Секція 1

ДОСЛІДЖЕННЯ АВТОМАТИЗОВАНИХ ЗАСОБІВ ДЛЯ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ

Медведєва Ю. В.
Національний аерокосмічний університет ім. М. Е. Жуковського «ХАІ»
Науковий керівник: Брежнєв Є. В.

Актуальність. Згідно зі статистикою [1], 60% організацій, які зазнали кібератак за останні два роки, заявляють, що вони були атаковані через невиправлену відому вразливість, де патч не було застосовано. 62% опитаних зазначають, що вони не мали інформації щодо вразливостей, які були використані під час кібератаки. В той же час 52% респондентів впевнені, що їх організації мають невигідну позицію у реагуванні на вразливості, оскільки вони використовують лише ручні процеси пошуку, аналізу та виправлення вразливостей [1]. Отже, процес управління вразливостями IT-систем є важливою та невід'ємною частиною забезпечення кібербезпеки організації, який практикується разом з управлінням ризиками та іншими практиками безпеки. Управління вразливостями включає в себе ідентифікацію, класифікацію, усунення та пом'якшення різних вразливостей у системі [2]. Для зменшення кількості ручної роботи та збільшення обсягів оброблюваної інформації під час управління вразливостями існують автоматизовані засоби, які повністю чи частково виконують задачі спеціаліста з управління вразливостями.

Метою даної роботи є дослідження автоматизованих засобів для управління вразливостями IT-систем організації .

Сучасний ринок надає широкий вибір засобів, призначених для виявлення слабких місць у системі організації щоб пом'якшити потенційні порушення безпеки в майбутньому. Кожний засіб володіє своїми функціями, перевагами та недоліками, тому основна задача лежить у порівнянні роботи і особливостей обраних засобів. Для цього використовується документація, література, демонстраційні матеріали та тестовий період використання. Результатом дослідження є виведена порівняльна таблиця обраних засобів.

Основні положення. Об'єктами дослідження були обрані три автоматизованих засоби для управління вразливостями на основі публічно-доступних рейтингів, документації та відповідності тестовій середі: Tenable.io (Tenable) [3], InsightVM (Rapid7) [4] та Qualys Vulnerability Management, Detection and Response (VMDR) (Qualys) [5]. Основними

категоріями для порівняння виступають набір можливостей, простота використання, рекомендації щодо пріоритезації, підтримка користувача, цінова політика, API та розширюваність, сторонні інтеграції.

Кожен критерій оцінюється експертом по десятибальній шкалі, де 1 відповідає найнижчій оцінці, 10 – найвищій. 0 відповідає відсутності інформації чи функціоналу. Для кожної категорії виведено вагу згідно з важливістю категорії – коефіцієнт, який враховується при виведенні підсумкової оцінки для кожного засобу. За результатами оцінювання визначається найбільш придатна система для конкретного кейсу тестового середовища.

Висновки. Автоматизовані засоби для управління вразливостями є невід'ємною частиною процесу управління вразливостями для забезпечення кібербезпеки організації. Для ефективного побудування процесу управління вразливостями важливим є вибір найбільш відповідного засобу для конкретної системи. В роботі було розглянуто три варіанту програмного забезпечення, проведено їх порівняльну характеристику та виведена найбільш придатна система для конкретного кейсу тестового середовища.

Список літератури

1. Ponemon study on gaps in vulnerability response. *Servicenow*. URL – https://www.servicenow.com/lpayr/ponemon-vulnerability-survey.html (дата звернення: 15.06.2022);

2. Що таке управління вразливістю?. *Технопедія.* URL – https://uk.theastrologypage.com/vulnerability-management (дата звернення: 15.06.2022);

3. Tenable.io. *Tenable.* URL – https://www.tenable.com/products/ tenable-io (дата звернення: 15.06.2022);

4. InsightVM. *Rapid7.* URL: https://www.rapid7.com/products/insightvm/ (дата звернення: 15.06.2022);

5. Vulnerability management. *Qualys*. URL: https://www.qualys.com/apps/vulnerability-management/ (дата звернення: 15.06.2022).

Відомості про авторів

Медведєва Юлія Віталіївна, магістрант кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 050-193-77-79, y.medvedieva@student.csn.khai.edu

Брежнєв Євген Віталійович, професор кафедри комп'ютерних систем, мереж і кібербезпеки, д. т. н., професор, e.brezhniev@csn.khai.edu