ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ В КОРПОРАТИВНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ ОРГАНІЗАЦІЇ»

Виконав студент 4 курсу, групи БСД-42
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та
кібернетична безпека»
(шифр і назва спеціальності)
Височин Ян Олександрович
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

RBVM		Risk-based vulnerability management
NVD	–	National Vulnerability Database
CVE	–	Common Vulnerabilities and Exposures
MIS	–	Management Information System
SVSS	–	Common Vulnerability Scoring System
CCE	–	Common Configuration Enumeration
CIS	–	Center for Internet Security

ВСТУП

Актуальність дослідження. Управління вразливістю є критично важливим компонентом стратегії інформаційної безпеки будь-якої організації. Це допомагає організаціям зменшити ризик кібератак, захистити конфіденційні дані, дотримуватися нормативних актів, підвищити ефективність роботи та підвищити репутацію бренду.

Управління вразливістю важливо для організацій. Це зумовлено багальма вимогами щодо забезпечення кібербезпеки. Своєчасно виявляючи та усуваючи вразливості, організації можуть значно знизити ризик успішних кібератак, тобто зменшити ризик.

Однією з вимог до забезпечення кібербезпеки є захист конфіденційних даних. Управління вразливістю допомагає захистити конфіденційні дані, такі як інформація про клієнтів, інтелектуальна власність і фінансові записи.

Кожна організація повинна дотримуватись норм законів щодо кібербезпеки. Дотримання нормативних актів вимагають від організацій впровадження програм керування вразливістю для захисту конфіденційних даних.

Добре розроблена програма управління вразливістю може допомогти організаціям покращити свою операційну ефективність за рахунок скорочення часу простою, спричиненого кібератаками.

Тому організаціям необхідно впровадити в свою роботу надійні програми управління вразливостями, тому що кібератака може серйозно знешкодити репутацію бренду організації.

Правильно обрана стратегія або план по управлінню вразливостями дозволяє ідентифікувати, оцінювати, визначати пріоритети та пом’якшувати вразливості, якими можуть скористатися кіберзловмисники при проведенні кібератак.

Об’єкт дослідження – процес управляння вразливостями в інформаційній системі організацій.

Предмет дослідження – методи та засоби управляння вразливостями в інформаційній системі організацій.

Мета роботи – розробити рекомендації щодо застосування методів та засобів управляння вразливостями в інформаційній системі організацій на базі платформи Rapid 7.

Наукові завдання:

дослідити процес управління вразливостями в інформаційній системі організації;

проаналізувати існуючі методи та засоби ;управління вразливостями

дослідити можливості роботи з програмного комплексу Rapid 7 InsightVM в інформаційній системі організації.

Практичне значення одержаних результатів полягає в розробці рекомендацій щодо застосування програмного комплексу Rapid 7, який доцільно використовувати в інформаційних системах організацій для управління вразливостями.

1 АНАЛІЗ ПРОЦЕСУ КЕРУВАННЯ ВРАЗЛИВОСТЯМИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

1.1. Призначення процесу управління вразливостями інформаційної системи організації

Деякі організації все ще вважають, що їх інформаційна інфраструктура є бездоганною просто тому, що вони ніколи не стикалися з інцидентом кібербезпеки, поки щось не піде не так і компанія не стане жертвою атаки зловмисного програмного забезпечення або витоку даних . Ось чому завчасне виявлення недоліків у безпеці та мінімізація лазівок є крайньою необхідністю для великих і малих організацій, і саме тут у гру вступає керування вразливими місцями [1].

Управління вразливістю є важливою частиною будь-якої стратегії кібербезпеки, яка стосується методів безпеки, які проактивно ідентифікують, запобігають, пом'якшують і класифікують уразливості в IT-системі.

Згідно з глосарієм кібербезпеки, уразливості можна визначити як «діри» в кібербезпеці, які залишають системи відкритими для кібератак. Якщо їх не усунути належним чином, використані вразливості можуть призвести до збоїв у роботі IT-систем, що потенційно призведе до дорогих витоків даних і збоїв у роботі [1].

Керування вразливістю — це проактивний процес, розроблений для виявлення, запобігання, пом'якшення та класифікації вразливостей. Залежно від характеру вразливості чи загрози потрібні різні підходи для її усунення. Саме тут на допомогу приходить управління виправленнями, оскільки це техніка усунення вразливостей програмного забезпечення в мережі шляхом розгортання виправлень. У цьому сенсі керування виправленнями є важливим компонентом управління вразливістю [1].

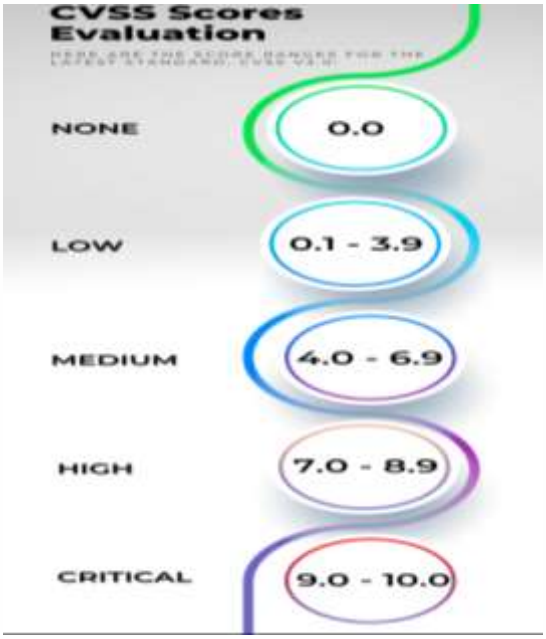
Як правило, оцінка вразливості є частиною процесу управління вразливістю. Щоб отримати більше корисної інформації про працездатність

системи, організації проводять численні оцінки вразливості, щоб розробити ефективний план дій щодо управління вразливістю.

Керування вразливістю на основі ризиків (RBVM) — це стратегія кібербезпеки, яка дозволяє організаціям використовувати аналітичні дані безпеки для виявлення, визначення пріоритетів і усунення найбільш серйозних уразливостей на основі контексту їхнього ризику. Ця концепція також зустрічається під назвою управління ризиками вразливості. На відміну від керування вразливістю, RBVM — це підхід, заснований на оцінці ризику, який зосереджується на ймовірності використання вразливості, а не лише на серйозності потенційних наслідків у разі її використання [1].

Рейтинг вразливостей. Багато організацій з кібербезпеки використовують Загальну систему оцінки вразливостей (CVSS), щоб оцінити та передати ступінь серйозності та характеристики вразливостей програмного забезпечення. Це безкоштовний і відкритий промисловий стандарт. Базова оцінка CVSS коливається від 0,0 до 10,0, і оцінки CVSS визначають ступінь серйозності Національною базою даних уразливостей (NVD).

NVD також містить дані про вразливості, які отримують автоматизовані рішення для керування вразливістю та IT-персонал.



Рим.1.1. Базова оцінка CVSS [1]

Розглянемо переваги управління вразливістю.

1.Економічна ефективність.

Керування вразливістю має важливе значення для захисту організації від дій зловмисників, які можуть спробувати скомпрометувати ваші системи. Технологія, яка називається керування вразливістю, постійно класифікує та підтримує атрибути кожного мережевого обладнання у вашій організації.

Однією з головних переваг процесу керування вразливістю є його економічна ефективність. Автоматизоване рішення позбавить вашу організацію від неефективного латання, а також сприятиме зменшенню технічної заборгованості.

Простіше кажучи, управління вразливістю допомагає структурі та чіткості системи безпеки організації, посилюючи її обґрунтування для зацікавлених сторін, які, таким чином, будуть більш готові підтримувати програми уразливості.

2. Швидке реагування на загрози

Актори загрози не відпочивають і не йдуть у відпустку! Кожного дня вразливі місця виявляються тоді, коли ми цього найменше очікуємо. Організації можуть переходити від реактивної до проактивної реакції за допомогою управління вразливістю.

Налаштування постійної стратегії керування виправленнями гарантує швидке виявлення основних уразливостей, надання їм пріоритету та наявність ресурсів для усунення. Роблячи це, він створює основу для швидшої та ефективнішої реакції на загрози, щойно вони матеріалізуються.

3. Покращує видимість і звітність

Огляд проекту допомагає зацікавленим сторонам зрозуміти повернення інвестицій у безпеку та може принести користь наступним проектам. Отримані звіти надають вищому керівництву ключові показники та показники, які допомагають у процесі прийняття обґрунтованих рішень щодо ключових ініціатив.

Результати звітів також допомагають команді створювати практичні інформаційні панелі та звіти про тенденції, що допомагає їм вимірювати продуктивність і стан програми.

5. Операційна ефективність

Підтримка узгодженості команди та системи з цілями та результатами проекту має вирішальне значення, особливо коли йдеться про високочутливу безпеку для організації.

Управління вразливими місцями має на меті визначити процедуру пошуку вразливих місць і їх усунення для підтримки узгодженості. Воно також має потенціал для скорочення ручного робочого процесу, і крім цього, також забезпечує постійний моніторинг, сповіщення та рішення для виправлення.

Визначимо основні етапи управління вразливістю

Управління вразливістю — це постійний проактивний механізм запобігання, який має включати такі кроки:

- *Сканування вразливостей* – сканування мережі, журнал брандмауера, тестування на проникнення або використання автоматизованого інструменту, наприклад сканера вразливостей.
- *Пошук вразливостей* – аналіз результатів сканування вразливостей і журналів брандмауера, а також пошук аномалій, які можуть свідчити про те, що у вашому середовищі відбулася атака.
- *Перевірка вразливостей* – визначення того, як виявлені помилки можуть потенційно бути зловживаними на комп’ютерах, програмному забезпеченні, мережах тощо. Це часто вимагає оцінки величини вразливості та небезпеки, яку вона становить для компанії.
- *Пом’якшення вразливостей* – рішення про те, як запобігти використанню вразливостей до випуску виправлень.
- *Виправлення вразливостей* – найважливішою частиною процесу керування вразливістю є фактичне усунення вразливостей за допомогою виправлення.

Основні заходи, які необхідні для впровадження процесу керування вразливістю в організації, можна представити у вигляді кроків, які, є необхідними під час налаштування процесу керування вразливими місцями.

1. Визначте свої цілі

Головною метою будь-яких вправ із керування вразливістю є якнайшвидший пошук і пом’якшення вразливостей.

Потім вам слід визначити другорядні цілі, наприклад визначити частоту сканування вразливостей . Одна з помилок сканування вразливостей полягає в тому, що цей процес не виконується регулярно, через що ваша компанія стає незахищеною, якщо будь-які вразливості залишаються надто довго без виявлення. Таким чином, якщо сканування буде виконано вчасно, ризики будуть значно знижені.

2. *Визначте ролі у вашій організації*

Ще один важливий аспект, про який вам слід подбати, — це розподіл ролей і обов’язків і чітке визначення ролей усіх зацікавлених сторін у процесі управління вразливістю. Необхідність такого процесу має розуміти кожен, хто бере участь.

Для ефективного процесу управління вразливістю CISA пропонує наступні типи ролей для призначення в організації:

- *Ролі моніторингу* – відповідальні люди повинні проаналізувати ступінь серйозності вразливостей, занести інформацію про вразливості в сховище та повідомити групу з усунення.
- *Ролі виправлення* – відповідальні працівники повинні виконувати такі дії, як аналіз впливу виправлень на організацію та розробка внутрішніх способів усунення вразливості (якщо вони недоступні).
- *Ролі авторизації* – вони є частиною персоналу процесу управління змінами та повинні вживати коригувальних дій, щоб визначити, чи можуть бути будь-які негативні наслідки.

3. Виберіть надійний інструмент керування вразливістю

Процедура управління вразливістю, від виявлення вразливості до виправлення, має стати максимально автоматизованою. Таким чином, операції будуть більш ефективними, а повторювані завдання та процеси зменшаться, що дозволить персоналу зосередитися на інших важливих завданнях. Завдяки автоматизованому підходу підприємства зможуть ефективно пом’якшувати

вразливі місця, які створюють загрози, уникаючи при цьому непотрібної шкоди бізнес-операціям.

Автоматизовані інструменти керування вразливістю дозволяють безперервно контролювати вашу інфраструктуру та оцінювати стан вашого середовища в реальному часі.

Правильно обране рішення для автоматичного керування вразливостями дозволяє пом'якшувати експлойти, досягати відповідності, усувати вразливості та встановлювати програмне забезпечення в будь-якій точці світу відповідно до вашого розкладу.

4. Оцініть ефективність вашої програми керування вразливістю.

Ведення та підтримка безперервної програми управління вразливістю дозволяє організації оцінювати ефективність виявлення, аналізу та пом'якшення вразливостей, а також надає рекомендації для прийняття майбутніх рішень.

Необхідно завжди вносити необхідні корективи у свої процеси, гарантуючи, що компанія зберігає вичерпне розуміння своїх критично важливих активів і забезпечує безпеку своєї інфраструктури.

Однією з переваг впровадження процесу керування вразливістю стане менше стресу для IT-команд і підвищена безпека для вашої організації.

1.2. Аналіз поняття та типи сканування вразливостей

Постійно мінливий ландшафт кібербезпеки ускладнює компаніям йти в ногу зі зловмисними намірами зловмисників. Щодня у системах можуть з'являтися нові вразливості, які можуть дати зловмисникам потрібний шанс зламати систему та викрасти дані чи вплинути на процеси вашої компанії [2].

Якщо ви хочете, щоб ваш бізнес був безпечним і здоровим, завжди слід дотримуватися профілактики.

Сканування вразливостей — це процес, який відповідає за виявлення, аналіз і звіт про недоліки безпеки та вразливості. Поряд з оцінкою вразливості сканування вразливостей є важливим кроком у життєвому циклі керування вразливістю .

Зазвичай цей процес виконує IT-відділ компанії, хоча є також сторонні постачальники послуг безпеки, які можуть взяти на себе це завдання. Сканування також може використовуватися зловмисниками , які шукають точки входу в мережу компанії.

Розглянемо типи сканування вразливостей

Деякі рішення для сканування вразливостей пропонують повне охоплення та можуть запускати різні типи сканування в різних середовищах, включаючи локальні, Unix, Linux , Windows , хмарні, зовнішні та локальні. Основні типи сканування вразливостей, які використовуються, – це сканування з автентифікацією та сканування без автентичності , але існують також інші типи сканування, які можна використовувати в конкретних ситуаціях [2].

Автентифіковані скани

Під час автентифікованого сканування тестувальники перевіряють системи з точки зору користувача. Тестер входить як користувач мережі, щоб перевірити наявність уразливостей, доступних для довірених користувачів або зловмисників, які отримали доступ як довірений користувач.

Неавтентифіковані сканування

Як випливає з назви, за допомогою неавтентифікованого методу тестувальники виконують сканування, не маючи привілеїв довіреного користувача, так само, як це зробив би зловмисник. Цей тип сканування виявляє вразливі місця, до яких можна отримати доступ навіть без довіреного доступу до мережі.

Інші типи сканування вразливостей

Зовнішнє сканування вразливостей: цей тип сканування націлено на ті області IT-екосистеми компанії, які доступні для Інтернету або без обмежень. Мережі, порти , системи, програми, веб-сайти тощо.

Внутрішнє сканування вразливостей: використовується для виявлення вразливостей, через які ваші системи стають відкритими після проникнення кібератаки або зловмисного програмного забезпечення .

Інтрузивне сканування вразливостей: таке сканування намагається використати вразливості, якщо їх виявлено. Використовувати інтрузивне сканування необхідно з обережністю, оскільки воно може перервати роботу ваших операційних систем і процесів, створити труднощі для вашого персоналу та клієнтів і підкреслити потенційну небезпеку та наслідки вразливості;

Ненав'язливе сканування вразливостей: ці сканування просто визначають уразливості та повідомляють про них, щоб ви могли їх своєчасно виправити;

Сканування вразливості навколишнього середовища: на основі середовища, в якому працює технологія вашого бізнесу. Спеціалізовані сканування доступні для різноманітних технологічних розгортань, у тому числі хмарних пристроїв , пристроїв Інтернету речей , мобільних пристроїв , веб-сайтів тощо.

Розглянемо сканування вразливостей проти тестування на проникнення [2].

Поширеною помилкою є те, що сканування вразливостей – це те саме, що тестування на проникнення , але між ними є значні відмінності:

Сканування вразливостей — це автоматизований високорівневий процес, який виконується програмним забезпеченням для пошуку потенційних слабких місць, тоді як тестування на проникнення включає в себе участь живої людини, яка фактично виконує перевірку, шукаючи у складності вашої мережі, щоб знайти та використати слабкі місця;

Роль сканування вразливостей полягає лише у виявленні слабких місць у вашій системі, тоді як тестування на проникнення є процесом, який вимагає глибшого розуміння вразливості. Тестер копне глибше, щоб визначити першопричину вразливості. Він також шукає вразливості бізнес-логіки, які може пропустити автоматичний сканер.

Тож найкращі методи сканування вразливостей включають наступні кроки.

Сканування кожного пристрою, який підключений до вашої екосистеми

Скануючи кожен актив в екосистемі, можна виявити різні недоліки інфраструктури та створити план їх усунення або прийняття ризику. Крім того, можна скласти список усіх мережевих пристроїв, незалежно від їхнього

призначення, і виберати із цього списку, які цілі включити до списку перевірки вразливостей.

Обов’язково треба призначити власників критично важливих активів, щоб було зрозуміло, хто відповідає за підтримання відповідного пристрою в робочому стані та кого вплине, якщо цей пристрій зламано.

Регулярно виконувати сканування

Сканування вразливостей насправді є мітками часу та показують стан мережі в певний момент часу. Інтервал часу між скануванням вразливих місць є фактором ризику , оскільки через цей проміжок ваші системи залишаються відкритими для нових уразливостей. Ви повинні вибрати, чи сканувати щотижня, щомісяця чи щокварталу, і врахувати вплив, який це матиме на ваш бізнес. Не всі пристрої у вашій мережі вимагатимуть щотижневого сканування, і не всі пристрої у вашій мережі слід включати до кожного квартального сканування.

Відстеження сканування та документування їх результатів

Кожне сканування вразливостей має плануватися згідно з графіком, узгодженим керівництвом, із механізмом аудиту, необхідним для створення детальних звітів із описом кожного сканування та його результатів. Документування сканувань дозволить вашій організації відстежувати тенденції вразливості та повторення проблем, таким чином визначаючи системи, які часто піддаються загрозам.

Створення плану відновлення

Процес виправлення має визначати конкретні рівні серйозності та терміновість усунення кожної знайденої вразливості, включаючи необхідний часовий проміжок після того, як результати сканування будуть задокументовані та пріоритет призначено кожному пристрою.

Пріоритет виправлення

Більшість атак на систему компанії пов’язані з уразливими місцями, яким можна було б запобігти за допомогою належних процедур виправлення. Пріоритезація виправлення активів може допомогти вашому бізнесу підвищити ефективність виправлення. Важливіше виправляти всі пристрої, які мають доступ

до Інтернету, ніж виправляти ідентичні пристрої, які вже були обмежені налаштуваннями чи брандмауерам.

Тож сканування вразливостей — це процес, яким не варто нехтувати. Процес потрібно виконувати регулярно, оскільки вразливі місця можуть з'явитися будь-коли, і без обережності ми можемо поставити під загрозу безпеку нашого бізнесу. Включення до вашої стратегії безпеки процесу керування вразливими місцями матиме великий вплив на безпеку вашої компанії, покращуючи час реагування на загрози, і ускладнить зловмисникам, які намагаються зламати ваші машини.

1.3. Аналіз поширених вразливостей і ризиків інформаційної системи

Управління вразливістю є найважливішим для успішної стратегії кібербезпеки, а CVE є її невід'ємною частиною.

Абревіатура CVE розшифровується як Common Vulnerabilities and Exposures і означає базу даних, що містить публічно оприлюднені вразливості та уразливості інформаційної безпеки. Система активно підтримується Національною службою кібербезпеки США FFRDC, якою, у свою чергу, керує корпорація MITRE.

Розглянемо різниця між уразливістю та ризиком.

Вразливі місця визначаються як недоліки системи, які створюють слабкі місця в інфраструктурі, які можуть бути використані під час кібератаки. Вони можуть складатися з чого завгодно: від програмного забезпечення без виправлень до незахищеного порту USB. Якщо їх залишити без нагляду, вони можуть дозволити кіберзлочинцям отримати доступ до системної пам'яті, встановити зловмисне програмне забезпечення, запустити шкідливий код або навіть викрасти, знищити та змінити конфіденційні дані.

Ураження являє собою єдиний випадок, коли система організації знаходиться під загрозою. Зазвичай описуваний як проста помилка, він відкриває організацію для різних випадків кібер-шкоди. Приклади включають, але не обмежуються витоком даних, порушенням даних та ідентифікаційною інформацією, яка викрадається та продається в Dark Web. Переважна більшість

інцидентів з безпекою спричинена викриттям, а не добре продуманими планами використання.

Історія системи CVE

Початкова концепція того, що згодом стане базою даних CVE, виникла в офіційному документі під назвою «На шляху до загального переліку вразливостей», написаному співавторами Стівеном М. Крісті та Девідом Е. Манном з корпорації MITRE. Дует представив документ на 2-му семінарі Університету Пердью з дослідження баз даних уразливостей безпеки, який відбувся в січні 1999 року [5, 6].

Починаючи з цього моменту, Крісті та Манн зібрали робочу групу, яка згодом стала редакційною колегією CVE з 19 членів, і склали оригінальний список CVE із 321 запису. У вересні 1999 року реєстр став загальнодоступним, і таким чином народилася система, яку ми знаємо сьогодні.

З моменту запуску списку CVE у 1999 році багато компаній із спільноти кібербезпеки підтримали цю ініціативу, випустивши сумісні продукти. До грудня 2000 року загалом 29 організацій брали участь у ініціативі зі своїми 43 супутніми пропозиціями.

На додаток до цього, база даних CVE була використана як відправна точка для багатьох абсолютно нових продуктів, таких як Національна база даних уразливостей США (NVD) NIST. Протягом багатьох років система продовжувала розвиватися і продовжує розвиватися й сьогодні, з моменту включення нових CNA у 2016 році. Таким чином, ініціатива розширюється з кожною організацією, яка приєднується до MITRE як співавтор [5, 6].

Як визначаються CVE?

Коли справа доходить до того, як визначається CVE, є просте емпіричне правило, яке потрібно пам’ятати: усі CVE є недоліками, але не всі недоліки є CVE. Недолік оголошується CVE, якщо він відповідає трьом дуже конкретним критеріям:

Помилка може бути виправлена окремо від будь-яких інших помилок.

Постачальник програмного забезпечення визнає та документує недолік як такий, що завдає шкоди безпеці його користувачів.

Вразливість впливає на єдину кодову базу. Дефектам, які впливають на кілька продуктів, призначається кілька CVE.

Кожному дефекту, визначеному як CVE, присвоюється номер, який називається ідентифікатором CVE або CVE ID. Ці ідентифікатори призначаються одним із понад 220 центрів нумерації CVE або скорочено CNA з 34 країн.

За даними MITER, CNA представлені різними організаціями, від постачальників програмного забезпечення та проектів з відкритим кодом до постачальників послуг винагороди за помилки та дослідницьких груп. Усі ці організації мають право призначати ідентифікатори CVE та публікувати їх записи за допомогою програми CVE. Протягом багатьох років до програми CNA приєднувалися асоціації та підприємства з багатьох галузей. Вимоги для цього мінімальні й не передбачають укладення контракту чи грошової комісії.

Міжнародним стандартом для ідентифікаторів CVE є CVE-[Year]-[Number]. Звичайно, частина [Year] представляє рік, коли було повідомлено про вразливість або ризик. [Номер] — це серійний маркер, призначений відповідним CNA.

Життєвий цикл запису CVE [6]

Життєвий цикл запису CVE складається з шести етапів:

1. Discover (Відкрийте для себе) - особа чи організація виявляють нову вразливість.

2. Report (Звіт) - discoverer повідомляє про вразливість учаснику програми CVE.

3. Request (запит) - учасник програми CVE запитує ідентифікатор CVE (CVE ID).

4. Reserve (резерв) - ідентифікатор зарезервовано, що є початковим станом запису CVE.

Зарезервований стан означає, що зацікавлені сторони CVE використовують ідентифікатор CVE для координації та керування вразливістю на ранній стадії, але CNA ще не готовий оприлюднити вразливість.

5. Submit (надіслати) - учасник Програми CVE подає деталі.

Деталі включають, але не обмежуються продуктами, на які впливає; уражені або виправлені версії продукту; тип уразливості, першопричина або вплив; і принаймні одне публічне посилання.

6. Publish (опублікувати) - після включення мінімально необхідних елементів даних до запису CVE відповідальний CNA публікує його в списку CVE.

Запис CVE тепер доступний для завантаження та перегляду.

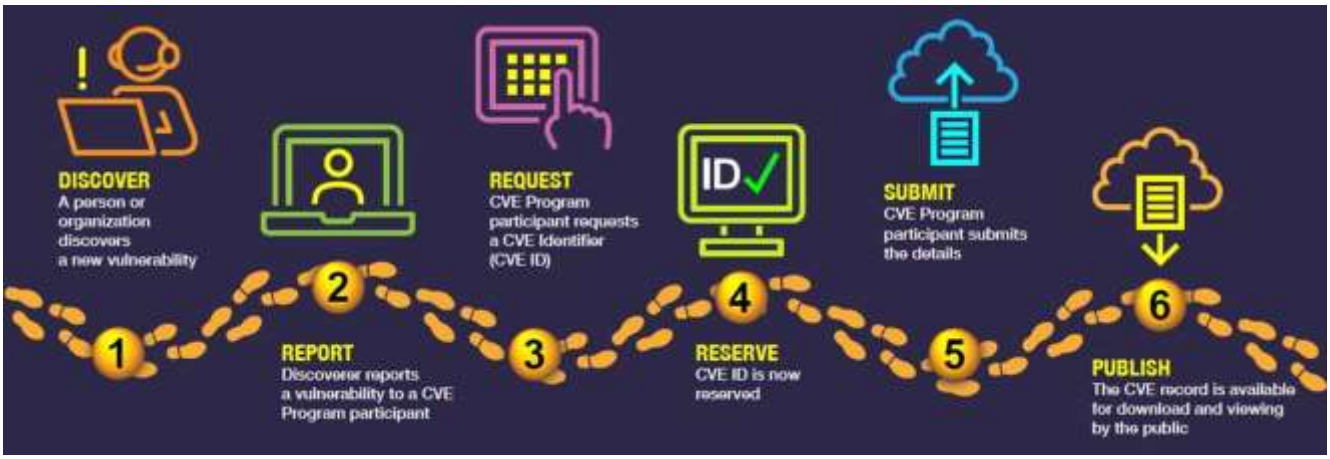


Рис.1.2. Життєвий цикл запису CVE [6]

Загальна система оцінки вразливості

Оцінка CVSS (загальна система оцінки вразливості) представляє числову інтерпретацію (за шкалою від 0 до 10) серйозності CVE . Команди Infosec часто використовують рейтинги CVSS як частину процесу оцінки вразливостей, щоб визначити пріоритетність усунення вразливостей із високим ризиком.

Скільки існує CVE?

Тисячі нових CVE публікуються щороку з моменту заснування програми в 1999 році. Умомент, коли я пишу цю статтю, офіційний веб-сайт CVE.org повідомляє про 177 353 CVE-записів у списку. Це зводиться до в середньому 7711 уразливостей і експозицій на рік, але реальність останніх кількох років полягає в тому, що ця цифра майже вдвічі більша: повідомляється про 15 000 нових CVE.

З понад 177 000 CVE, які зараз зареєстровані, більше половини належать до 50 найкращих світових постачальників програмного забезпечення. Наприклад, такі компанії, як Microsoft або Oracle, мають понад 6000 недоліків у своїх продуктах.

Програма CVE є важливою і була створена для спрощення обміну інформацією про відомі вразливості між організаціями. Це можливо, оскільки вищезазначені ідентифікатори CVE дають фахівцям з кібербезпеки можливість легко знаходити інформацію про недоліки в різних авторитетних джерелах, використовуючи один і той самий знаменник.

Завдяки цій системі організаціям пропонується постійно оновлювати свої стратегії безпеки відповідно до найновіших уразливостей і ризиків, які з'являються. На додаток до цього, список CVE є надійною базою для компаній, щоб оцінити охоплення рішень, які вони використовують, і вирішити, чи варто інвестувати в більш надійні засоби захисту чи ні.

Використання ідентифікаторів CVE також є кращим напрямком дій не лише для запобігання кібератакам, але й для виявлення вразливостей системи та реагування на них. Шукаючи ідентифікатори CVE у разі виявлення проблеми, організації можуть досить швидко отримати точну інформацію про певний експлойт із кількох сертифікованих джерел, що дозволяє їм належним чином визначати пріоритети щодо його подолання.

Чи можуть кіберзлочинці використовувати CVE? На жаль, так само, як організації можуть використовувати CVE для своєї вигоди, так само можуть і групи кіберзлочинців. Коли вразливості стають відомі широкому загалу, між їх публікацією та пом'якшенням для всіх користувачів програмного забезпечення існує певний проміжок часу, яким можуть скористатися хакери.

Однак переваги CVE значно переважують їхні недоліки. По-перше, список обмежений лише відомими вразливими місцями та ризиками. Крім того, обмін інформацією в рамках спільноти кібербезпеки є одним із найнадійніших способів зменшити вектори кібератак у поєднанні з надійними рішеннями кібербезпеки, які підтверджують ці знання.

Список CVE – це просто список. Але коли справа доходить до запобігання атакам, найбільше значення має швидкість виконання виправлень CVE. Чим довший час, тим вищий ризик бути використаним. Стратегія кібербезпеки організації завжди повинна враховувати останні загрози, але це означає, що потрібна стратегія.

1.4. Статистика вразливостей кібербезпеки

Уразливості кібербезпеки послаблюють системи та відкривають двері для кіберзлочинців.

Уразливість кібербезпеки зазвичай відноситься до недоліку програмного коду, який дозволяє зловмиснику отримати доступ до мережі або системи. Уразливі місця роблять компанії та окремих осіб відкритими для низки загроз, включаючи зловмисне програмне забезпечення та захоплення облікових записів [7,8].

Існує величезна кількість можливих вразливостей і потенційних наслідків для їх використання. Національна база даних про вразливості (NVD) уряду США, яка доповнюється списком Загальних вразливостей і вразливостей (CVE), наразі містить понад 176 000 записів. Одним із відомих прикладів уразливості кібербезпеки є недолік CVE-2017-0144 Windows, який відкрив двері для атак програм-вимагачів WannaCry через експлойт EternalBlue. Ще одним сумно відомим випадком є ботнет Mirai, який поширився через використання багатьох недоліків.

Після виявлення вразливостей розробники зазвичай швидко працюють над випуском оновлення або «патча». В ідеалі всі користувачі встановлюють оновлення до того, як зловмисники зможуть використати вразливість. Але реальність така, що в багатьох випадках зловмисники швидко атакують, щоб скористатися відомою слабкістю. Крім того, навіть коли випущено виправлення, повільне впровадження оновлень означає, що зловмисники можуть використовувати вразливості через роки після їх виявлення.

Розглянемо найпопулярнішу статистику вразливостей у системі кібербезпеки та факти.

1. У першому кварталі 2022 року було опубліковано понад 8000 уразливостей.

База даних NVD містить 8051 вразливість, опубліковану в першому кварталі 2022 року. Це приблизно на 25 відсотків більше, ніж за той самий період минулого року. Якщо ці цифри вірні, це означатиме невелике зростання порівняно з минулим роком, оскільки у 2021 році їх було опубліковано близько 22 000.

2. Половина внутрішніх уразливостей веб-додатків вважаються високими.

У звіті Edgescan про статистику вразливостей за 2022 рік проаналізовано серйозність уразливостей веб-додатків. Було виявлено, що майже кожна десята вразливість у додатках, що виходять з Інтернету, вважається високою або критичною. Це зросло до 15 відсотків, якщо мета зазвичай обробляла онлайн-платежі [8].

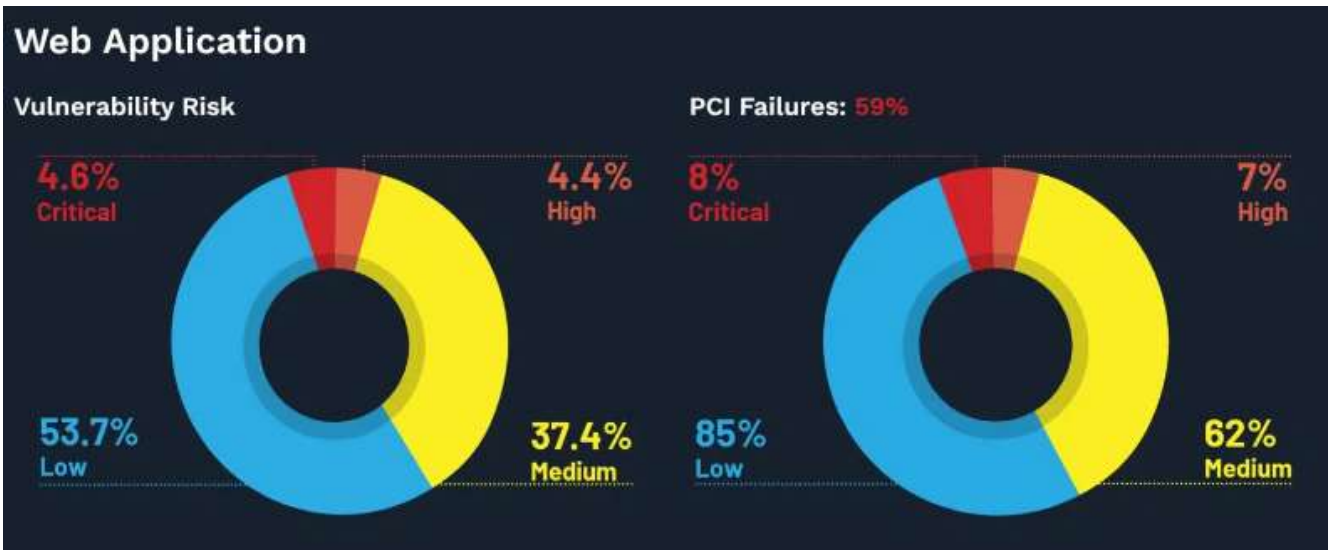


Рис. 1.3 Статистика вразливостей вразливостей веб-додатків за 2022 рік [7]

3. Організації з понад 100 співробітниками бачать більше вразливостей із високим або критичним ризиком

У звіті Edgescan за 2021 рік було розподілено ступінь серйозності вразливостей відповідно до розміру компанії [8]. Невеликі компанії зі 100

співробітниками або менше мали найменшу частку вразливостей із середнім, високим або критичним ризиком (загалом п’ять відсотків). Компанії з понад 10 000 співробітників бачать найбільшу частку вразливостей із середнім і критичним ризиком, тоді як організації середнього розміру з 101–1000 співробітниками бачать найбільшу частку вразливостей з високим ризиком.

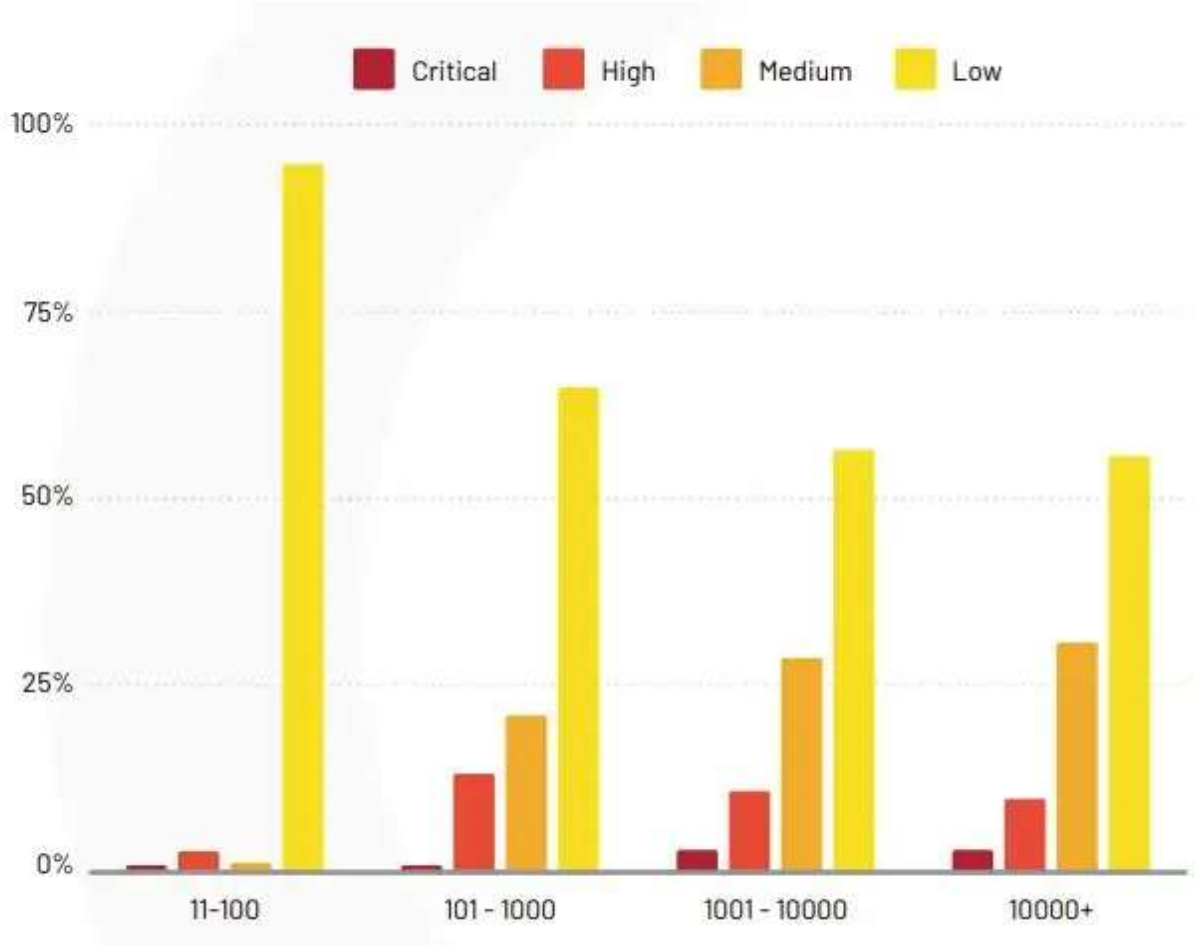


Рис.1.4. Ступінь серйозності вразливостей відповідно до розміру компанії [8]

4. Середній час до відновлення (MTTR) становить приблизно 58 днів

За даними Edgescan, середній час, витрачений на усунення вразливостей в Інтернеті, становив 57,5 днів. Це незначне покращення порівняно з минулим роком, коли MTTR становив 60,3 дня [7,8].

Однак це залежить від галузі. Для державних адміністрацій, наприклад, MTTR становив 92 дні, тоді як для організацій охорони здоров’я – лише 44 дні.

Дані показують, що чим менше постраждала організація, тим швидше вона може відновитися.

5. Найсерйознішою уразливістю 2021 року була CVE-2021-44228

CVE-2021-44228 — це вразливість, що впливає на Log4j, бібліотеку реєстрації з відкритим кодом, яка використовується в тисячах проектів, програм і веб-сайтів. Ця вразливість дозволяла зловмисникам запускати довільний код на будь-якій ураженій системі, і хоча її було швидко виправлено, дуже ймовірно, що велика кількість уразливих програм залишається онлайн.

6. Найдавнішій уразливості, виявленій у 2020 році, був 21 рік

Цікаво, що Edgescan знайшов досить стару вразливість, яка існує з 1999 року: CVE-1999-0517. Це впливає на простий протокол керування мережею версії 2 (SNMPv2), який використовується для керування пристроями та комп'ютерами в IP-мережі. Уразливість може дозволити несанкціонований доступ SNMP через вгаданий рядок спільноти. Його базова оцінка загальної системи оцінки вразливостей (CVSS) становить 7,5, що робить його слабким місцем високого рівня [7,8].

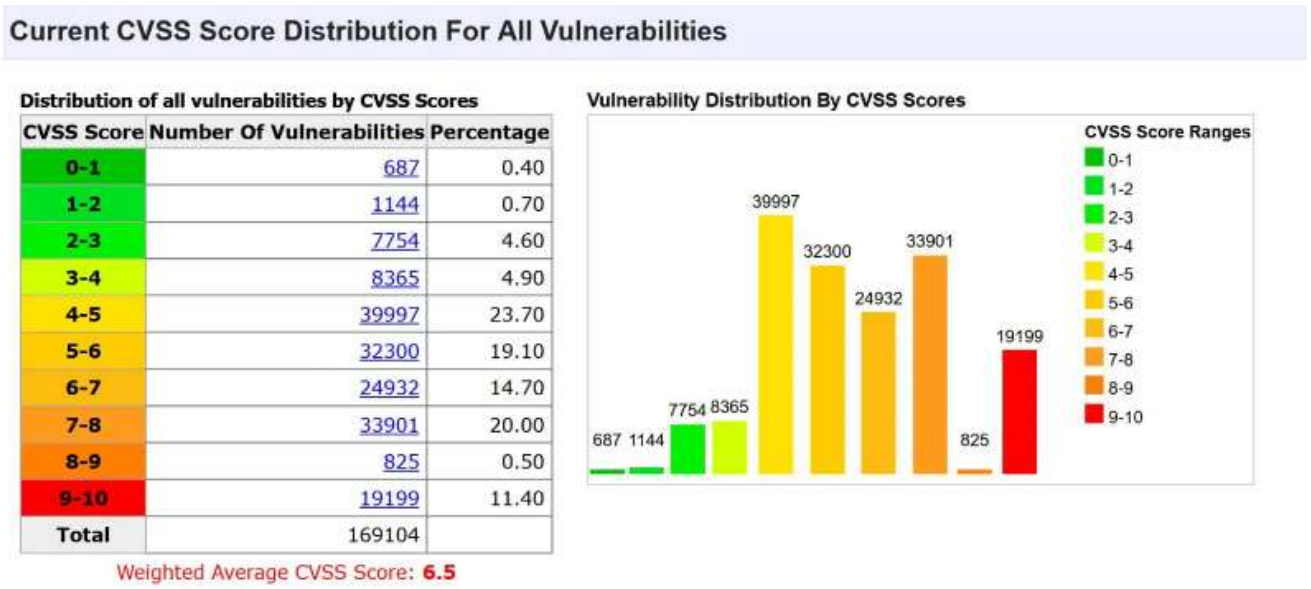
7. Перші критичні вразливості у великій хмарній інфраструктурі були виявлені в січні 2020 року

На початку 2020 року дослідники Check Point виявили та повідомили про критичні вразливості в інфраструктурі Microsoft Azure. Згідно зі статтею Check Point, де детально описується вразливість, дослідники «хотіли спростувати припущення про те, що хмарні інфраструктури безпечні». Уразливості отримали найвищу оцінку CVSS 10,0. Якісна оцінка тяжкості 9,0-10,0 є «критичною» [7].

Ці вразливості дозволяють зловмисникам скомпрометувати програми та дані користувачів, які використовують те саме обладнання.

8. Більше 11% вразливостей мають критичний бал

Відповідно до CVE Details , із приблизно 176 000 вразливостей понад 19 000 мають оцінку CVSS 9,0–10,0. При цьому переважна більшість (77,5 відсотка) мають оцінку від 4,0 до 8,0.



Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	687	0.40
1-2	1144	0.70
2-3	7754	4.60
3-4	8365	4.90
4-5	39997	23.70
5-6	32300	19.10
6-7	24932	14.70
7-8	33901	20.00
8-9	825	0.50
9-10	19199	11.40
Total	169104	

Weighted Average CVSS Score: **6.5**

Рис.1.5. Статистика вразливостей, які мають критичний бал [7]

9. 75% атак у 2020 році використовували вразливості, яким було принаймні два роки

Згідно зі звітом Check Point Cyber Security Report 2021 , три з чотирьох атак скористалися недоліками, про які повідомлялося в 2017 році або раніше. І 18 відсотків атак використовували вразливості, які були розкриті в 2013 році або раніше, що робить їх принаймні сім років тому.

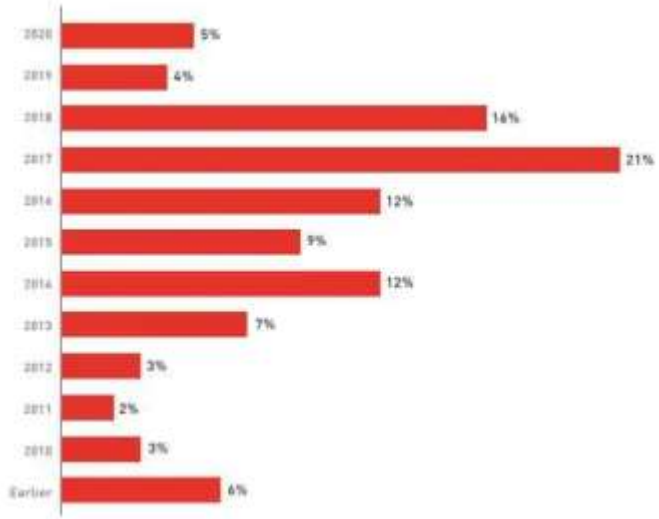


Рис.1.6. Відсоток атак у 2020 році використовували старі вразливості

10. У 2020 році кількість атак уразливостей віддаленого доступу Citrix зросла на 2066%.

За даними Check Point, у 2020 році кількість атак з використанням уразливостей у продуктах віддаленого доступу значно зросла. Кількість атак Citrix зросла більш ніж у 20 разів, а атак Cisco, VPN і RDP – на 41%, 610% і 85%. відповідно.

11. 31% компаній виявили спроби використання вразливостей програмного забезпечення

У звіті Positive Technologies за 2020 рік повідомляється, що майже третина виявлених загроз пов'язана зі спробами використання програмного забезпечення. Згідно зі звітом: «Більше половини спроб стосувались уразливості CVE2017-0144 у реалізації протоколу SMBv1. Це та сама вразливість, яка використовується сумнозвісним програмним забезпеченням-вимагачем WannaCry, і для якої у 2017 році було випущено виправлення. Але зловмисники зберегли її у своїх арсеналах, шукаючи комп'ютери, які не оновлювалися протягом останніх 3,5 років».

12. Уразливості високого ризику присутні на периметрах мережі 84% компаній

Інше дослідження, проведене Positive Technologies, виявило тривожну статистику про те, що 84 відсотки компаній мають уразливі місця високого ризику у своїх зовнішніх мережах. Також виявилося, що більше половини з них можна видалити, просто встановивши оновлення.

13. Кожена четверта вразливість залишається відкритою через 18 місяців

Досить тривожним висновком звіту Veracode за 2021 рік є те, що через півтора року близько 27 відсотків вразливостей все ще залишаються відкритими.

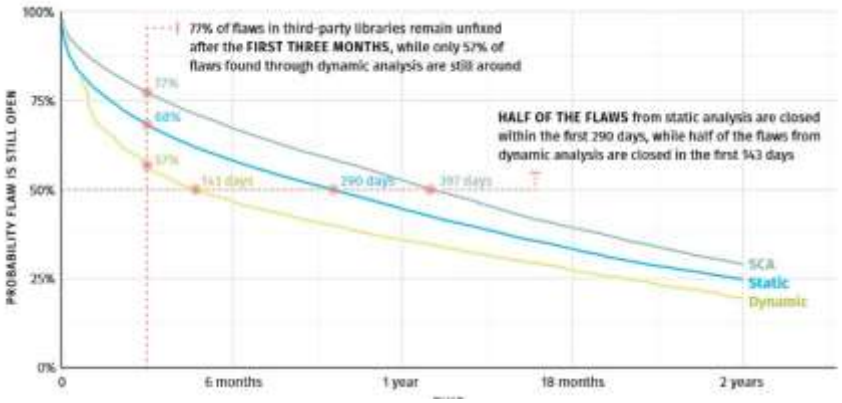


Рис.1.6. Статистика відкритих вразливостей

23. Часте сканування корелює з набагато швидшим часом виправлення

Veracode виявив, що програми, які регулярно сканували вразливості, мали набагато швидший середній час виправлення. Ті, хто проводив понад 260 сканувань на день, усували 50 відсотків недоліків протягом 62 днів. Цей час було збільшено до 217 днів для додатків, які виконують лише 1–12 сканувань на день.

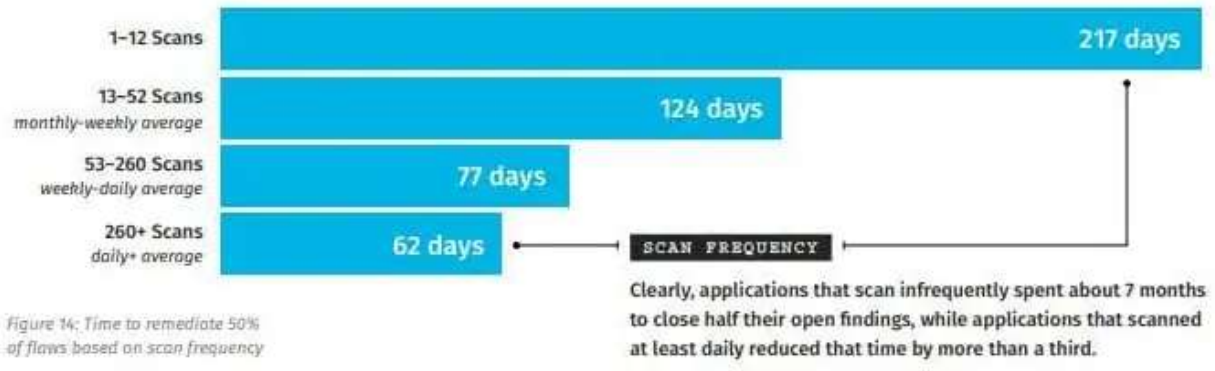


Рис.1.7. Частота сканувань та час на їх виправлення

Підводячи підсумок, можна сказати, що управління вразливістю є критично важливим компонентом стратегії інформаційної безпеки будь-якої організації. Це допоможе організаціям зменшити ризик кібератак, захистити конфіденційні дані, дотримуватися нормативних актів, підвищити ефективність роботи та підвищити репутацію бренду.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ КЕРУВАННЯ ВРАЗЛИВОСТЯМИ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

2.1. Визначення життєвого циклу управління вразливостями

Життєвий цикл керування вразливими місцями — це безперервний послідовний процес кібербезпеки, який полягає в виявленні, оцінці, визначенні пріоритетів і діях проти вразливостей з метою посилення безпеки організації.

Уразливості можна описати як діри, виявлені в IT-системі, які роблять систему відкритою для кібератак. Деякі організації вважають, що їхні системи бездоганні, тому що на них досі не вплинули кібератаки, що в деяких випадках може бути правдою, але в багатьох випадках компанії не усвідомлюють, що їхні системи можуть мати недоліки, доки не стане надто пізно. діяти. Ось чому методи управління вразливістю відіграють вирішальну роль у безпеці вашої компанії та конфіденційності даних [4].

Управління вразливістю стосується процесу проактивного виявлення, запобігання, пом’якшення та класифікації вразливостей в IT-системі на основі рівня загрози, якою вони володіють. Уразливості потрібно усувати відразу після їх виявлення , інакше зловмисники можуть скористатися ними, щоб проникнути у вашу систему та викрасти дані. Це важлива частина, яка є наріжним каменем для першокласної стратегії безпеки [4].

Процес керування вразливістю вимагає проходження кількох кроків для належного захисту ваших систем. Разом ці кроки представляють життєвий цикл керування вразливістю, і він розроблений, щоб дати можливість підприємствам виявляти вразливості в безпеці своїх комп’ютерних систем, ранжувати активи, оцінювати, звітувати та виправляти недоліки, а потім підтверджувати, що їх виправлено.

Життєвий цикл керування вразливістю складається з наступних кроків та етапів. Визначимо їх детальніше [4].

Життєвий цикл керування вразливістю можна розділити на п’ять етапів, кожен із яких має свою особливу роль у виявленні, запобіганні, пом’якшенні та класифікації вразливостей у вашій IT-інфраструктурі.

Рис. 2.1. Життєвий цикл управління вразливостями [4]

П’ять кроків є послідовними, тому, коли завершується останній крок життєвого циклу, процес запускається знову.

Крок 1: оцінка

Першим етапом життєвого циклу управління вразливістю є етап оцінки. На цьому етапі експерти з кібербезпеки звужують і визначають активи, які потрібно проаналізувати на наявність вразливостей. Наступним етапом процесу оцінки є оцінка кожного активу на наявність вразливостей і створення звіту для визначення тих, які потребують виправлення, додаткових досліджень або виправлення.

Існує два широко використовувані методи для завершення оцінки вразливості: використання «агента», що вимагає встановлення датчика на окремих активах для виявлення вразливостей, або використання мережевого рішення, яке вимагає підключення всіх кінцевих точок до однієї мережі.

Крок 2: визначення пріоритетів

Після виявлення та оцінки вразливостей у системі починається процес пріоритезації. На цьому етапі необхідно виконати три підетапи. По-перше, виявленим вразливостям потрібно присвоїти значення на основі їх важливості. Оскільки вразливості тепер упорядковані на основі їх важливості, настав час оцінити загрозу для кожного активу. Виходячи з рівня ризику, можливо розставити пріоритети для відновлення активів, від найбільш до найменш ризикованих.

Крок 3: Дія

Коли є є вразливі місця, виявлені та ранжовані на основі рівня впливу, який вони приносять активам, на які впливають. Маючи інформацію, зібрану на перших кроках, настав час розпочати процес усунення вразливостей. Існує більше способів, за допомогою яких можна виправити вразливості залежно від рівня загрози:

Низький рівень ризику: можна взяти на себе ризики активів для інформаційної системи організації;

Середня вразливість: для вищих рівнів уразливості можна зменшити вразливість, щоб не дати зловмиснику скористатись уразливістю за допомогою політик безпеки;

Висока вразливість: для ресурсів, які мають високий рівень уразливості, рекомендується повністю усунути вразливість за допомогою виправлень.

Крок 4: Переоцінка

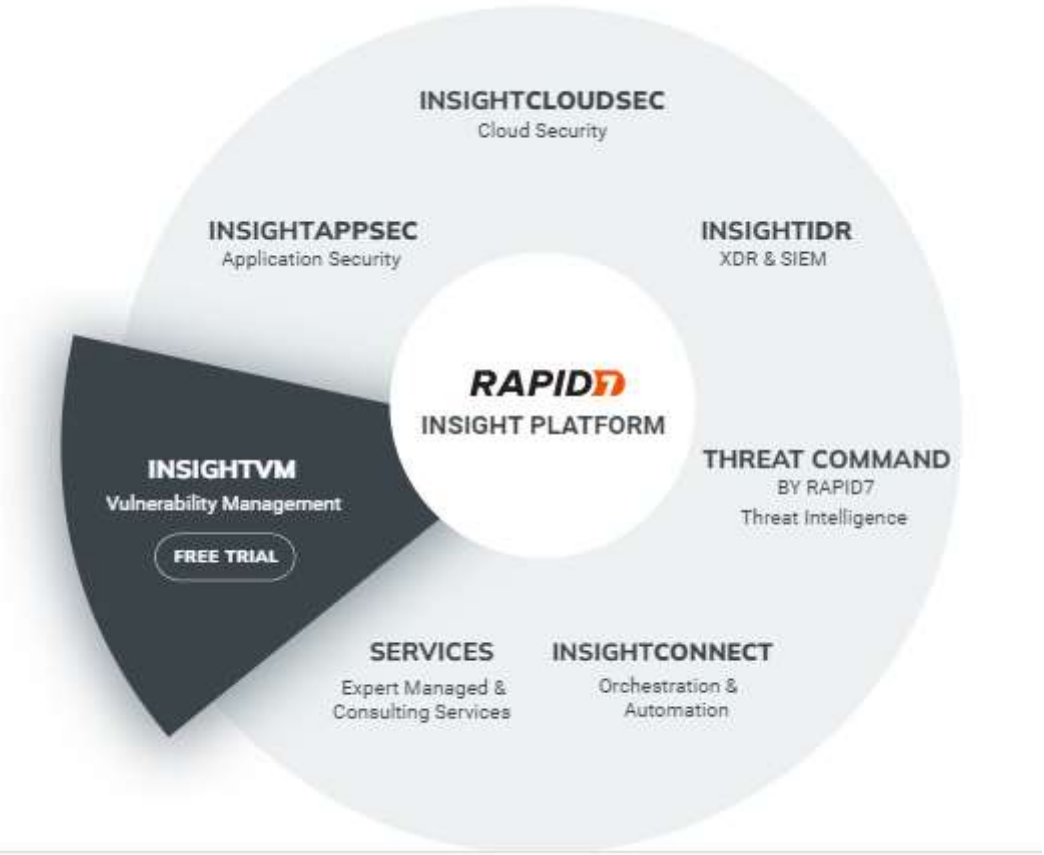
Після усунення вразливостей і застосування правильного рішення на основі рівня загрози, яку вони приносять системі, необхідна повторна оцінка. Процес повторної оцінки дасть вам уявлення про те, чи були дії, які ви вжили для усунення вразливості, ефективними чи ні.

Крок 5: Покращення

Це останній крок у життєвому циклі керування вразливістю. Після виконання всіх попередніх кроків ви можете виявити недоліки, які потрібно виправити. Таким чином, регулярно переглядаючи життєвий цикл, можна знайти

способи покращити та посилити безпеку своїх систем, щоб зловмисники не могли втручатися у вашу компанію.

2.2. Аналіз можливостей платформи Rapid 7



Рішення платформи Rapid 7 Insight включає:

InsightIDR XDR і SIEM;

Threat Intelligence (Розвідка загроз) - Threat Command;

Vulnerability Management (Управління вразливістю) – InsightVM;

Dynamic Application Security Testing (Динамічне тестування безпеки додатків) - InsightAppSec;

Orchestration & Automation (SOAR) (Оркестровка та автоматизація (SOAR)) - InsightCOnnect;

Cloud Security (Хмарна безпека) – InsightCloudSec;

2.3. Аналіз функцій InsightVM щодо виявлення вразливостей в інформаційній системі

InsightVM дозволяє чітко виявляти та усувайте ризики, використовуючи повне сканування мережі організації. Це дозволяє виявляти ризики для всіх кінцевих точок і інформаційної системи.

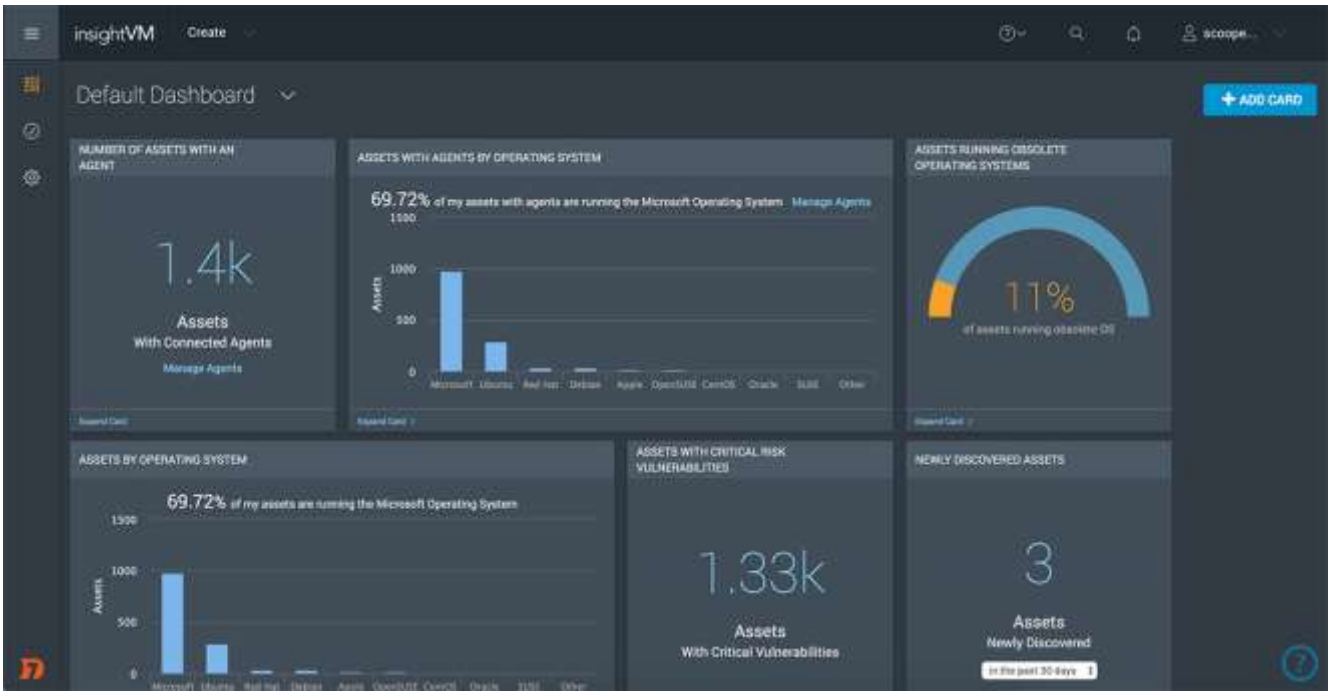
Особливість InsightVM в тому, що з її використанням дозволяє усунути вразливості. Розставка пріоритетів для ризиків і покрокові вказівки IT-спеціалістам і DevOps надають більш ефективне їх усунення.

Оцінка політики дозволяє відстежувати та повідомляти про прогрес. Це можливо за рахунок перегляду свої ризиків в режимі реального часу прямо з інформаційної панелі.

Функції керування вразливістю InsightVM:

Легкий агент кінцевої точки

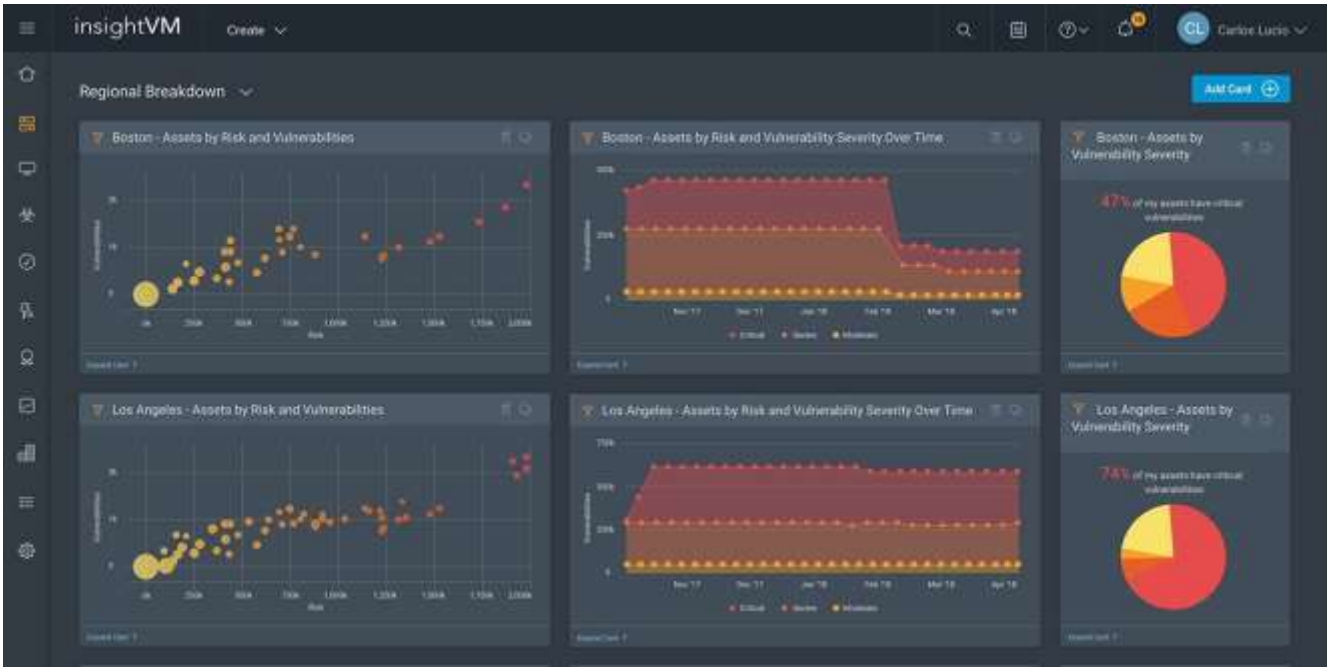
Агент Rapid7 Insight автоматично збирає дані з усіх кінцевих точок, навіть від віддалених співробітників і конфіденційних активів, які не можна активно сканувати, або які рідко приєднуються до корпоративної мережі.



Живі інформаційні панелі

Більшість інформаційних панелей програмного забезпечення є статичними: це знімок ризику в певний час, на який неможливо натиснути та миттєво застарів.

Інформаційні панелі InsightVM Live є живими та інтерактивними за своєю природою. Це дозволяє легко створювати спеціальні картки та повні інформаційні панелі для будь-кого — від системних адміністраторів до CISO — і запитувати кожну картку простою мовою, щоб відстежувати прогрес вашої програми безпеки.

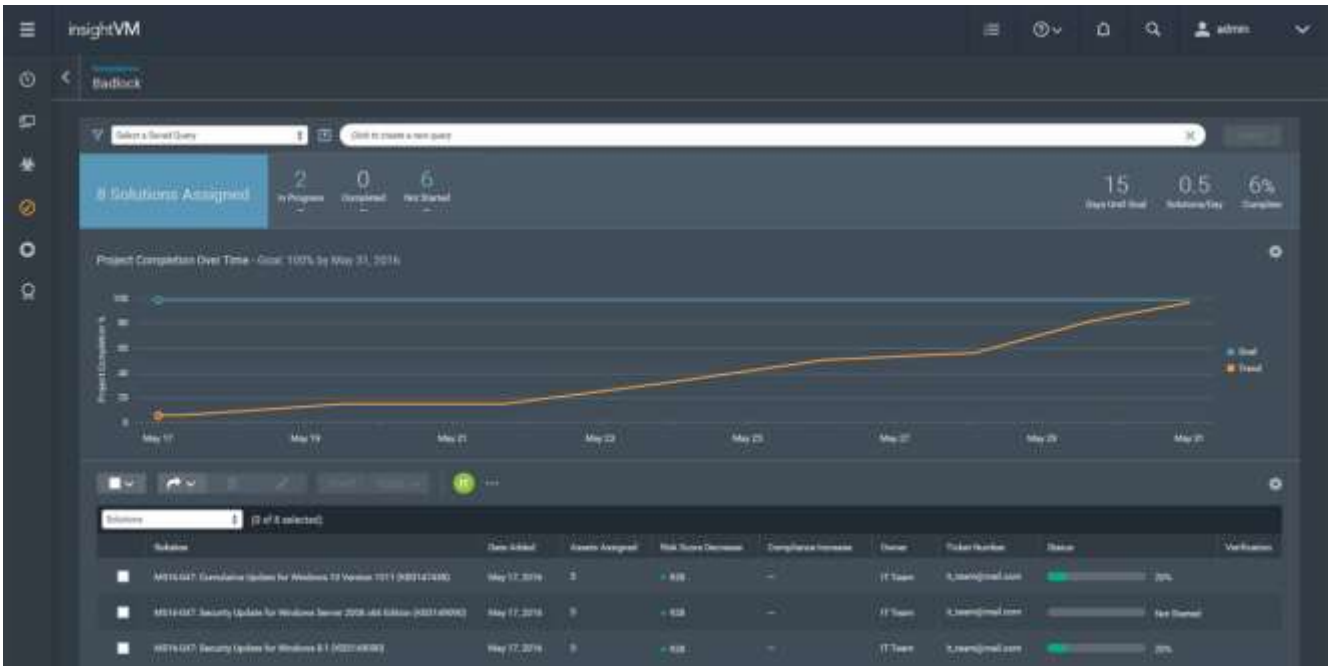


Пріоритезація реального ризику

Оцінки ризику на основі CVSS призводять до тисяч «критичних» уразливостей. Жодна компанія, навіть з армією аналітиків, не має на це часу. Наша оцінка реального ризику надає більш ефективну шкалу від 1 до 1000, яка базується на ймовірності використання зловмисником уразливості під час реальної атаки. Завдяки підтримці каналів загроз і бізнес-контексту InsightVM дає змогу визначати пріоритети вразливостей так, як це зробили б зловмисники.

IT-інтегровані проекти відновлення

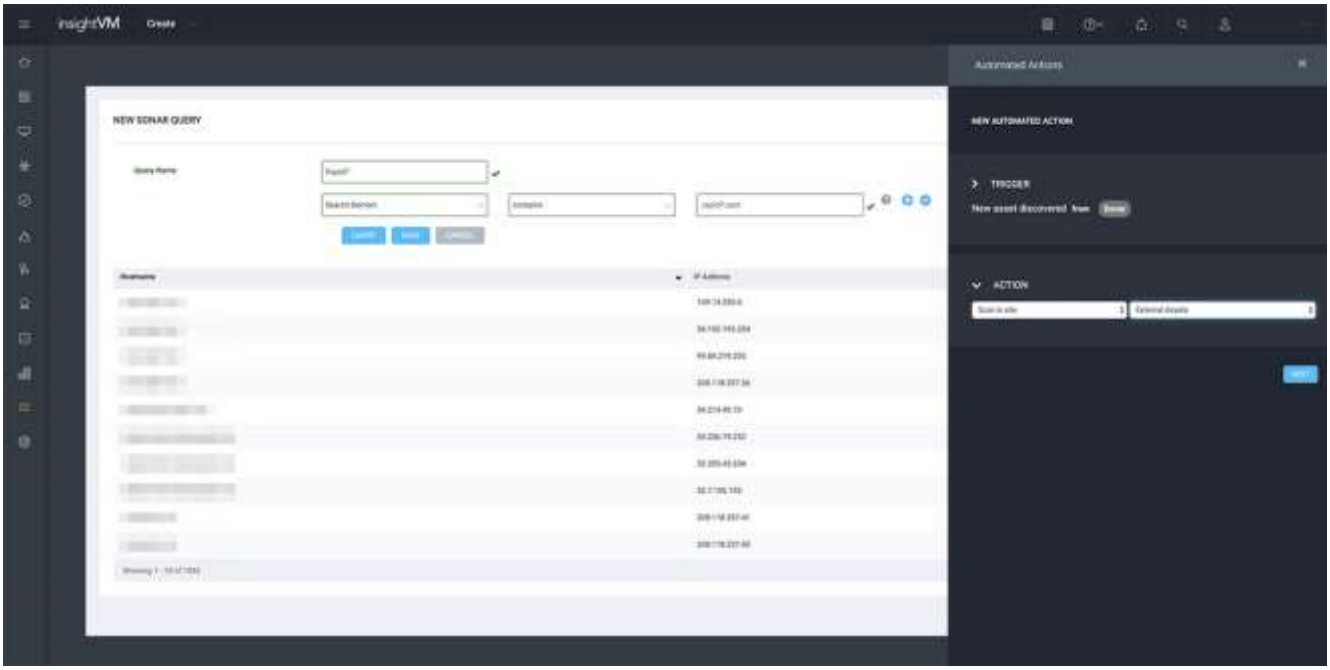
Використання цієї функції дозволяє викинутие тисячі сторінок звітів про виправлення, складні електронні таблиці та незрозумілі теги електронної пошти. За допомогою Remediation Projects групи безпеки можуть призначати та відстежувати обов'язки з виправлення в режимі реального часу, забезпечуючи постійну видимість того, наскільки добре вирішуються проблеми.



Моніторинг поверхні атаки за допомогою Project Sonar

У міру того, як організація росте, а інфраструктура стає складнішою, стежити за мінливою поверхнею атак стає все складніше. InsightVM напряму

інтегрується з Project Sonar, дослідницьким проектом Rapid7, який регулярно сканує загальнодоступний Інтернет, щоб отримати уявлення про глобальний вплив поширених вразливих зон. Використовуючи Attack Surface Monitoring із Project Sonar, можна бути впевнені, що маєте знання про вразливості на всіх своїх зовнішніх активах, як відомих, так і невідомих.



Інтегровані канали загроз

Канали загроз в InsightVM дозволяють мені відсортувати шум інших уразливостей «високого» ступеня тяжкості з низькою ймовірністю експлуатації та перейти безпосередньо до важливих вразливостей — тих, які активно атакують зловмисники.

Цілі та SLA

Крім сповіщень про вразливості високої критичності та обмінних повідомлень електронною поштою, які часто надходять із оцінкою вразливості, ми не часто запитуємо себе: «Яка справжня ефективність моєї програми керування вразливістю?» Відповісти на це запитання стає все важче, коли виконання завдань із відновлення охоплює кілька команд і проектів. Ось де з'являються цілі та SLA.

Завдяки цілям і угодам про рівень обслуговування можна переконатися, що досягаєте (і відстежуєте) прогрес у досягненні цілей і угод про рівень обслуговування (SLA) належним темпом, а також підтримуєте відповідність стандартам, які встановлено для своєї програми.

Простий у використанні RESTful API

Команда з кібербезпеки повинна мати повноваження контролювати Консоль безпеки, а не навпаки. RESTful API InsightVM дозволяє легко досягти більшого у вашій унікальній програмі безпеки. Його створено для легкої автоматизації практично будь-якого аспекту керування вразливістю, від збору даних до аналізу ризиків, і інтеграції можливостей InsightVM з іншими вашими процесами.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЗАСТОСУВАННЯ ПРОГРАМНОГО КОМПЛЕКСУ RAPID 7 INSIGHTVM

3.1. Початок роботи з консоллю безпеки InsightVM

Консоль безпеки — це локальний сканер уразливостей і система керування. Його основні функції дозволяють визначати ризики у середовищі інформаційної системи організації, упорядковувати пристрої та визначати пріоритети усунення.

InsightVM містить такі компоненти:

Консоль безпеки - це компонент, який використовується для створення сайтів, сканування, створення звітів і багато іншого. Доступ до консолі безпеки здійснюється через веб-інтерфейс користувача через будь-який із підтримуваних браузерів.

База даних PostgreSQL -вбудована база даних PostgreSQL, яка зберігає всі дані сканування ресурсів і використовується для створення звітів.

Механізм сканування - Scan Engines відповідають за виконання завдань сканування активів. Особливістю є те,, що Scan Engines лише тимчасово зберігає дані сканування перед надсиланням їх назад на консоль безпеки для інтеграції та тривалого зберігання.

Для початку роботи на платформі необхідно створити сайт.

Сайт — це набір активів, призначених для сканування. Ви повинні створити сайт, щоб запустити сканування свого середовища та знайти вразливі місця.

Сайт складається з:

цільові активи;

шаблон сканування;

один або кілька скануючих механізмів;

інші налаштування, пов’язані зі скануванням, наприклад розклади або сповіщення.

Існують різні способи додавання активів на сайт. Вказати цільові активи можна кількома способами:

за іменем особи, адресою чи діапазоном;

за назвою групи активів;

за допомогою динамічного підключення для відкриття.

Зазначення окремих активів або діапазонів є хорошим вибором для ситуацій, коли адреси активів, імовірно, залишатимуться стабільними.

Зазначення груп ресурсів дає змогу сканувати на основі логічних груп, які було створено раніше. У разі сканування динамічних груп активів можна сканувати залежно від того, чи відповідають активи певним критеріям. Наприклад, можна сканувати всі активи, операційною системою яких є Ubuntu.

Додавання активів через з’єднання ідеально підходить для цільового середовища з високим плином часу, наприклад розгортання віртуалізованих активів. Віртуальні машини не є незвичайними для постійних змін, таких як встановлення різних операційних систем, підтримка різними пулами ресурсів або їх увімкнення та вимкнення. Оскільки членство активів у такому сайті базується на постійному виявленні віртуальних активів, список активів змінюється відповідно до зміни цільового середовища, що відображається в результатах кожного сканування.

Сайт можна створювати через агентів Rapid7 Insight.

Сайт агентів Rapid7 Insight Agents — це спеціальний сайт, який автоматично містить усі активи, на яких інстальовано та запущено агенти Rapid7 Insight Agents. Цей сайт не можна видалити чи відредагувати.

Розглянемо сканування різних типи активів для різних цілей у різний час. Шаблон сканування — це попередньо визначений набір атрибутів сканування, які можна вибрати швидко, а не визначати властивості вручну, наприклад цільові активи, служби та вразливості. InsightVM містить різноманітні попередньо налаштовані шаблони сканування, які допоможуть вам оцінити свої вразливості відповідно до найкращих практик для певної потреби.

Використання різноманітних шаблонів є хорошою ідеєю, оскільки ви можете поглянути на свої активи з різних точок зору. Коли ви вперше скануєте сайт, ви можете просто виконати сканування для виявлення, щоб дізнатися, що

працює у вашій мережі. Потім ви можете виконати сканування вразливостей за допомогою шаблону повного аудиту, який включає широкий і вичерпний діапазон перевірок. Якщо у вас є активи, які збираються запустити у виробництво, можливо, саме час сканувати їх за допомогою шаблону відмови в обслуговуванні. Небезпечні перевірки — це хороший спосіб перевірити їх стабільність, не впливаючи на робочий процес у вашому бізнес-середовищі. Ви також можете застосувати різні шаблони до різних типів активів; наприклад, веб-аудит для веб-серверів і веб-додатків.

Глобальний адміністратор також може налаштувати шаблони сканування або створити нові відповідно до потреб вашої організації. Створивши сайти вибраних активів і застосувавши найбільш релевантний шаблон сканування, ви можете проводити сканування відповідно до ваших потреб. Особливістю є те, що сканування має збалансувати три важливі фактори продуктивності: час, точність і ресурси. Якщо ви налаштуєте шаблон для швидшого сканування, наприклад, додавши потоки, ви можете заплатити ціну за пропускну здатність.

Вибір шаблону сканування

Якщо ви хочете змінити шаблон сканування для існуючого сайту, клацніть піктограму «Редагувати» цього сайту в таблиці «Сайти» на домашній сторінці.

Якщо ви хочете вибрати шаблон сканування під час створення нового сайту, натисніть кнопку Створити сайт на домашній сторінці.

Вибір наявного шаблону сканування:

1. У Конфігурації сайту перейдіть на вкладку Шаблони .

2. Виберіть наявний шаблон сканування з таблиці. Типовим є повний аудит без Web Spider . Це хороше початкове сканування, оскільки воно забезпечує повне охоплення ваших активів і вразливостей, але працює швидше, ніж якби було включено Web Spider.

3. Збережіть зміни.

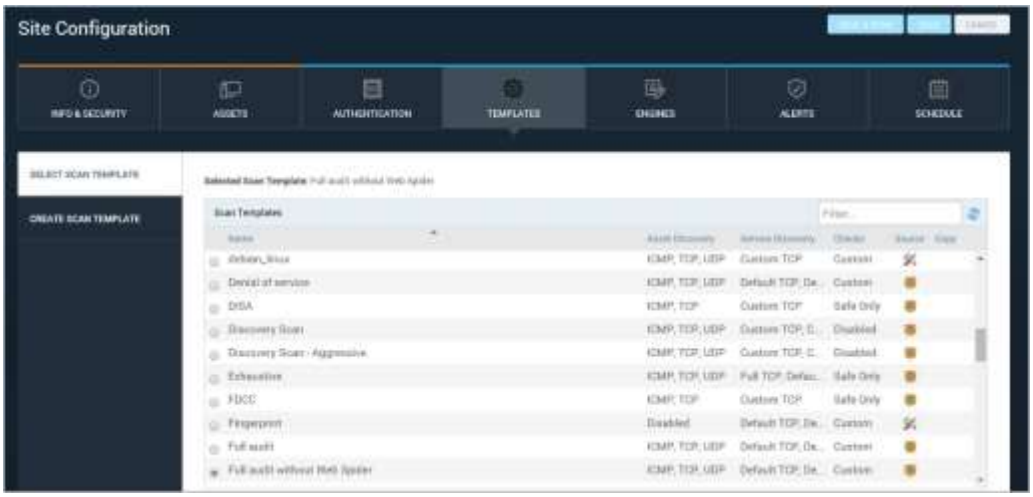


Рис. 3.1. Конфігурація сайту

Створення нового шаблону сканування

1. Натисніть піктограму «Копіювати» поруч із шаблоном у списку, на основі якого ви хочете створити новий, або натисніть «Створити шаблон сканування» , щоб почати з нуля.

Відкриється нова вкладка з конфігурацією шаблону сканування.

2. Змініть шаблон за бажанням.

3. Натисніть Зберегти .

4. Поверніться до вкладки з конфігурацією шаблону сканування .

5. Натисніть піктограму «Оновити» у верхній частині таблиці «Шаблони сканування» , щоб з’явився новий шаблон.

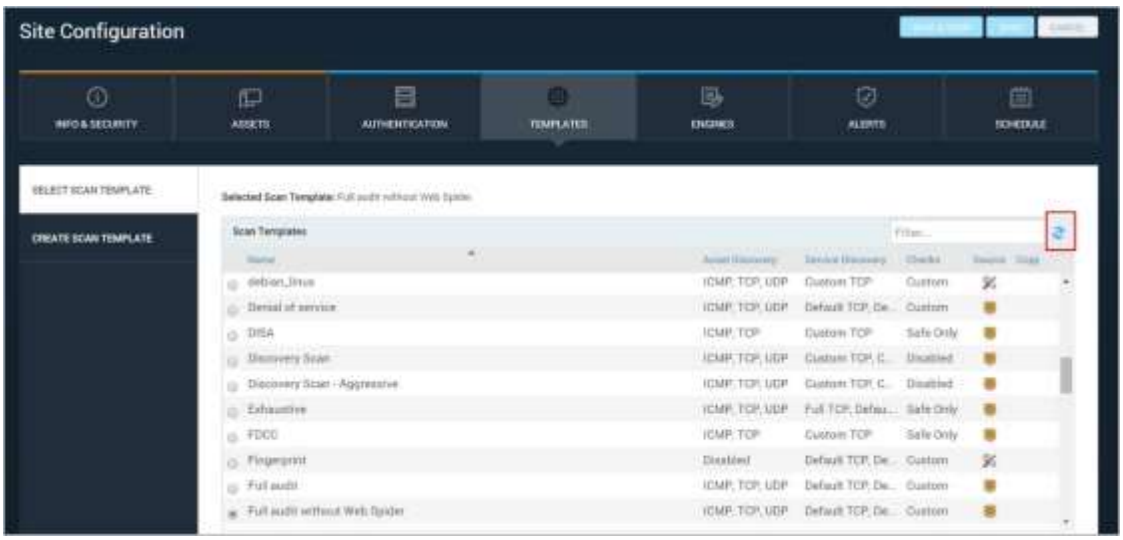


Рис.3.2. Оновлений шаблон сканування

6. Збережіть зміни.

Оцінка результатів сканування

Після виявлення всіх активів і вразливостей у вашому середовищі важливо проаналізувати цю інформацію, щоб визначити основні загрози безпеці, такі як активи з високим ризиком, уразливості, потенційне зараження шкідливим програмним забезпеченням або порушення політики.

Assess дає вказівки щодо перегляду та сортування результатів сканування, щоб визначити пріоритети безпеки. Він включає такі розділи:

Розташування активів і робота з ними: є кілька способів детально переглянути результати сканування, щоб знайти певні активи. Наприклад, ви можете знайти всі активи, які працюють під керуванням певної операційної системи або належать певному сайту. Цей розділ охоплює ці різні шляхи. Тут також обговорюється, як сортувати дані активів за різними показниками безпеки та як переглядати детальну інформацію про кожен актив.

Робота з уразливими місцями : залежно від вашого середовища сканування може виявити тисячі вразливих місць.

Пояснення показників уразливості

InsightVM використовує 3 метрики для представлення даних таблиці на основі вразливостей і ключових показників ефективності (KPI):

Вразливі місця;

Знайдені вразливості;

Випадки вразливості;

Вразливі місця

«Уразливість» — це унікальна, визначена та оприлюднена слабкість програмного забезпечення. Кожна вразливість зазвичай визначається системою перерахування, за винятком кількох винятків, які залежать від типу програмного забезпечення. Хоча існує кілька систем перерахування, система загальних вразливостей і вразливостей (CVE) є найбільш широко використовуваною та прийнятною системою сьогодні.

Знайдені вразливості

«Виявлення вразливості» — це визначення того, що актив певним чином уразливий до вразливості. Наприклад, якщо InsightVM показує 50 знайдених уразливостей для однієї вразливості, це означає, що 50 активів у вашій мережі вразливі до цієї вразливості.

Випадки вразливості

«Екземпляр вразливості» стосується конкретного стану активу, через який він стає вразливим. Актив може бути вразливим до тієї самої вразливості різними способами. Поширені причини цього сценарію:

Наявність кількох версій одного програмного забезпечення, встановленого на активі одночасно; усі вони вразливі до тієї самої вразливості

Бути вразливим до тієї самої вразливості через кілька мережевих портів

Екземпляри вразливості – це найбільш детальний доступний перегляд для визначення рівня ризику у вашому середовищі.

Робота зі звітами

Ви можете забажати, щоб будь-яка кількість людей у вашій організації переглядала дані про активи та вразливості без фактичного входу в консоль безпеки. Наприклад, головному спеціалісту з інформаційної безпеки (CISO) може знадобитися переглянути статистичні дані про ваші загальні тенденції ризиків з часом. Або членам вашої команди безпеки може знадобитися побачити найбільш критичні вразливості для конфіденційних активів, щоб вони могли визначити пріоритетність проектів виправлення. Для цих зацікавлених сторін може бути непотрібним або небажаним доступ до самої програми. Створюючи звіти, ви можете поширювати важливу інформацію людям, які її потребують, електронною поштою або інтеграцією експортованих форматів, таких як XML або CSV.

Звіти пропонують багато різноманітних способів перегляду даних сканування, від бізнес-орієнтованих перспектив до детальних технічних оцінок. Ви можете дізнатися все, що вам потрібно знати про вразливості та способи їх усунення, або ви можете просто перерахувати служби, запущені на ваших мережевих активах.

Ви можете створити звіт на сайті, але звіти не прив’язані до сайтів. Ви можете проаналізувати активи у звіті будь-якою кількістю способів, включаючи всі відскановані корпоративні активи або лише один.

Якщо ви перевіряєте відповідність PCI, ви використовуватимете такі шаблони звітів у процесі аудиту:

Атестація відповідності;

Резюме PCI;

Деталі вразливості.

3.1. Рекомендації щодо створення звітів

Шаблони та розділи звітів

Цей використовують додаток, щоб допомогти вам вибрати правильний вбудований шаблон звіту для ваших потреб.

Вбудовані шаблони звітів і включені розділи

Створення користувацьких шаблонів документів дає змогу включати стільки чи менше інформації у звіти, скільки цього вимагають ваші потреби. Наприклад, якщо вам потрібен звіт, у якому перераховано лише всі активи, упорядковані за рівнем ризику, найкращим рішенням може бути спеціальний звіт. Цей шаблон включатиме лише розділ. Або, якщо вам потрібен звіт, у якому перераховано лише вразливості, створіть шаблон із розділом.

Налаштування шаблону звіту документа передбачає вибір розділів, які будуть включені в шаблон. Кожен шаблон звіту в наступному розділі містить список усіх розділів, доступних для кожного шаблону звіту документа, включно з тими, які відображаються у вбудованих шаблонах звітів, і ті, які можна включити в налаштований шаблон. Ви можете виявити, що даний вбудований шаблон містить усі розділи, які вам потрібні в конкретному звіті, що робить непотрібним створювати спеціальний шаблон.

Формат звіту про активи (ARF)

XML-шаблон формату звіту про активи (ARF) упорядковує дані для подання результатів сканування політики та порівняльного аналізу на відповідність SCAP 1.2.

Аудиторський звіт

З усіх вбудованих шаблонів Аудит є найповнішим за обсягом. Ви можете використовувати його, щоб забезпечити детальний огляд стану безпеки у вашому середовищі. Шаблон звіту про аудит надає велику кількість детальної інформації про виявлені активи:

імена хостів та IP-адреси

виявлені служби, включаючи порти, протоколи та загальні проблеми безпеки

бали ризику, залежно від алгоритму скорингу, обраного адміністратором

користувачів і груп активів, пов’язаних з активами

виявлені бази даних*

виявлені файли та каталоги*

результати проведених оцінок політики*

сайти-павуки*

Він також надає багато інформації про вразливості:

постраждалих активів

описи вразливостей

рівні тяжкості

посилання та посилання на важливі джерела інформації, такі як поради щодо безпеки

загальна інформація про рішення

Крім того, шаблон звіту про аудит містить діаграми із загальною статистикою щодо виявлених уразливостей і рівнів серйозності.

Шаблон аудиторського звіту містить такі розділи:

Обкладинка

Виявлені бази даних

Виявлені файли та каталоги

Виявлені послуги

Виявлена системна інформація

Виявлені користувачі та групи

Виявлені вразливості

Резюме

Оцінка політики

Павукова структура веб-сайту

Картка звіту про вразливості за вузлом

Базове порівняння

Ви можете використовувати базове порівняння, щоб спостерігати за тенденціями, пов’язаними з безпекою, або оцінювати результати сканування порівняно з результатами попереднього сканування, яке ви використовуєте як базове, як у наведених нижче прикладах.

Ви можете використовувати перше сканування, яке ви виконали на сайті, як базовий рівень. Під час першого сканування воно могло виявити велику кількість вразливостей, які ви згодом усунули. Порівняння поточних результатів сканування з результатами першого сканування допоможе вам визначити, наскільки ефективною була ваша робота з виправлення.

Ви можете використовувати сканування, яке виявило особливо низьку кількість вразливостей, як еталон доброго «здоров’я» безпеки.

Ви можете використовувати останнє сканування, що передує поточному, щоб перевірити, чи певний патч усунув уразливість у цьому скануванні.

Інформація про тенденції вказує на зміни, виявлені під час сканування, наприклад:

нові активи та послуги

активи або служби, які більше не працюють після останнього сканування

нові вразливості

Раніше виявлені вразливості не з’явилися під час останнього сканування

Інформація про тенденції корисна для вимірювання прогресу заходів з відновлення або спостереження за змінами навколишнього середовища з часом. Щоб тренд був точним і значущим, переконайтеся, що порівнювані сканування відбувалися за ідентичних умов:

той же сайт був просканований

використовувався той самий шаблон сканування

якщо базове сканування було виконано з обліковими даними, останнє сканування було виконано з тими самими обліковими даними.

Шаблон огляду керівника містить такі розділи:

Базове порівняння

Обкладинка

Резюме

Тенденції ризику

Вразливості з найвищим ризиком

Шаблон «Вразливості з найвищим ризиком» містить список 10 найпопулярніших уразливостей відповідно до рівня ризику. Цей шаблон корисний для визначення найбільших загроз безпеці як пріоритетних для виправлення.

Кожна вразливість перерахована з оцінками ризику та CVSS, а також посиланнями та посиланнями на важливі джерела інформації.

Шаблон звіту про вразливі місця з найвищим ризиком містить такі розділи:

Обкладинка

Деталі вразливості найвищого ризику

Зміст

Щойно виявлені активи

За допомогою цього шаблону ви можете переглядати активи, які були виявлені під час сканування протягом певного періоду часу. Це корисно для відстеження змін у вашому інвентарі активів. Окрім загальної інформації про кожен актив, у звіті наведено оцінки ризику та вказано, чи є в активах уразливості з пов’язаними експлойтами або наборами шкідливих програм.

3.2. Рекомендації щодо застосування методів та засобів управління вразливостями

Rapid7 — провідна компанія з кібербезпеки, яка надає широкий спектр рішень, які допомагають організаціям керувати вразливими місцями інформаційних систем. Ось деякі рекомендації від Rapid7 щодо керування вразливими місцями інформаційної системи:

Проводьте регулярне сканування вразливостей: використовуйте автоматизовані інструменти для сканування систем і виявлення вразливостей. Виконуйте регулярне сканування, щоб виявити нові вразливості та переконатися, що існуючі вразливості виправлено.

Пріоритезація вразливостей: визначте пріоритетність вразливостей на основі їх серйозності та потенційного впливу на ваші системи. Це допоможе вам спершу зосередитися на найбільш критичних уразливостях і відповідно розподілити ресурси.

Швидко виправляйте вразливості: як тільки вразливості виявлені, виправляйте їх якнайшвидше. Це допоможе зменшити ризик використання та звести до мінімуму вплив будь-яких успішних атак.

Запровадити жорсткі засоби контролю доступу: запровадити жорсткі засоби контролю доступу, щоб обмежити доступ неавторизованих користувачів до конфіденційної інформації та критичних систем. Це включає впровадження надійних паролів, двофакторну автентифікацію та обмеження доступу до конфіденційної інформації на основі принципу «необхідність знати».

Моніторинг систем на наявність підозрілої активності. Використовуйте інструменти моніторингу, щоб виявити будь-яку підозрілу активність у своїх системах, наприклад незвичайні спроби входу або незвичний мережевий трафік. Це може допомогти вам визначити потенційні атаки та швидко реагувати, щоб мінімізувати їхній вплив.

Проводьте регулярні тренінги з питань безпеки: розкажіть своїм співробітникам про важливість кібербезпеки та про те, як виявляти потенційні загрози та реагувати на них. Це допоможе знизити ризик людської помилки та покращити загальну гігієну кібербезпеки.

Створіть план реагування: розробіть план реагування, у якому описано, як ви будете реагувати на інцидент безпеки, включно з тим, як ви стримаєте інцидент, зменшите збитки та відновитеся після інциденту.

Впроваджуючи ці рекомендації, організації можуть краще керувати вразливими місцями своєї інформаційної системи та зменшити ризик успішних кібератак.

ВИСНОВКИ

В результаті виконання бакалаврської роботи, метою якої було дослідити методи та засоби управління вразливостями інформаційної системи організації, було отримано наступні результати:

Інформаційні системи організації потребують використання методів та засобів забезпечення кібербезпеки. Для цього розробляється стратегія кібербезпеки організації, важливою складовою управління вразливістю. В роботі визначено основні переваги управління вразливістю.

Поява нових вразливостей впливає на виконання бізнес-процесів організацій. Тому виникає необхідність створювати процес, який відповідає за виявлення, аналіз і звіт про недоліки безпеки та вразливості – сканування вразливостей. В результаті аналізу було визначено основні типи сканування та особливості їх застосування.

В роботі проведено аналіз бази даних CVE та її місце і важливість при управління вразливостями, а саме етапи життєвого циклу запису CVE.

На основі аналізу статистики вразливостей було встановлено кількість можливих вразливостей і потенційних наслідків для їх використання. Тому було визначено необхідність застосування програмних комплексів для застосування методів та засобів управління вразливостями в інформаційній системі організації.

Наступним кроком було визначено життєвий цикл управління вразливостями, як процесу проактивного виявлення, запобігання, пом’якшення та класифікації вразливостей в IT-системі на основі рівня загрози, якою вони володіють. В основі життєвого циклу було визначено п’ять етапів, які відіграють свою роль у виявленні, запобіганні, пом’якшенні та класифікації вразливостей.

На основі проведеного аналізу було обрано платформу Rapid 7, яка надає різномантні послуги, щодо забезпечення кібербезпеки інформаційної системи організації. Для управління вразливостями дана платформа пропонує InsightVM, виявляти та усувайте ризики, використовуючи повне сканування мережі

організації. Це дозволяє виявляти ризики для всіх кінцевих точок і інформаційної системи.

Результатом виконання бакалаврської роботи була розробка рекомендацій щодо роботи з консоллю безпеки InsightVM, для виконання різних завдань щодо виявлення вразливостей інформаційної системи організації. Це дозволить фахівцям з кібербезпеки краще розуміти основні дії для виявлення вразливостей в інформаційній системі організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. What Is Vulnerability Management? [Електронний ресурс] / Smriti Chand // Yourarticlelibrary – Режим доступу до ресурсу: https://heimdalsecurity.com/blog/vulnerability-management/ .
2. What Is Vulnerability Scanning: Definition, Types, Best Practices [Електронний ресурс] – Режим доступу до ресурсу: https://heimdalsecurity.com/blog/vulnerability-scanning/ .
3. Vulnerabilities in Corporate Information Systems [Електронний ресурс] / Positive Technologies – 2018. – Режим доступу до ресурсу: https://www.ptsecurity.com/ww-en/analytics/corporate-vulnerabilities-2018/.
4. Vulnerability Management Lifecycle: Step by Step Through the Process [Електронний ресурс] – Режим доступу до ресурсу: https://heimdalsecurity.com/blog/vulnerability-management-lifecycle/.
5. CVE [Електронний ресурс] – Режим доступу до ресурсу: https://www.cve.org/About/Process
6. NATIONAL VULNERABILITY DATABASE [Електронний ресурс] – Режим доступу до ресурсу: https://nvd.nist.gov/
7. Статистика виявлення вразливостей [Електронний ресурс] – Режим доступу до ресурсу: https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/.
8. VULNERABILITY STATISTICS REPORT [Електронний ресурс] / Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth, Ron Lieber // Edgescan - 2021. – Режим доступу до ресурсу: https://info.edgescan.com/hubfs/Edgescan2021StatsReport.pdf.
9. Rapid 7 InsightVM Guide [Електронний ресурс] Режим доступу до ресурсу: https://www.esecurityplanet.com/network-security/security-information-event-management-siem.html.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)