інфраструктуру для забезпечення конфіденційності даних у транзакціях із збереженням верифікованості та цілісності.

Блоковий шифр «Кипарис» [1] було розроблено з урахуванням вимог до постквантових примітивів. Перевагами алгоритму є висока швидкодія, стійкість до диференціального криптоаналізу, постквантова стійкість [2].

Запропонована схема криптографічного захисту базується на поєднанні симетричного шифрування, постквантових примітивів та децентралізованих технологій для забезпечення цілісності даних.

Нижче описані ключові етапи циклу гібридного шифрування.

1) *Генерація ключа*. Створення випадкового сесійного ключа (256/512 біт залежно від необхідного рівня стійкості) із використанням криптографічно стійкого генератора псевдовипадкових чисел.
2) *Шифрування даних алгоритмом «Кипарис»*. Використання ARX-архітектури алгоритму забезпечує високу швидкість обробки на пристроях з обмеженими ресурсами та мінімальну затримку.
3) *Інкапсуляція ключа*. Захист сесійного ключа публічним ключем отримувача за допомогою PQC-алгоритму (на базі решіток, наприклад, ML-KEM). Це гарантує стійкість до квантового криптоаналізу (алгоритм Шора).
4) *Розподілене зберігання*. Розміщення гешу шифротексту, посилання та зашифрованого сесійного ключа в блокчейні, а шифротексту – в off-chain сховищі (IPFS) для оптимізації навантаження на мережу. Отримувач, завантаживши дані з IPFS, порівнює їхній геш із записом у блокчейні.

Інтеграція «Кипарису» в архітектуру децентралізованої обробки транзакцій створює надійний рівень захисту приватних даних, дозволяючи реалізувати механізми вибіркового доступу та гарантувати конфіденційність.

1. Andrushkevych A., et al. A prospective lightweight block cipher for green IT engineering. *Green IT Engineering: Social, Business and Industrial Applications*. Cham: Springer International Publishing. – 2018. – P. 95-112.
2. Родінко, Марія Юріївна. Методи побудови та дослідження властивостей малоресурсних блокових шифрів та їх компонентів : дисертація ... доктора філософії за спеціальністю 122 – комп'ютерні науки (12 – Інформаційні технології). – Харків : Харківський національний університет імені В. Н. Каразіна, 2020. – 201 с.

Автоматизація реагування на інциденти у мультихмарних середовищах засобами SOAR-платформ: проблеми крос-хмарної інтеграції

УДК 004.056.5

Марценюк Є. В. [1]

Національний університет «Львівська політехніка»,
[1]yevhenii.v.martseniuk@lpnu.ua

Дедалі частіше корпоративні інфраструктури розгортаються у форматі мультихмарних середовищ, що поєднують ресурси Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP). За даними аналітичної компанії Flexera, понад 87% підприємств використовують більш ніж одного хмарного провайдера [1]. Розподілена природа таких середовищ суттєво ускладнює процеси виявлення та реагування на інциденти інформаційної безпеки. Платформи Security Orchestration, Automation and Response (SOAR) є визнаним інструментом автоматизації операцій безпеки, проте їх ефективне застосування у мультихмарних конфігураціях стикається з низкою структурних обмежень, зумовлених гетерогенністю хмарних екосистем.

Зокрема, кожен хмарний провайдер реалізує власну модель подій безпеки, власний формат телеметрії та індивідуальні механізми управління доступом: AWS використовує CloudTrail та Security Hub з форматом ASFF (Amazon Security Finding Format), Azure — Microsoft Sentinel із власною схемою подій, а GCP — Security Command Center на базі CSCC API [2]. Відсутність уніфікованого стандарту обміну даними призводить до семантичних розривів при агрегації сигналів та спричиняє збої автоматизованих playbooks у крос-хмарних сценаріях. З огляду на зростання кількості атак на мультихмарні інфраструктури, зокрема атак типу cloud-hopping та credential harvesting, дослідження механізмів подолання зазначених обмежень набуває критичного практичного значення.

Метою роботи є аналіз архітектурних та операційних обмежень, що перешкоджають ефективній автоматизації реагування на інциденти у мультихмарних середовищах засобами SOAR-платформ, а також розроблення підходів до нормалізації подій безпеки та уніфікації механізмів інтеграції з API хмарних провайдерів.

Дослідження базується на порівняльному аналізі архітектур провідних SOAR-платформ — Splunk SOAR, Palo Alto XSOAR та IBM Security QRadar SOAR — у контексті їх інтеграції з нативними інструментами безпеки AWS, Azure та GCP. Застосовано метод структурного аналізу API-інтерфейсів та форматів подій безпеки (ASFF, Microsoft Graph Security API, GCP Security Command Center API) з метою ідентифікації семантичних та синтаксичних розривів. Для оцінки ефективності реагування використовується методологія PICERL (Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned) відповідно до рекомендацій NIST SP 800-61r2 [3]. Практична частина включає розроблення та верифікацію нормалізаційних схем (field mapping) для приведення різнорідних форматів подій до уніфікованого внутрішнього представлення на основі OCSF (Open Cybersecurity Schema Framework) [4].

У ході дослідження ідентифіковано три категорії обмежень крос-хмарної автоматизації SOAR. По-перше, структурні обмеження, зумовлені несумісністю схем подій: поля severity, asset_id та resource_type мають відмінну семантику в ASFF, Microsoft Sentinel та GCP CSCC, що ускладнює уніфіковану кореляцію. По-друге, операційні обмеження, пов'язані з різними моделями аутентифікації та авторизації: AWS IAM Roles, Azure Service Principals та GCP Service Accounts вимагають окремих конфігурацій доступу для кожного playbook-коннектора. По-третє, темпоральні обмеження: затримки надходження телеметрії з різних

хмарних провайдерів варіюються від 30 секунд до декількох хвилин, що критично впливає на автоматичне зіставлення подій при розслідуванні крос-хмарних ланцюжків атак.

Висновки та практична значущість. Розроблена нормалізаційна схема на базі OCSF дозволяє скоротити кількість помилкових спрацювань автоматизованих playbooks на 34% у порівнянні з конфігурацією без нормалізації, що підтверджено тестовим розгортанням у лабораторному мультихмарному середовищі. Впровадження централізованого Identity Broker-шару для управління доступом між SOAR-платформою та API провайдерів скорочує час конфігурації нових інтеграцій у середньому на 60%.

Таблиця 1

Порівняння механізмів інтеграції SOAR з API хмарних провайдерів

Характеристика	AWS	Microsoft Azure	Google Cloud
Нативний SIEM/SOAR	Security Hub + GuardDuty	Microsoft Sentinel	Security Command Center
Формат подій	ASFF	Microsoft Graph Security API	CSCC API (JSON/gRPC)
Модель доступу	IAM Roles + STS	Service Principals (Entra ID)	Service Accounts + Workload Identity
Затримка телеметрії	~30–90 сек	~60–120 сек	~30–60 сек
Підтримка OCSF	Часткова (Preview)	Відсутня (власна схема)	Відсутня (власна схема)
Інтеграція SOAR (оцінка)	Висока	Висока	Середня

1. Flexera 2024 State of the Cloud Report. Flexera Software LLC, 2024. URL: https://www.flexera.com/blog/cloud/cloud-computing-trends-flexera-2024-state-of-the-cloud-report/
2. Kindervag J., McDonald K. Cloud-Native Security Guide: AWS, Azure, and GCP Security Services Comparison. Palo Alto Networks, 2023. 68 p.
3. Cichonski P., Millar T., Grance T., Scarfone K. Computer Security Incident Handling Guide. NIST Special Publication 800-61 Revision 2. NIST, 2012. 79 p.
4. Open Cybersecurity Schema Framework (OCSF) Specification v1.1. OCSF Project Contributors, 2023. URL: https://schema.ocsf.io/

AHP-підхід в управлінні інформаційною безпекою

УДК 004.056:519.816

Наталія Маслова[1,2], Р. Ткачук[1], Олена Любименко[2]

[1]Львівський державний університет безпеки життєдіяльності,
[2]Донецький національний технічний університет,
masgpp2@gmail.com, rlvtk@ukr.net, olena.liubymenko@donntu.edu.ua

У сучасних умовах цифрової трансформації та постійного зростання кількості кіберзагроз особливого значення набуває ефективне управління