УДК 004.056
DOI: 10.31673/2409-7292.2022.040006

Захаржевський А.Г., Голобородько С.О., Захаренков А.О.

ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ХМАРНОГО СЕРЕДОВИЩА НА БАЗІ РІШЕННЯ CISCO CLOUDLOCK

У статті проаналізовано методи та засоби забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock. Розглянуто призначення, основні функції та склад програмного комплексу Cisco Cloudlock. За рахунок сучасних алгоритмів, з'являється можливість на початку розпізнати аномалії поведінки та попередити можливу кібератаку.

Ключові слова: Cisco Cloudlock, кібербезпека, кібератака, аномалія поведінки користувача.

Вступ

Захист хмарного середовища є обов'язковою складовою забезпечення кіберзахисту у корпоративному сегменті. На сьогоднішній день класичні методи до захисту даних у хмарному середовищі вже не забезпечують належний рівень захисту від сучасних кіберзагроз. Інтеграція системи контролю та безпеки даних у хмарному середовищі дозволяє проводити моніторинг подій та вчасно ліквідувати загрози безпеки всередині та поза межами хмарного середовища. Крім несанкціонованого витоку конфіденційної інформації існують інші види інформаційних загроз, які націлені на часткове або повне зупинення робочих процесів в компанії, блокування оперативного доступу до належних зовнішніх та внутрішніх інформаційних ресурсів, погіршення продуктивності хмарної інфраструктури або її повне зупинення тощо.

Комплексний підхід до захисту даних в хмарному середовищі побудований на конфіденційності, цілісності та доступності. Саме тому компанія Cisco створила брокер безпеки доступу до хмарного середовища (CASB, Cloud Access Security Broker), що забезпечує кібербезпеку в хмарній системі на найвищому рівні. Саме тому, для дослідження була обрана технологія на базі рішення саме цієї компанії.

Аналіз публікацій

Cisco – широко відомий бренд IT-корпорації Cisco Systems з США під яким у всьому світі випускаються мережеві маршрутизатори, комутатори, бездротові пристрої, системи відеонагляду. Діяльність компанії постійно масштабується та охоплює все більше і більше нових областей IT-галузі.

Cisco пропонує системи безпеки, телефонію на базі Інтернету, хмарні системи та інші рішення для спільної роботи і корпоративних мереж. Також компанія бере участь у розвитку Інтернету речей (IoT), проводить освітні програми і пропонує одну з багаторівневих і ретельних систем сертифікації інженерів комунікаційних технологій.

Компанія Cisco Systems [1], визнаний лідер в області мережевих рішень, пропонує також широкий вибір продуктів в області забезпечення інформаційної безпеки - від міжмережевих екранів і систем запобігання атак до засобів контролю вмісту, захисту різних додатків, систем індивідуального захисту серверів.

У кожній з цих областей компанія Cisco Systems [2] досягла результатів і займає перші місця на світовому ринку. Це було б неможливо без досліджень і розробок, на які щорічно витрачається близько 500 мільйонів доларів - більше, ніж заробляють в рік деякі інші постачальники ринку інформаційної безпеки. Визначальним елементом стратегії хмарного провайдера має бути повне виконання нормативних вимог, це дозволить підвищити рівень безпеки і сконцентрувати ресурси на конкретних проектах з підвищення захищеності. Класичні заходи з управління ризиками будуть ефективні тільки з ростом бізнесу хмарного провайдера, коли управління ризиками буде направлено як на вибір контрзаходів і оптимізацію витрат, так і на підвищення прозорості бізнес-інфраструктури.

З технологічної точки зору захист хмарного провайдера в цілому схожа на захист віртуалізації в корпоративній сегменті, при цьому бажано використовувати практики вже побудованих систем. Наприклад, в загальнодоступних документах Amazon 200 сторінках

[3] наводяться кращі приклади побудови захищеної інфраструктури, в тому числі класичні: сегментування мережі, відділення хмарної інфраструктури від мережі внутрішньої діяльності провайдера (кадрів, бухгалтерії і т.п.).

З точки зору забезпечення безпеки, хмари це лише один з різновидів інфраструктурних платформ, нехай навіть з високим ступенем автоматизації. Зрозуміло, що в хмарі не обійтися без процесів, які добре зарекомендували себе в традиційних фізичних системах. Такі основні функції, як міжмережевий екран, IDS/IPS, віртуальне закриття вразливостей (Virtual Patching) та антивіруси, є обов'язковими елементами будь-якої концепції безпеки, будь то фізичні, віртуальні або хмарні системи. А ось завдання, що виникають при управлінні цими функціями, в різних інфраструктурах відрізняються [4].

Необхідно, щоб всі сервери з локальних, внутрішніх або зовнішніх хмар були ідентифіковані і інтегровані в концепцію управління безпекою. При використанні хмарних сервісів цього можна домогтися за допомогою прямої інтеграції з брокером хмарних сервісів, який в будь-який момент може надати інформацію про наявність різних хмарних серверів. Зіставляти вручну параметри експлуатованих серверів до вимог систем безпеки в динамічних середовищах неможливо, а при спробах такого порівняння виникають численні помилки.

Мета статті – розглянути особливості застосування технології забезпечення кібербезпеки хмарного середовища базі рішення Cisco Cloudlock.

Реалізація технології забезпечення кібербезпеки хмарного середовища в рішенні Cisco Cloudlock

Cisco Cloudlock - спеціальне рішення для хмари для безпечного доступу до такого середовища. Брокер дозволяє безпечно проводити операції в хмарі. Cisco Cloudlock націлений на захист користувачів, даних і додатків в хмарі. Надає можливість створити колективний рейтинг довіри для додатків і внесення їх в білий або чорний список в залежності від рівня потенційного ризику.

Типові рішення платформи Cloudlock CASB безпеки працюють шляхом захисту периметра мережі, захисту трафіку в мережі і управління мобільні пристрої. Ці рішення важливо мати, але у них є сліпа пляма: хмарні додатки, які з'єднуються з локальними програмами та даними, а також з іншими хмарними додатками. Некеровані користувачі, пристрої та мережі створювати уразливості, які ці рішення не бачать.

Cloudlock автоматично виявляє хмарні додатки, підключені до вашої середовищі, забезпечуючи видимість того, що додатки, до яких підключені користувачі, і то, як вони використовують і обмінюються даними. Це допомагає організаціям контролювати додатки за допомогою класифікація і моніторинг дій та відкликання доступу при необхідності.

Cloudlock відстежує всі дії користувачів, які відбуваються в будь-якому виявленому хмарному додатку і підключається до загальнодоступних API кожної хмарної платформи. Коли користувач завантажує файл в Dropbox [5], наприклад, Dropbox записує цю подію і передає його Cloudlock через API; Cloudlock потім може сканувати контент за допомогою попередньо налаштованого механізму класифікації, оцінити його в контексті налаштованих політик, визначити, порушення, і негайно відреагувати, зашифрувати їх або помістити файл в карантин. Також інтеграція з іншими інструментами дозволяє проводити детальну експертизу після атаки. Cloudlock відстежує дії керованих і некерованих користувачів, пристроїв і мереж.

Хоча багато хмарних додатків пропонують засоби управління безпекою, вони не можуть забезпечити цілісне уявлення про всі додатки з сторона користувача; наприклад, Google і Dropbox можуть відображати дії користувачів, але IT-адміністратори не можуть зіставити інформацію між ними, а тим більше в тисячах додатків, які сьогодні використовує більшість організацій.

Cloudlock забезпечує цілісний погляд, це відкрите рішення, легко інтегральне з існуючими рішеннями мережевої безпеки, SIEM, EMM і IAM (рис. 1), воно може також використовувати журнали інших CASB, щоб розширити видимість. На відміну від рішень

CASB (рис. 2) на основі шлюзів, Cloudlock не встає між користувачами і їх хмарними додатками. Він знаходиться в AWS, поряд з іншими хмарними додатками, відстежує дані в режимі реального часу і в стані спокою.

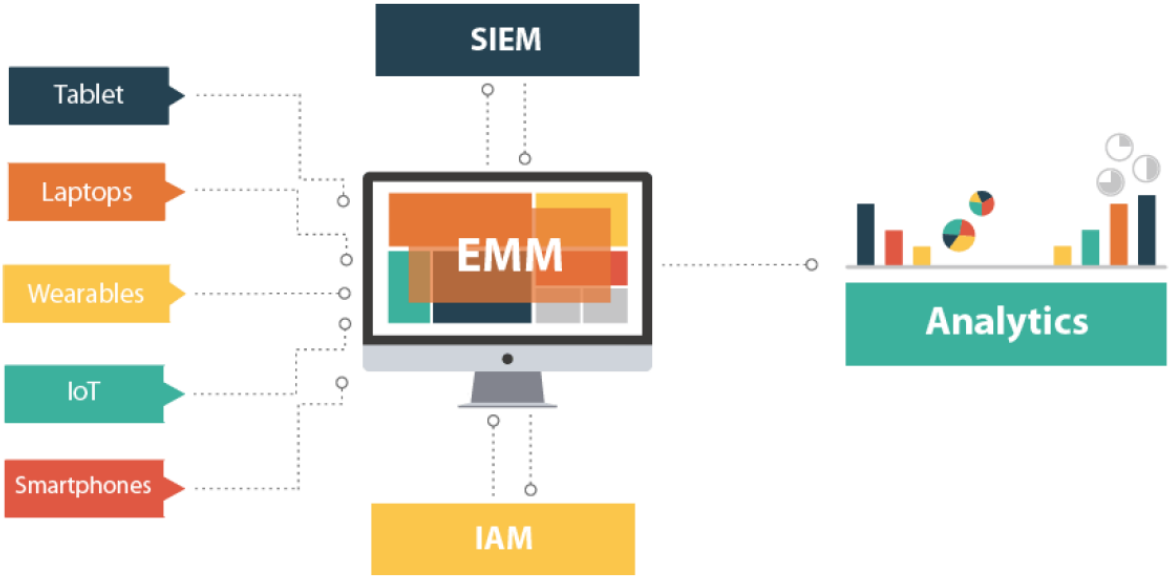

Рис. 1. Існуючі рішення безпеки, що інтегруються з Cloudlock

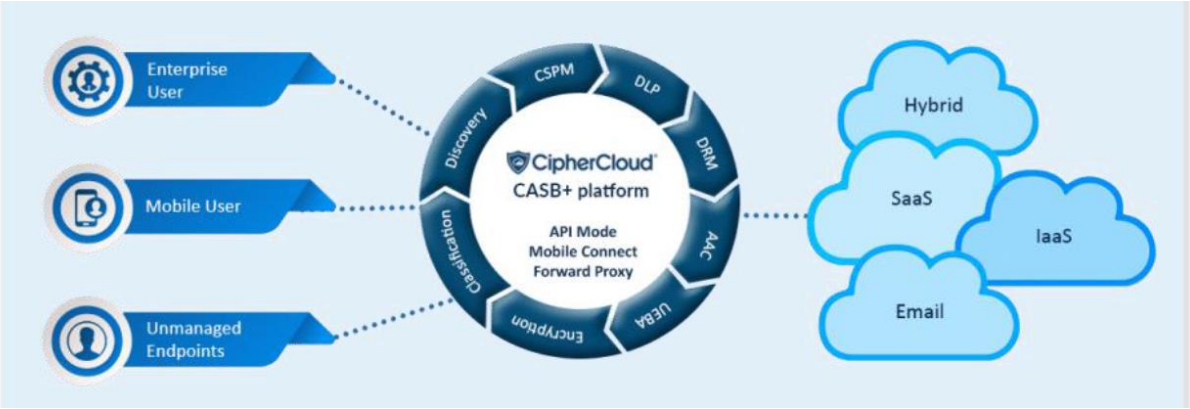

Рис. 2. Схема роботи CASB

В результаті дії Cloudlock не впливають на продуктивність або масштабованість так само, як проксі або шлюзи. Це також дозволяє нове розгортання Cloudlock забезпечити видимість того, які дані використовувалися і як вони передавалися в минулому, а не тільки з моменту розгортання, як з CASB (рис. 3), не заснованими на API.

Cloudlock налаштовується швидко і легко, не відволікаючи користувачів. Він складається з набору мікросервісів, наприклад для даних, класифікації або захисту від загроз. Мікросервіси доступні через призначений для користувача інтерфейс Cloudlock або через API для інших продуктів. Програмне забезпечення поставляється з більш ніж 80 зумовленими політиками, які можна налаштувати в міру необхідності, наприклад, для визначення рівня чутливості, підходяща близькість даних, розкриття даних або політики по відділах.

Наприклад, організація може дозволити хмарним додаткам зберігати один номер кредитної картки, але ідентифікація сотень з них може викликати попередження і дії. Деталізовані політики можна створювати і розгортати в кількох хмарних додатках, позбавляючи адміністраторів від необхідності налаштовувати індивідуальні політики згідно з додатками.

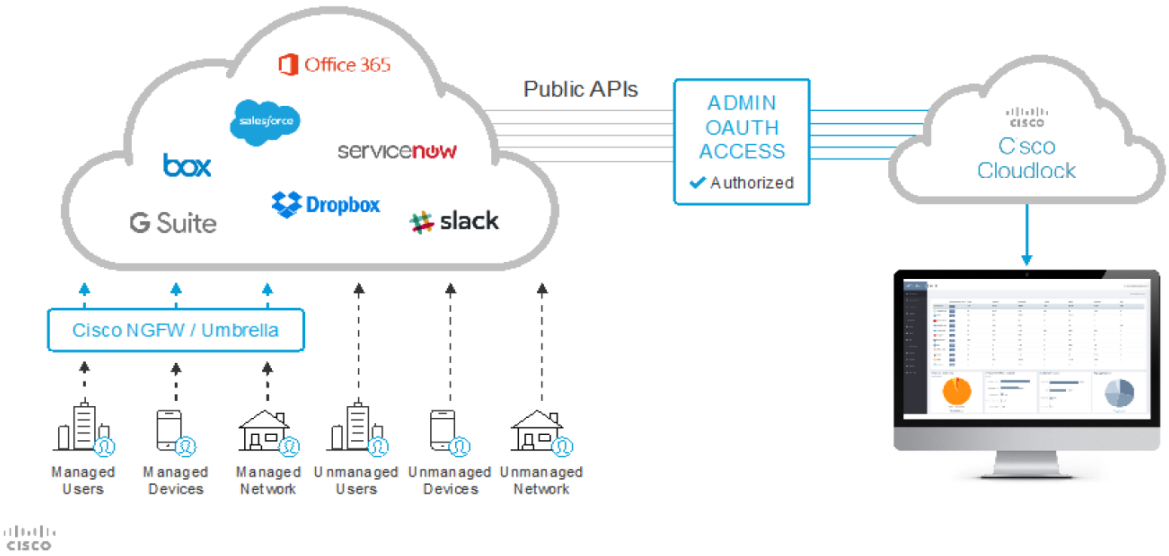

Рис. 3. CASB – API Access (хмара - хмара)

Політики можуть застосовуватися до користувачів індивідуально або в групах в залежності від поведінки, місця розташування та IP-адреси. Cloudlock відстежує дії користувачів і може переглядати журнали Office 365, Google, Dropbox, Box, Salesforce або інших хмарних додатків через API [6].

Можна створити політики, які будуть діяти автоматично при виникненні подій, наприклад, автоматичний відгук токен OAuth і відключення з'єднання для заборонених додатків або автоматичне шифрування і приміщення в карантин даних, таких як коли номер кредитної картки додається там, де його бути не повинно.

ESG Lab провела практичну оцінку функцій безпеки додатків Cloudlock за допомогою демонстраційної середовища. тестування зосереджені на простоті використання, наочності і захисту підключених хмарних додатків. Середовище включає хмарні додатки для спільної роботи / продуктивності (Office 365, Slack), обміну файлами (Dropbox, Box), хмарного сховища (Google Drive, AWS), CRM (Salesforce), управління IT-послугами (ServiceNow) і ідентифікація / єдиний вхід (OneLogin, Okta).

Налаштування Cloudlock відбувається в рамках вже розгорнутого середовища Cloudlock, тому ESG Lab почала вивчення варіантів конфігурації. На вкладці «Налаштування» ESG Lab можна легко управляти платформами, шифрувати файли, додавати і видаляти користувачів і ролі, управляти інтеграцією з іншими додатками, такими як безпека Cisco Umbrella DNS, а також керувати логінами SSO і токенами API (рис. 4).

Наприклад, Cloudlock може відстежувати всі або вибрані домени Google і організаційні одиниці (OU), певні сегменти AWS S3, канали Slack і домени Office 365, Box і Dropbox. Панель управління Cloudlock пропонує високорівневе уявлення про те, що відстежує Cloudlock: поведінка, дані і додатки. Кожна вкладка включає в себе звіт верхнього рівня з чотирма ключовими статистичними даними за минулий тиждень, які можуть вказувати на порушення або витік даних. Ці зведені вкладки об'єднують деталі, які також можна переглянути на вкладках меню зліва. Вони можуть відразу попередити адміністраторів про потенційно небезпечному доступі до середовища.

Кожна вкладка включає додаткові докладні відомості та діаграми, що зв'язують аномальні дії з рівнями ризику, хмарними додатками, користувачами і місцями розташування. За необхідності можна досліджувати поведінкові тенденції (Data Risk), які включають діаграми і графіки, що показують лінії тенденцій, схильність активів в залежності від хмарної платформи та місцезнаходження, а також докладну інформацію про активність активів і завантаження по користувачах.

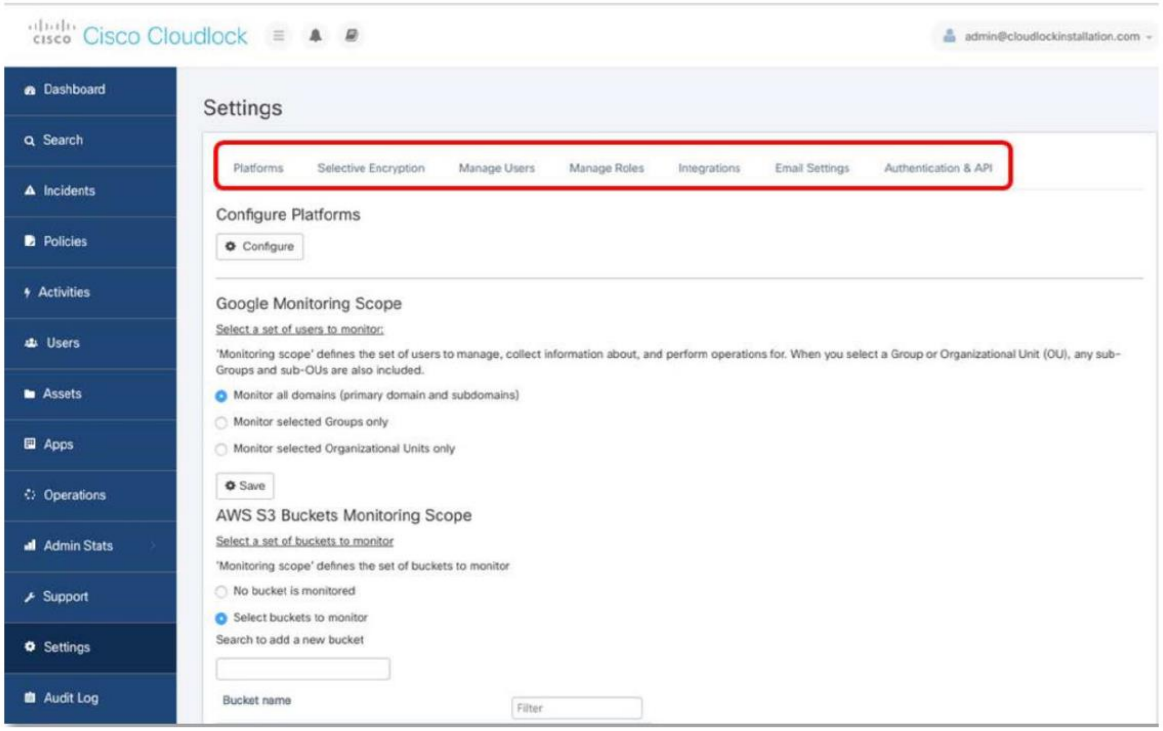

Рис. 4. Інтерфейс налаштувань Cloudlock

На панелі управління ризиками додатків показані важливі деталі для оцінки рівнів ризику хмарних додатків. У лівому верхньому кутку знаходиться список розгорнутих додатків з найбільшим ризиком, включаючи кількість користувачів і рейтинг ризику, який створюється на основі комбінації рейтингів CTR, аналізу Cyberlab, категорії додатки і ризику області доступу.

Області доступу визначають, до яких даних додаток може отримати доступ у призначених для користувача середовищах, наприклад повні дані, контакти і можливість діяти від імені користувача. Визначення областей доступу може додати екстрені заходи захисту.

Вгорі праворуч гістограма відстежує кількість додатків в кожній категорії ризику; при натисканні на панель високого ризику (нижче) відкриваються додаткові відомості про додатки з високим рівнем ризику за датою, а також відомості про кожного додатку, включеному в категорію. Клацання по назві додатка надає списки всіх подій додатки, користувачів і областей доступу, а натискання на кнопку «Впорядкувати» дозволяє рекласифікувати додаток (рис. 5).

Адміністратори можуть легко і швидко побачити, до якої інформації має доступ кожен додаток, в стовпці Області доступу. Наприклад, ESG Lab переглянула області доступу DocuSign до додатка, підключеному до OAuth, включаючи доступ до основної інформації, повний доступ до даних, обмежений доступ до даних і файлів, а також можливість управляти діями користувачів. Ці області доступу можуть викликати проблеми при зловмисному використанні, що є основною причиною того, що це додаток класифікується як додаток з високим ризиком.

Остання панель інструментів Policies & Incidents. У списку вказані всі хмарні платформи, а також оцінка безпеки і кількість користувачів цієї платформи; об'єкти; інциденти; критичні проблеми; оповіщення; та ін. Графік інцидентів за серйозністю можна фільтрувати по хмарній платформі; клацання по круговій діаграмі дозволяє адміністраторам переглядати інциденти, засновані на порушенні політики безпеки. Таким чином, інтерфейс Cloudlock дозволяє швидко визначати загрози та потенційно можливі заходи щодо реагування та такі загрози.

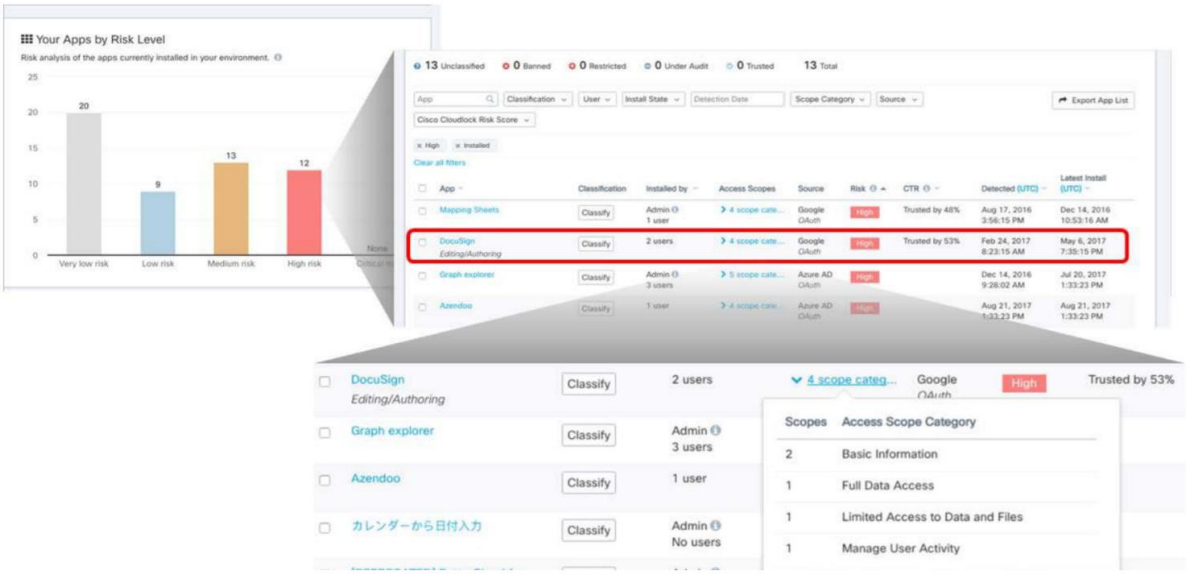

Рис. 5. Інтерфейс функціоналу Cloudlock

Висновки

Cisco Cloudlock захищає хмарні ідентифікатори, дані та додатки, забезпечує відповідність вимогам політики безпеки та підвищує ефективність. Це відкрите та автоматизоване рішення, яке створюється з урахуванням хмарних навчальних записів, використання даних та ризиків екосистеми програм, що надає діючі аналітичні дані про кібербезпеку.

Низка функцій, що пропонує Cisco Cloudlock є корисними та важливими для фахівців кібербезпеки для забезпечення захисту хмарного середовища. Воно забезпечує крос-платформну аналітику поведінки користувачів та суб'єктів (UEBA) для SaaS, середовища IaaS, PaaS та IDaaS. Також, Cisco Cloudlock використовує вдосконалене машинне навчання, алгоритми виявлення аномалій на основі таких факторів, як діяльність поза білим списком країни та дії на відстані з неможливою швидкістю.

Перелік посилань

1. U.S. Companies View Cloud Computing as Key to Improved Data Protection [Електронний ресурс]. - Режим доступу: http://investor.ca.com/releasedetail.cfm?releaseid=674043

2. Cloud Computing. Benefits, risks and recommendations for information security. European Network and Information Security Agency (ENISA). November, 2009. [Електронний ресурс]. - Режим доступу: http://www.enisa.europa.eu/activities/risk-management/files/deliverable

3. Commission proposes a comprehensive reform of the data protection rules. Правовий портал Європейської Комісії. [Електронний ресурс]. - Режим доступу: http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

4. Working Paper on Cloud Computing Privacy and Data Protection Issues (“Sopot Memorandum”). / International Working Group on Data Protection in Telecommunications. 51st meeting, 23-24 April 2012, Sopot (Poland) [Електронний ресурс]. - Режим доступу: http://www.datenschutz-berlin.de/content/europa-international/internati

5. Колісник Д. Р., Місевич К. С., Коваленко С. В. Системна архітектура IoT-Fog-Cloud для систем аналізу великих даних і кібербезпеки: огляд туманних обчислень, впровадження аудиту інтернету речей // [Електронний ресурс]. – Науковий журнал «Сучасний захист інформації». – Київ, ДУТ. – с. 34-38 Режим доступу : World Wide Web. – URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/2442.

6. Місевіч К.С. Технологія забезпечення кібербезпеки хмарного середовища на базі рішення Cisco Cloudlock // [Електронний ресурс]. – Збірник матеріалів XIII Науково-практична конференція. – Київ, ВІТІ, - с. 195 Режим доступу : World Wide Web. – URL: http://www.viti.edu.ua/files/zbk/2020/c_2020.pdf .

Надійшла: 22.11.2022 Рецензент: д.т.н., професор Вишнівський В.В.