміналістики, які працюють з електронними доказами. Адже, цей сервіс спрямований на надання функціоналу, який надає можливість здійснювати операції з обробки даних, аналізувати цифрові сліди, виконувати пошук та фільтрування даних забезпечуючи взаємодію з іншими системами та рішеннями цифрової криміналістики.

Основні функції API

Спеціалізований інтерфейс програмного забезпечення може мати різноманітні функції в залежності від вимог користувачів, а також на базі нього можна розвивати нові процедури і методи. Перш за все, головна функція це отримання даних, які можуть бути використані, як електронні докази. Тому, API має мати методи отримання, фільтрації, обробки та аналізу різноманітних джерел даних. Тому, наявна підтримка для різних типів даних, що використовуються в цифрових доказах, таких як формати файлів, метадані, логи та інше. Це дозволяє криміналістам працювати з різноманітними джерелами електронних доказів та проводити аналіз даних у різних контекстах. Отримавши дані, досить корисно їх візуалізувати. Дана властивість, дозволяє аналізувати та відображати результати обробки електронних доказів у зручному форматі. API може надавати захист конфіденційності даних, пропонуючи інструменти для шифрування даних під час обробки електронних доказів. Крім того, спеціалізоване API може використовувати штучний інтелект та машинне навчання для виявлення шаблонів та аномалій у поведінці системи, що може бути корисним для виявлення злочинної діяльності та своєчасне сповіщення користувачів. Оскільки AWS пропонує широкий спектр інструментів для обробки даних та аналізу, спеціалізоване API для цифрової криміналістики може бути легко інтегрованим з іншими сервісами, що дозволяє створювати складні рішення для обробки електронних доказів у великих обсягах даних.

Подальший розвиток

Спеціалізований інтерфейс програмного забезпечення для цифрової криміналістики може розвиватися у багатьох напрямках в майбутньому. Наприклад, можливості аналізу даних можуть розширюватися за допомогою нових алгоритмів та методів машинного навчання. Це дозволить криміналістам отримувати більш точні та швидкі результати при розслідуванні кримінальних справ. Також, API може стати більш доступним та легко інтегрованим з іншими системами та рішеннями, такими як Google cloud чи Azure. Для забезпечення безпеки та конфіденційності даних, API може розвиватися в напрямку підвищення захисту та шифрування даних, що обробляються. В цілому, розвиток API для цифрової криміналістики може сприяти поліпшенню роботи криміналістів та допомогти в боротьбі з кримінальною діяльністю.

Висновки

У результаті роботи було досліджено сучасний стан цифрової криміналістики в хмарних середовищах, розглянуто поширені проблеми та шляхи їх вирішення. Також, було сформовано загальне бачення фреймворку, реалізація його у вигляді інтерфейсу програмного забезпечення, який може стати потужним інструментом для збору, аналізу та обробки даних, які використовуються у кримінальному розслідуванні, та його подальший розвиток. У майбутньому розвиток API для цифрової криміналістики може забезпечити додаткові можливості аналізу даних, використання нових методів машинного навчання та розширення інтеграцій з іншими системами та технологіями. Отже, готовність до хмарної криміналістики можна ідентифікувати як механізм, спрямований на надання можливості отримати будь-яку інформацію, необхідну для початку та вдалого завершення розслідування.

Перелік використаних джерел

1. Einstein gravity in a nutshell / K. Ruan, J. Carthy, T. Kechadi, M. Crosbie. — 2011.
2. *NIST.* NIST Cloud Computing Forensic Science Challenges // Reviews of Modern Physics. — 2014.
3. Survey on Cloud Forensics and Critical Criteria for Cloud Forensic Capability A Preliminary Analysis / K. Ruan, I. Baggili, J. Carthy, T. Kechadi // ADFSL Conference on Digital Forensics. — 2011.