УДК 004.67, 004.91
DOI: 10.31673/2409-7292.2022.040009

Андрущенко К.Ю., Ющенко М.О.

АВТОМАТИЗАЦІЯ ПРОЦЕСУ РЕАГУВАННЯ НА ІНЦИДЕНТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

В статті розглянуто процес автоматизації реагування на інциденти інформаційної безпеки організації. Визначено основні етапи планування автоматизації, ключові моменти і рекомендовано послідовність дій для розробки коректного сценарію реагування на інцидент певного типу. В якості прикладу наведено процес побудови сценарію реагування на інцидент типу «фішинг» відповідно до визначеного для прикладу набору рішень інформаційної безпеки, що можуть бути наявні в організації. Описано відповідні кроки сценарію реагування у форматі тексту, плану і графічно. Наведено графічний приклад реалізації розробленого плану в системі класу SOAR.

Ключові слова: інциденти інформаційної безпеки, автоматизація, реагування, сценарій, SOAR.

Вступ

На сьогоднішній день ландшафт кіберзагроз змінюється настільки швидко, що командам безпеки складно організувати швидкий і ефективний процес реагування. Щодня аналітики приймають рішення, які можуть вплинути на всю організацію і безпека компанії надмірно залежить від персоналу, який часто використовує ручні процеси для обробки сповіщень безпеки і величезної кількості даних з різних систем захисту інформації.

Неправильно обраний процес реагування, відсутність доступу до необхідних систем, перенасиченість даними з різних рішень, виконання постійно повторюваних дій – все це ускладнює процес реагування і становить загрозу для організації. Одним із завдань менеджерів інформаційної безпеки організації є побудова ефективного процесу реагування на інциденти інформаційної безпеки.

Ключові моменти побудови процесу реагування на інциденти інформаційної безпеки

Реалізація будь-яких процесів, що повинні бути реалізовані в організації, неможлива без достатнього ресурсного забезпечення [1]. Для побудови процесу реагування на інциденти в першу чергу необхідно виділити достатню кількість ресурсів – працівників, що будуть займатись розробкою сценаріїв реагування, фінансування закупки і підтримки відповідних рішень інформаційної безпеки, відповідно час на реалізацію задачі, а також ресурси для постійного моніторингу стану автоматизованої системи реагування.

1) **Першим кроком** у прийнятті рішень щодо керування інцидентами ІБ повинна бути систематизація класів інцидентів [1].

Переважно всюди для попередньої класифікації класів інцидентів фактично використовуються рішення інформаційної безпеки для виявлення і реагування на загрози різних типів – такі як рішення забезпечення антивірусного захисту (NGAV,EDR), міжмережеві екрани (IDS, IPS), контроль безпеки хмарних ресурсів, захист корпоративної пошти тощо.

Також в подібних рішеннях майже завжди для класифікації інцидентів використовується фреймворк MITRE ATT&CK [2], або Cybersecurity Kill Chain [3]. Це дозволяє забезпечити уніфікацію типів інцидентів інформаційної безпеки організації, що надходять з різних рішень та забезпечує відповідність міжнародним нормам класифікації інцидентів.

2) **Другим кроком** є розробка сценаріїв реагування для кожного актуального в організації типу інциденту з урахуванням доступних або запланованих для придбання засобів.

Загалом процес систематизації і автоматизації процесу реагування на інциденти інформаційної безпеки є непростим і доволі довгим. Тому найчастіше на початкових етапах впровадження автоматизації обирають декілька найбільш актуальних типів інцидентів і

першочергово розробляють для них ефективні сценарії реагування та автоматизують кроки, які можливо виконати без залучення аналітика інформаційної безпеки.

При розробці сценарію в першу чергу необхідно враховувати вхідні дані (які є можливості для виявлення інциденту і яка інформація доступна на початку розслідування) і бажаний результат, часові рамки розслідування. Для ефективної побудови автоматизації процесу реагування на інциденти, сценарії для обраних типів інцидентів обов'язково мають бути задокументовані в тому чи іншому вигляді з чітким описом послідовності дій, позначенням автоматизованих етапів і моментів, в яких має бути прийняте рішення про подальші дії аналітиком інформаційної безпеки. Сценарії можуть бути задокументовані в графічному вигляді (блок-схема) або у вигляді послідовних пунктів.

3) **Третім кроком** є власне автоматизація розроблених сценаріїв з використанням відповідних рішень інформаційної безпеки. В результаті для побудови зручного і ефективного, автоматизованого процесу реагування в організації необхідні інструменти для збору даних (з кінцевих точок, мережевих пристроїв, поштових серверів, серверів управління доменом, хмарних активів тощо), бажано інструмент для централізації і кореляції даних (клас рішень SIEM) і власне для автоматизації необхідне рішення класу SOAR – Security Orchestration, Automation and Response.

Даний крок полягає в тому, щоб реалізувати розроблені сценарії реагування у відповідних рішеннях – налаштувати збір даних, забезпечити можливість виявлення інцидентів, централізацію інформації з різних джерел, підключення необхідних рішень до системи SOAR за допомогою інтеграцій, і власне налаштування сценаріїв у самій системі SOAR.

Приклад побудови сценарію автоматизованого реагування на інцидент інформаційної безпеки типу «Фішинг»

Припустимо, в організації одними з найбільш розповсюджених, ключових типів актуальних інцидентів було визначено клас загроз «Фішинг».

В організації наявні інструменти збору і аналізу інформації:

IBM Security QRadar;	MS Active Directory;
IBM Security SOAR;	MS Exchange;
Symantec Endpoint Protection:	CRITs (Collaborative Research Into Threats);
Symantec Data Loss Prevention;	OmniTracker Service Desk;
Symantec Messaging Gateway;	Cisco Email Security Appliance (ESA).

Перший крок побудови сценарію реагування визначено, тип інциденту – фішинг. Другий крок – необхідно зрозуміти вхідні дані – звідки і в якому вигляді надходить інформація про виявлення загрози типу «фішинг» і якого результату необхідно досягти. В даному випадку необхідно досягти уникнення або принаймні мінімізації збитків від даної загрози, при цьому забезпечивши співробітникам доступ до інформації, якщо спрацювання є помилковим. Ризик від помилкового допуску зловмисного листа до користувача є значним, тому не можна пропустити підозрілий лист до того, як буде визначено, що він є безпечним. При цьому не можна значно затримувати надходження листа (якщо він безпечний), адже це може спричинити порушення бізнес- процесів.

Аналіз всіх листів, що надходять в організацію, перед їх пропуском є вкрай часо- і ресурсозатратним, невиправданим процесом. Тому на даному етапі необхідно додати елемент автоматизації. Для цього враховуючи початкові умови, наявні в організації інструменти, можна використати рішення класу захисту корпоративної пошти - Symantec Messaging Gateway (далі – SMG).

SMG аналізуватиме вхідну пошту відповідно до попередньо заданих налаштувань і пропускатиме санкціоновані листи, затримуючи підозрілі. Сповіщення від SMG про

затриманий підозрілий лист в даному випадку і будуть вхідними даними для генерації інциденту і ініціації сценарію розслідування.

Також при розробці сценарію реагування важливо враховувати, що цей процес необхідно постійно аналізувати і покращувати для забезпечення оптимізації. І якщо є механізм, який дозволить статично відсікати, наприклад, точно небезпечні листи, бажано його реалізувати. Наприклад, в даній типовій організації всі дані централізовано зберігаються в SIEM рішенні IBM QRadar. Там також наявний механізм фільтрації листів електронної пошти, що надходять в організацію. Тому при виявленні небезпечних листів, можна додавати їх артефакти відповідно в списки блокування QRadar (що мають назву Reference Set), і наступного разу аналогічний лист не надійде на вхід Cisco ESA і не потребуватиме повторного аналізу.

Звичайно якщо заблокований лист при аналізі визначений безпечним – його необхідно в незмінному вигляді надіслати користувачу.

Так може виглядати текстовий опис приблизно розпланованого сценарію реагування на інцидент інформаційної безпеки типу «фішинг» з урахуванням наявних в компанії інструментів – рішень інформаційної безпеки, що можуть допомогти в розслідування даного типу інциденту. Звичайно від початкової ідеї до кінцевого результату, який вирішено реалізовувати в організації і сценарії реагування можуть вноситись масштабні зміни. Кінцева реалізація може повністю відрізнятись від текстового опису, плану, або розробленої блок-схеми, якщо наприклад у адміністратора безпеки, що займався його розробкою, відсутній досвід роботи з рішенням SOAR (або з іншими задіяними рішеннями) і розуміння принципів їх роботи.

Автоматизація кроків сценарію також визначається за деякими факторами. Всі процеси передачі інформації з одного рішення в інше бажано автоматизувати, якщо це можливо, для збереження часу аналітика. Адже при передачі інформації не приймаються безпосередні рішення і не вимагається аналіз даних. Для інших моментів сценарію, в першу чергу, необхідно зрозуміти чи може рішення на цьому етапі бути прийняте автоматично, чи є в організації достатньо засобів, які вичерпно і коректно визначать наступний крок. Наприклад, для досліджуваного плейбуку це може бути аналіз артефактів в CRITs, адже аналітик не виконає пошук і аналіз краще, ніж відповідна програма, рішення, затверджене для використання в організації.

На початкових етапах використання автоматизованого сценарію реагування можна додати ручні завдання для перевірки коректності виконання етапу, а в подальшому прибрати їх або приховати. Для деяких задач можна залишити як автоматизоване рішення, так і ручне підтвердження коректності прийнятого рішення аналітиком.

Звичайно для цих випадків необхідно також оцінити можливість і трудомісткість відповідної автоматизації. В рідкісних випадках написання інтеграцій для автоматизації є вкрай складним або неможливим. Також на початковому етапі можливо прийняття рішення про ручну обробку певного етапу і запланувати його автоматизацію в подальшому.

І другий тип рішень в сценарії реагування – коли в організації недостатньо засобів автоматизованого аналізу (або достатньо надійних рішень для даної задачі не існує) і рішення обов’язково має приймати аналітик. Подібні задачі можуть як бути, так і не бути наявні в сценарії, залежно від типу інциденту і задачі реагування.

Планування сценарію загалом може відбуватись по різному, залежно від адміністратора, який цим займається. Наприклад, можна зробити це в декілька етапів:

визначити пріоритетний для автоматизації тип інциденту;

розписати приблизну послідовність дій, яка необхідна для розслідування інциденту і варіанти кінцевого результату;

детально розписати послідовність дій, дії при різних результатах виконання умов сценарію;

побудувати блок-схему дій, при наявності досвіду роботи з рішенням SOAR можна одразу враховувати формат сценарію в системі;

перенести сценарій в систему SOAR, забезпечити необхідні інтеграції і налаштування, протестувати і відредагувати за необхідністю;

відповідно відредагувати схему, опис сценарію та затвердити документально.

Після виконання всіх попередніх дій можна вводити автоматизований сценарій реагування на інцидент відповідного типу в експлуатацію в організації.

Деякі організаційні моменти, як наприклад визначення працівників, що відповідатимуть за контроль системи SOAR, виконання ручних етапів розслідування, налаштування інструментів безпеки не розглянуто в даній статті.

В результаті, перший приблизний план може мати такий вигляд:

Проект сценарію обробки подій для виявлення фішингу:

1. Е-маіл повідомлення на вхід Resilient надходять з SMG по Custom-дії, або лист надходить від адміністратора безпеки.

2. Resilient виконує розбір листа, виділяє, якщо там є лінкі, вкладення, створює інцидент, додає в артефакти вкладення, лінкі, IP-адресу відправника, причину карантину.

3. Отримуємо (вираховуємо) хеш на вкладення, яке дістали з листа.

4. Через API звертаємось до репозиторію зразків коду CRITs та шукаємо там хеш вкладення, лінкі, IP-адресу.

a. Якщо в CRITs знаходимо, то по API звертаємось до QRadar до створених вже там ReferensSets, ReferensTables та перевіряємо що там є ці IP-адреса, лінки. Якщо їх там немає то додаємо.

b. Якщо в CRITs не знаходимо то ідемо на VT\IBM xForce та шукаємо там хеш, лінкі, IP-адреси. Якщо є негативна інформація щодо цих артефактів то по API заносимо в CRITs вкладення, IP-адресу відправника, лінкі.

i. Якщо на VT\IBM xForce не знаходимо нічого негативного по хеш, лінкам, IP-адресам, необхідно закрити інцидент та відправити оригінал листа на Cisco ESA для аналізу.

ii. Якщо від Cisco ESA прийде інформація, що там нічого не виявлено підозрілого чи зловмисного, Cisco ESA повідомляє інформацію про статус розгляду листа Resilient та відправляє лист на Exchange отримувачу.

iii. Якщо від Cisco ESA прийде інформація, що у листі виявлено підозрілі вкладення чи зловмисний код, лист блокується в карантині Cisco ESA, Cisco ESA повідомляє інформацію про статус розгляду листа Resilient, по API звертаємось до QRadar до створених вже там ReferensSets, ReferensTables та перевіряємо що там є ці IP-адреса, лінки. Якщо їх там немає то додаємо. Закриваємо інцидент.

На основі початкового плану можна розробити детальну послідовність дій з урахуванням логіки роботи системи і інтеграцій і, відповідно до детального опису подій, можна розробити блок-схему для візуалізації дій сценарію реагування (Рис.1).

1) На вхід SOAR надходить лист з SMG, з якого генерується інцидент. За допомогою скрипту лист оброблюється і необхідні дані – посилання, IP-адреси, причина карантину зберігаються в Системі.

2) За допомогою кастомної інтеграції обробляється вкладення за наявності – вираховується хеш файлу. Якщо файл – архів формату zip – вираховується хеш усіх вкладених файлів.

3) Здійснюється перевірка наявності значень артефактів в CRITs, артефакти поділяються на 2 списки – наявні в CRITs (1), відсутні в CRITs (2).

4) Для списку (2) перевіряється наявність спрацювань в підключених TI Feeds. Проаналізовані артефакти поділяються на 2 списки – наявні спрацювання (3), відсутні спрацювання (4).

Умова: дані відсутні в списку (3):

5) Перевіряється наявність даних зі списку (2) в QRadar Referense Sets та вносяться відсутні дані.

6) Закривається інцидент

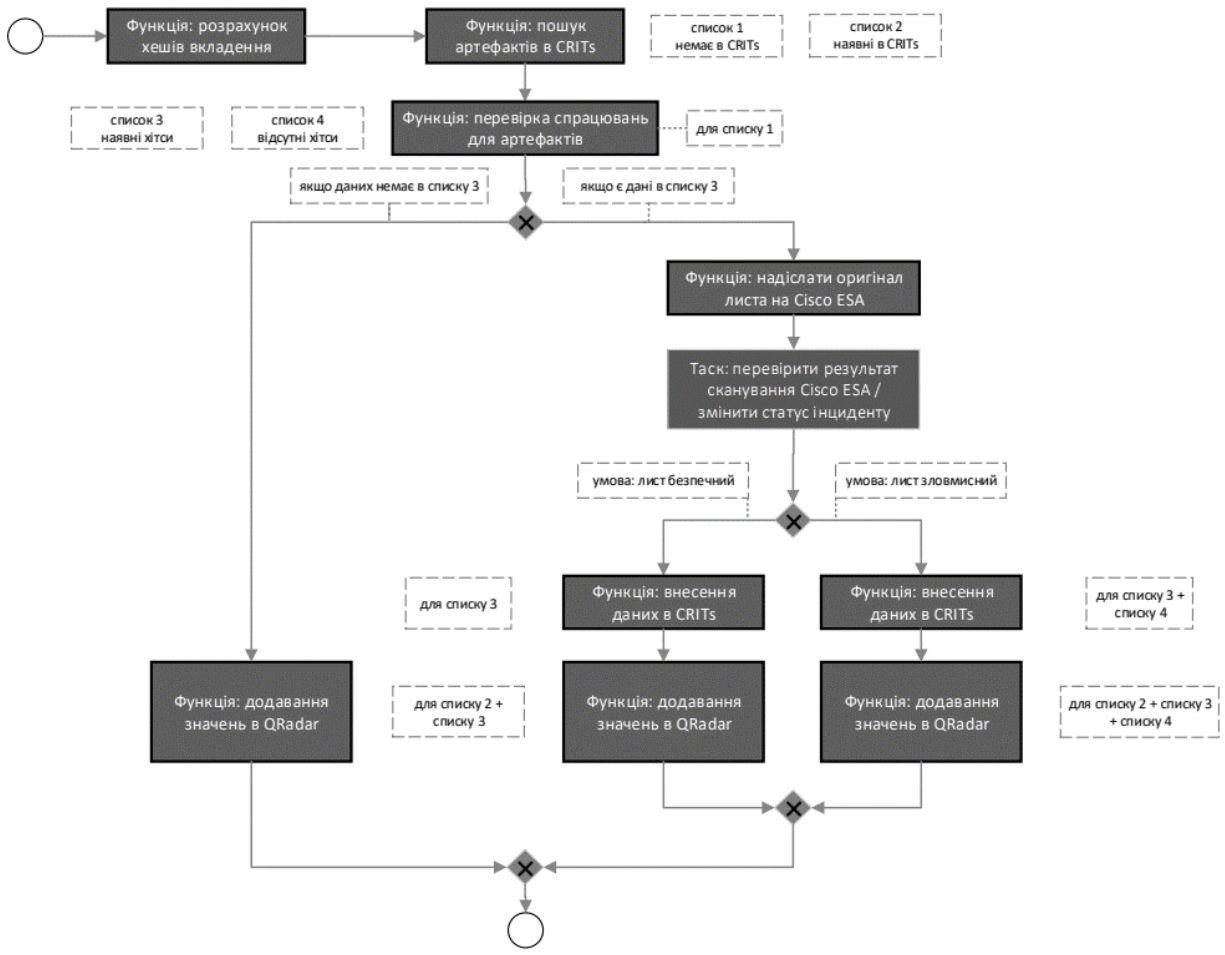

Рис. 1. Приклад блок-схеми сценарію розслідування інциденту типу «фішинг»

Умова: дані наявні в списку (3):

5) Надсилається оригінал листа на Cisco ESA.

6) Здійснюється ручна перевірка результату (виконується видане завдання), відмічається відповідний результат згідно з інструкціями.

Умова: лист безпечний.

7) Вносяться артефакти зі списку (3) в CRITs.

8) Перевіряється наявність даних зі списку (2) і списку (3) в QRadar Referense Sets та вносяться відсутні дані.

9) Закривається інцидент.

Умова: лист зловмисний.

7) Вносяться артефакти зі списку (3) і списку (4) в CRITs.

8) Перевіряється наявність даних зі списку (2), списку (3) і списку (4) в QRadar Referense Sets та вносяться відсутні дані.

9) Закривається інцидент.

І фінальна реалізація даного сценарію на прикладі використання SOAR рішення IBM Security SOAR (колишній Resilient) має такий вигляд (Рис. 2):

Висновки

Безпека організації на сьогоднішній день значно залежить від швидкості обробки сповіщень, що надходять від рішень інформаційної безпеки і загалом швидкості реагування на будь-які нестандартні події в інформаційному середовищі організації. Чи не єдиним ефективним варіантом забезпечення достатньо швидкого процесу реагування є автоматизація.

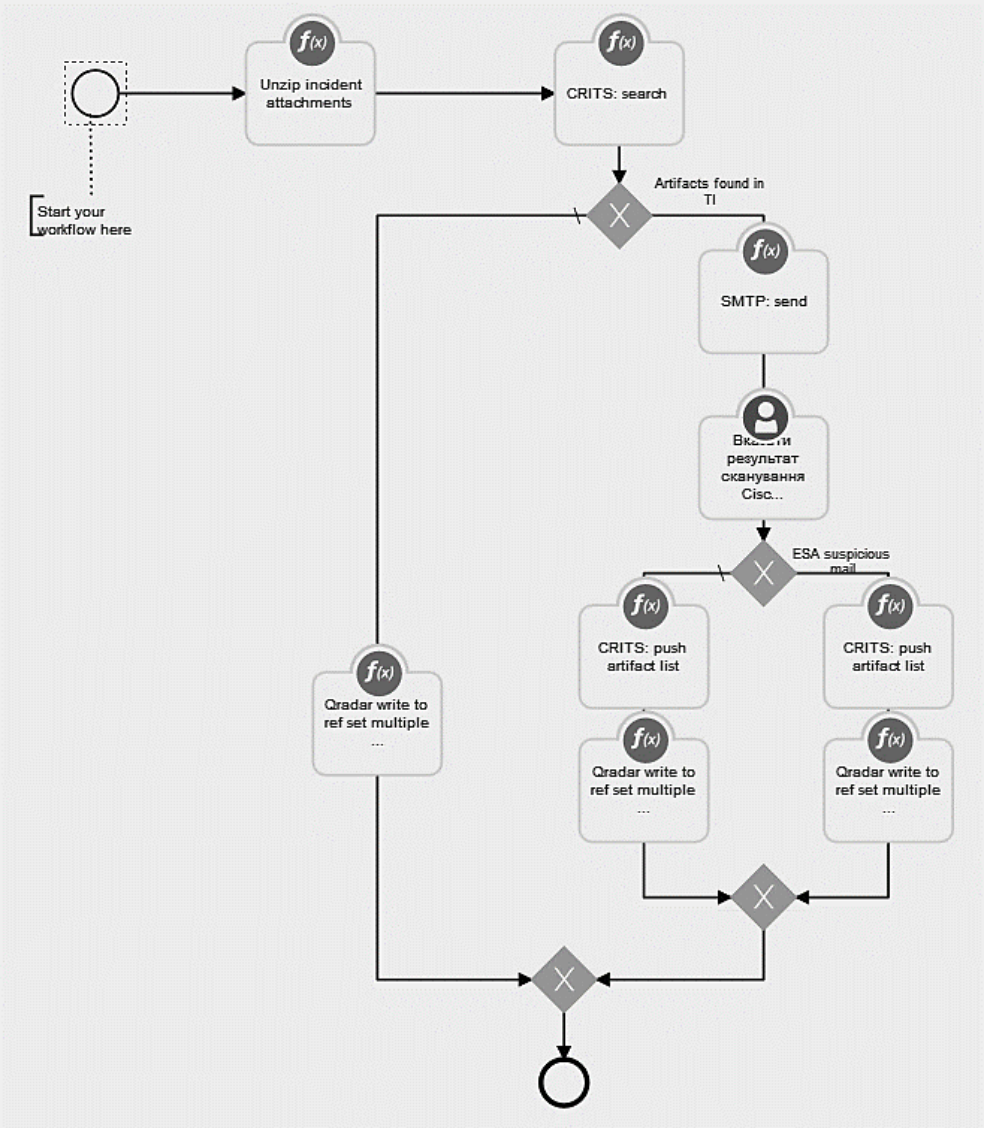

Рис. 2. Приклад блок-схеми сценарію розслідування інциденту типу «фішинг», реалізований в системі IBM Security SOAR

Автоматизація процесу реагування на інциденти інформаційної безпеки потребує достатньо багато часу і ресурсів на впровадження, проте значно прискорює реагування на інциденти інформаційної безпеки організації і відповідно покращує рівень захисту при коректному налаштуванні всіх автоматизацій і постійному контролю роботи відповідних сценаріїв. Також автоматизація певних процесів розслідування забезпечує скорочення часу обробки і аналізу повторюваної інформації, економить час аналітиків на розслідування інцидентів та забезпечує вищий рівень надійності ніж при ручній обробці.

Перелік посилань

1. Гладиш С.В. Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах [Електронний ресурс] // - Режим доступу: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/7536/11-Gladysh.pdf?sequence=1 (19.10.2022)

2. MITRE ATT&CK [Електронний ресурс] // - Режим доступу: https://attack.mitre.org/ (19.10.2022)

3. The Cyber Kill Chain [Електронний ресурс] // - Режим доступу: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (19.10.2022)

Надійшла: 30.11.2022 Рецензент: д.т.н., доцент Ахрамович В.М.