ВИЯВЛЕННЯ ТА РЕАГУВАННЯ НА ЗАГРОЗИ В ДИНАМІЧНИХ ХМАРНИХ ІНФРАСТРУКТУРАХ

Ворошилов А.О., Заніздра П.Ю., Солоніченко О.О., Талипов І.В., Шевченко І.О.

Кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки,
Україна.

E-mail: anton.voroshylov@nure.ua,
pavlo.zanizdra@nure.ua, oleksii.solonichenko@nure.ua,
ihor.talypov@nure.ua, illia.shevchenko1@nure.ua

Abstract

As organisations migrate to dynamic cloud environments (AWS, Azure, Google Cloud), traditional perimeter-based security tools often fail to provide necessary visibility, creating significant security blind spots. Cloud Detection and Response has emerged as a critical paradigm to address these gaps by offering real-time behavioural monitoring and actionable response capabilities across workloads, identities, and APIs. This article analyses the functional necessity of Cloud Detection and Response, contrasting it with legacy systems like EDR and SIEM. It further explores the core components of effective Cloud Detection and Response solutions – cloud-native telemetry, behavioural analytics, and integrated response mechanisms – and examines their application in mitigating cloud-specific threats such as lateral movement, API abuse, and misconfiguration exploitation in hybrid and multi-cloud architectures.

Виявлення та реагування в хмарі (CDR) надає можливості відстеження та реагування в режимі реального часу у всіх хмарних середовищах. Замість того, щоб покладатися на периметральні інструменти або застарілі методи виявлення, CDR допомагає зрозуміти, що відбувається всередині хмари, від активності робочих навантажень до поведінки ідентичностей, і реагувати до того, як загрози поширяться [1].

При роботі в AWS, Azure або Google Cloud активність у хмарі відрізняється від традиційних IT-середовищ [1], [2]. Присутні короткочасні робочі навантаження, розгалужені API, надмірні дозволи та кілька команд, які запускають нові служби, часто без відома IT-команд або команд безпеки. CDR надає дані про активність у хмарі та контекст, необхідний для розуміння всього цього. За допомогою правильного рішення CDR можна виявляти підозрілу активність, таку як зміни в неправильній конфігурації, незвичайні схеми аутентифікації або підвищення привілеїв, а потім швидко розслідувати та вживати заходів.

Основною метою цього дослідження є визначення та оцінка ролі Cloud Detection and Response (CDR) як важливого рівня в сучасних системах кібербезпеки, демонстрація його здатності усунути прогалини у видимості, виявляти складні загрози, пов'язані з хмарними технологіями, в режимі реального часу та сприяти швидкому реагуванню на інциденти з урахуванням ризиків [3].

Не можна покладатися на інструменти, розроблені для локальних середовищ, щоб захистити хмарну інфраструктуру. Традиційні платформи виявлення та реагування зосереджуються на кінцевих точках, сигнатурах та статичних системах. Але хмарні середовища не є статичними. Вони також не мають чітких меж [4], [5]. Відмінності між CDR та традиційними інструментами:

– CDR vs. EDR (Endpoint Detection and Response, виявлення та реагування на кінцевих точках): EDR забезпечує захист традиційних кінцевих точок (ноутбуків, серверів), але не має видимості хмарних площин управління, безсерверних функцій та взаємодій API, які є основним фокусом CDR;

– CDR vs. SIEM (управління інформацією та подіями безпеки): SIEM агрегує історичні журнали для розслідування після інциденту. На відміну від цього, CDR призначений для виявлення в режимі реального часу та негайного активного реагування;

– CDR vs. CSPM (управління станом безпеки хмари): CSPM обробляє ризики статичної неправильної конфігурації, тоді як CDR виявляє активне використання цих конфігурацій під час виконання ;

– CDR проти XDR (розширене виявлення та реагування): XDR об'єднує дані з різних доменів, таких як кінцеві точки, мережа, хмара тощо. Деякі платформи XDR містять базові функції CDR, але більшість з них не мають глибокої хмарної видимості, яку пропонують автономні платформи CDR.

Аналіз функціональних компонентів. Ефективна система CDR працює шляхом постійного аналізу поведінки в інфраструктурі, ідентифікаційних даних та робочих навантаженнях [5]. Метод вирішення завдань виявлення базується на трьох основних компонентах:

– хмарна телеметрія: збір різноманітних даних безпосередньо від хмарних провайдерів (наприклад, журнали активності Azure, журнали аудиту Kubernetes, записи доступу до API), а не лише на основі стандартних журналів подій;

– виявлення на основі поведінки: вихід за межі статичних сигнатур для використання поведінкового аналізу. Це дозволяє виявляти аномалії, такі як незвичайні шаблони автентифікації, підвищення привілеїв або контейнери, що спілкуються зі зловмисними доменами;

– реакція з урахуванням ризиків: надання можливостей не тільки для оповіщення, але й для дій – ізоляція активів, деактивація скомпрометованих облікових записів або запуск автоматизованих робочих процесів для обмеження «радіусу ураження» атаки.

Використання CDR підтверджується його застосуванням у конкретних сценаріях загроз, пов'язаних із хмарними технологіями [6]:

– бічне переміщення: виявлення зловмисників, які використовують хмарні функції для переміщення між службами, контейнерами або ролями IAM;

– зловживання API та обліковими даними: позначення аномальних моделей викликів API або підозрілих дій при вході, що відхиляються від встановлених базових показників (наприклад, несподівані географічні регіони або часові рамки);

– методології інтеграції: успішне впровадження CDR вимагає інтеграції з управлінням ризиками, щоб визначити пріоритетність сповіщень на основі критичності активів, та управлінням вразливостями, щоб пов'язати спостережуване підозріле поведінку з основними причинами (вразливостями, які можна використати), тим самим оптимізуючи виправлення.

Ці найкращі практики впровадження CDR допоможуть отримати максимальну віддачу від стратегії CDR [7].

1. Визначають хмарні сервіси в організації. Монітонг платформи як послуги (PaaS), інфраструктури як послуги (IaaS) та програмне забезпечення як послуги (SaaS). CDR повинна охоплювати не тільки очевидні активи, а й критично важливі послуги, робочі навантаження, контейнери та постачальників ідентифікації.

2. Надання пріоритету правильній хмарній телеметрії. Журнали подій корисні, але їх недостатньо, тому потрібно витягувати дані з API, площин управління, агентів робочих навантажень та хмарних інструментів, таких як журнали аудиту Kubernetes, щоб виявити поведінку, яку статичні конфігурації можуть пропустити.

3. Приведення логіки виявлення у відповідність із загальними фреймворками, такими як MITRE ATT&CK для хмари, щоб посилатися на тактики та техніки та перевірити, чи платформа вловлює те, що повинна.

4. Зосередження на сповіщеннях. Занадто багато виявлень призводить до шуму та втоми від сповіщень. Налаштування політик, щоб придушити очікувану поведінку та виявити аномалії, що відповідають ризику, такі як використання нових привілеїв, надмірне переміщення даних або зміни в критичній інфраструктурі.

5. Інтеграція CDR в існуючі робочі процеси. Це повинно покращити сценарії реагування на інциденти, а не створювати нові з нуля та закриття циклів за допомогою виправлення.

Виявлення та реагування в хмарі (CDR) – це не додаткова функція, а фундаментальна вимога для забезпечення безпеки сучасних динамічних хмарних інфраструктур. Ця функція усуває критичні прогалини в видимості, які залишають традиційні інструменти, орієнтовані на периметр, забезпечуючи виявлення на основі поведінки в режимі реального часу та інтегровані можливості реагування.

Перетворюючи великі обсяги хмарних сигналів на корисну інформацію, CDR дозволяє командам безпеки працювати зі швидкістю хмари, виявляючи загрози до їх поширення. Майбутня ефективність хмарної безпеки залежить від глибокої інтеграції CDR з більш широкими системами управління вразливістю та ризиками, що змінює позицію організації з реактивного реагування на тривоги до проактивного, усвідомленого ризиків постійного реагування.

В ході виконання роботи проведено аналіз важливості використання Cloud Detection and Response (CDR) в сучасних системах кібербезпеки, демонстрація його здатності усунути прогалини у видимості, виявляти складні загрози, пов'язані з хмарними технологіями, в режимі реального часу та сприяти швидкому реагуванню на інциденти з урахуванням ризиків. Визначено роль CDR, його оперативну сферу застосування на відміну від традиційних засобів безпеки (EDR, SIEM, CSPM, XDR). Проаналізовано конкретні обмеження традиційних методів виявлення в умовах динамічного, безмежного характеру хмарних середовищ. Визначено основні функціональні компоненти, що складають надійне рішення CDR, та критичні випадки використання CDR та найкращі практики для його впровадження в складних гібридних та мультихмарних екосистемах.

*Л*ітература

1. Mathieu, L. (2024), Mastering AWS Security: Strengthen Your Cloud Environment Using AWS Security Features Coupled with Proven Strategies. Germany: Packt Publishing, 370 p.

2. Google Cloud DevOps Engineer: A Comprehensive Guide to Google Cloud DevOps Engineer Certification, (2024). Germani: Cybellium Ltd, 226 p.

3. Shah, M. (2023), Cloud Native Software Security Handbook: Unleash the Power of Cloud Native Tools for Robust Security in Modern Applications. Germany: Packt Publishing, 372 p.

4. Nomani, Q. (2024), Mastering Cloud Security Posture Management (CSPM): Secure Multi-cloud Infrastructure Across AWS, Azure, and Google Cloud Using Proven Techniques. Germany: Packt Publishing. 472 p.

5. Опірський І. Р., Олійник А. В., Василишин С. І. (2025), "Дослідження ефективності XDR рішень для виявлення та усування загроз", Сучасний захист інформації, №2(62). С.141-157. DOI: 10.31673/2409-7292.2025.027390.

6. Радівілова, Т., Кіріченко, Л., Пантєлєєв, В., Мазепа, А. і Білодід, В. (2024), "Аналіз методів автентифікації для вебзастосунків та реалізація вебзастосунку з інтегрованою системою автентифікації", Сучасний стан наукових досліджень та технологій в промисловості, 3(29). С. 76–90. DOI: 10.30837/2522-9818.2024.3.076.

7. Alghawli, A. S. A., Radivilova, T. (2024), "Resilient cloud cluster with DevSecOps security model, automates a data analysis, vulnerability search and risk calculation", Alexandria Engineering Journal, 107. P. 136-149. DOI:10.1016/j.aej.2024.07.036