УДК 004.056.5:004.7

Бугай Олександр Анатолійович,

здобувач другого (магістерського) рівня вищої освіти
Харківського національного університету радіоелектроніки

Балагура Дмитро Сергійович,

к.т.н., доцент доцент кафедри безпеки інформаційних технологій
Харківського національного університету радіоелектроніки

АВТОМАТИЗОВАНЕ ВИЯВЛЕННЯ ШКІДЛИВИХ ОБ'ЄКТІВ У AMAZON S3 НА ОСНОВІ ІНТЕГРАЦІЇ SHUFFLE SOAR ТА YARA

Анотація. Запропоновано подієво-орієнтовану архітектуру виявлення потенційно шкідливих об'єктів у хмарному сховищі Amazon S3. Розглянуто інтеграцію сповіщень Amazon S3, функцій AWS Lambda, платформи оркестрації Shuffle SOAR та правил YARA. Описано алгоритм від надходження файла до перевірки його вмісту, формування рішення про ізоляцію й передавання сповіщення фахівцю з кібербезпеки. Показано особливості організації автоматизованого сценарію та необхідність контролю повторних подій, прав доступу й хибних спрацювань. Практичне моделювання демонструє функціональну узгодженість компонентів, але не є вимірюванням точності детектування. Запропонований підхід може використовуватися як основа для автоматизації первинного аналізу об'єктів хмарного сховища.

Ключові слова: хмарна безпека, Amazon S3, AWS Lambda, Shuffle SOAR, YARA, шкідливе програмне забезпечення, автоматизація реагування.

Використання об'єктних хмарних сховищ спрощує обмін файлами, але створює ризик потрапляння до корпоративних інформаційних систем шкідливих вкладень та заражених архівів. Сам факт розміщення такого об'єкта в Amazon S3 не означає виконання шкідливого коду, небезпека виникає під час подальшого завантаження, відкриття або оброблення файлу. Тому важливим завданням є автоматична перевірка нових об'єктів до їх використання та узгоджене реагування на результати аналізу.

Мета публікації полягає в обґрунтуванні й описі подієво-орієнтованого процесу виявлення потенційно шкідливих об'єктів Amazon S3 шляхом інтеграції засобів перевірки вмісту файлів із платформою автоматизації реагування Shuffle SOAR.

Архітектура процесу складається з чотирьох основних компонентів. Amazon S3 зберігає файли та формує подію про створення об'єкта; AWS

Lambda приймає цю подію й передає відомості про об’єкт через HTTP webhook; Shuffle SOAR керує послідовністю автоматизованих дій, YARA здійснює пошук визначених бінарних або текстових шаблонів у вмісті файла [1]. Механізми workflow та webhook підтримуються платформою Shuffle [2]. Правила YARA містять умови збігу, а результати спрацювання повинні розглядатися як ознаки потенційної загрози, а не безумовний доказ шкідливості [3].

За наявності відповідності правилам YARA процес передбачає ізоляцію файла в карантинному сховищі або обмеження доступу до нього, фіксацію індикаторів та сповіщення відповідального фахівця. Можливе також передавання підтверджених індикаторів до суміжних сервісів AWS. Виявлення потенційно шкідливих об’єктів у хмарному середовищі AWS здійснюється за допомогою аналізу файлів із використанням правил YARA та додаткових механізмів моніторингу Amazon GuardDuty. Після виявлення підозрілої активності платформа Shuffle SOAR забезпечує автоматизацію подальших дій реагування, зокрема формування сповіщень, ізоляції небезпечних файлів або ініціювання їх видалення.

Практична реалізація запропонованого підходу передбачає автоматизовану перевірку файлів, що завантажуються до хмарного сховища Amazon S3. Після надходження нового файлу сервіс AWS Lambda автоматично отримує повідомлення про цю подію та передає інформацію про файл до платформи Shuffle SOAR. Далі система отримує файл із хмарного сховища та перевіряє його за допомогою правил YARA для виявлення ознак шкідливого програмного забезпечення. За результатами перевірки Shuffle SOAR визначає подальші дії.

Отже, поєднання Amazon S3, AWS Lambda, Shuffle SOAR і YARA забезпечує архітектурну основу для відтворюваного автоматизованого контролю нових файлів у хмарному сховищі. Науково-практична цінність запропонованого підходу полягає у формалізації послідовності дій,

розмежуванні виявлення та реагування, а також визначенні перевірюваних вимог до коректності роботи.

Список використаних джерел

1. Amazon Web Services. Amazon S3 Event Notifications. AWS Documentation. URL: https://docs.aws.amazon.com/AmazonS3/latest/userguide/EventNotifications.html
2. Shuffle. Workflows. Shuffle Documentation. URL: https://github.com/Shuffle/shuffle-docs/blob/master/docs/workflows.md
3. VirusTotal. Writing YARA Rules. YARA Documentation. URL: https://yara.readthedocs.io/en/stable/writing_yara_rules.html