МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЗАХИСТОМ ІНФОРМАЦІЇ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “МЕТОДИКА УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ З ВИКОРИСТАННЯМ TENABLE SC”

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Максим ЗАЙЧЕНКО
(підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. УБД 41
Максим ЗАЙЧЕНКО
Ім’я, ПРІЗВИЩЕ

Керівник: Євгенія ІВАНЧЕНКО
Д.т.н., професор Ім’я, ПРІЗВИЩЕ

Рецензент: Юрій ПЕПА
К.т.н., доцент Ім’я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра Управління кібербезпекою та захистом інформації

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УКБЗІ
_____Світлана ЛЕГОМІНОВА
“_____”_____2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Зайченку Максиму Віталійовичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Методика управління вразливостями з використанням Tenable SC”,
керівник кваліфікаційної роботи ІВАНЧЕНКО Євгенія, д.т.н., професор,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “24“ лютого 2025 р. №56.

2. Строк подання кваліфікаційної роботи “12” травня 2025р.

3. Вихідні дані до кваліфікаційної роботи: *вразливість, управління вразливостями, методи та засоби управління вразливостями, застосування Tenable SC, нормативні документи, стандарти, міжнародні стандарти, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
   1. Проаналізувати основи та цикл процесу управління вразливостями.
   2. Дослідити технічні засоби спрямовані на процес управління вразливостями та їх роль у ньому.
   3. Визначити методику застосування Tenable SC у рамках управління вразливостями.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання “5“ березня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2025	
2.	Збір та аналіз літератури.	29.03.2025	
3.	Аналіз основ та циклу процесу управління вразливостями.	08.04.2025	
4.	Дослідження технічних засобів спрямованих на процес управління вразливостями та їх роль у ньому.	15.04.2025	
5.	Визначення методики застосування Tenable SC у рамках управління вразливостями.	22.04.2025	
6.	Формулювання висновків за результатами проведеного дослідження.	29.04.2025	
7.	Оформлення роботи.	06.05.2025	
8.	Оформлення презентації.	09.05.2025	
9.	Отримання рецензії на роботу.	12.06.2025	
10.	Захист в ДЕК.	__.06.2025	

Здобувач вищої освіти _____ Максим ЗАЙЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Зайченко М.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: “Методика управління вразливостями з використанням Tenable SC”

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ЗАЙЧЕНКО Максим у кваліфікаційній роботі проаналізував основ та цикл процесу управління вразливостями, дослідив технічні засоби спрямовані на процес управління вразливостями та їх роль у ньому, визначив методику застосування Tenable SC у рамках управління вразливостями.

ЗАЙЧЕНКО Максим показав розуміння проблеми дослідження та бачення основних теоретичних і практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на двох конференціях.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ЗАЙЧЕНКА Максима на оцінку “відмінно” та присвоїти їй кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Євгенія ІВАНЧЕНКО
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

“____“_____2025 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Зайченко М.В. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління кібербезпекою та
захистом інформації _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ЗАЙЧЕНКА Максима
на тему “Методика управління вразливостями з використанням Tenable SC”

Актуальність. У сучасних умовах стрімкого зростання кількості кіберзагроз і вразливостей управління вразливостями є одним із ключових напрямів забезпечення кібербезпеки. Вчасне виявлення, аналіз і усунення вразливостей дозволяють знижувати ризики компрометації інформаційних систем. Професійні платформи, зокрема Tenable Security Center (Tenable SC), забезпечують автоматизацію та систематизацію цих процесів, що дозволяє організаціям будувати повноцінний цикл управління вразливостями.

З огляду на зазначене, дослідження методики управління вразливостями з використанням Tenable SC є актуальним та практично значущим завданням у сфері кібербезпеки.

Позитивні сторони.

1. У роботі розглянуто теоретичні основи та міжнародні підходи до управління вразливостями, що забезпечує комплексність дослідження.
2. Викладено порівняльний аналіз провідних платформ управління вразливостями та обґрунтовано вибір Tenable SC для реалізації методики.
3. Розроблено практичну методику впровадження процесу управління вразливостями за моделлю SANS VMMM із використанням можливостей Tenable SC, що підвищує прикладне значення роботи.
4. Кваліфікаційна робота оформлена відповідно до встановлених вимог, логічно структурована, містить ілюстративний матеріал і ґрунтується на широкій джерельній базі, що включає 60 сучасних джерел, зокрема англомовних.

Недоліки.

Доцільно було б доповнити роботу оцінкою економічної доцільності впровадження обраної платформи в організаціях різного масштабу, що могло б розширити прикладну цінність дослідження.

Однак вказане зауваження не знижує загальної позитивної оцінки кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач ЗАЙЧЕНКО Максим заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент: _____ Юрій ПЕПА
к.т.н., доцент *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню методиці управління вразливостями з використанням Tenable SC. Робота складається зі вступу, трьох розділів, що містять 12 рисунків, висновків та списку використаних джерел, що містить 60 найменувань. Загальний обсяг роботи становить 86 аркушів, з яких 9 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є визначення методики управління вразливостями з використанням Tenable SC.

Об'єктом дослідження є процес управління вразливостями.

Предмет дослідження – методика управління вразливостями з використанням Tenable SC.

Методи дослідження. Методи дослідження. Для досягнення мети в роботі застосовано методи аналізу і синтезу, порівняльного аналізу, класифікації, експертної оцінки та системного підходу.

Методи аналізу і синтезу використано для обґрунтування теоретичних засад і вимог до технічних рішень. Порівняльний аналіз і систематизація використані для дослідження можливостей провідних платформ управління вразливостями та визначення їх переваг і недоліків. Метод класифікації застосовано для структурування етапів процесу управління вразливостями відповідно до моделі SANS VMMM. Метод експертної оцінки – для аналізу функціоналу Tenable SC. Системний підхід забезпечив узгодження методичних і технічних рішень у межах повного циклу управління вразливостями.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні, реалізації та для покращення процесу управління вразливостями у контексті зміцнення загального стану інформаційної безпеки.

Ключові слова: ВРАЗЛИВІСТЬ, УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ, МЕТОДИКА УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ, TENABLE SC, TENABLE SECURITY CENTER.

ABSTRUCT

The qualification work is devoted to the study of the vulnerability management methodology using Tenable SC. The work consists of an introduction, three chapters containing 12 figures, conclusions, and the list of references containing 60 items. The total volume of the work is 86 pages, of which 9 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to define the methodology for vulnerability management using Tenable SC.

The object of the study is the process of vulnerability management.

The subject of the study is the methodology for vulnerability management using Tenable SC.

Research methods. In order to achieve the set goal, the methods of analysis and synthesis, comparative analysis, classification, expert assessment, and a systematic approach were applied.

The methods of analysis and synthesis were used to justify the theoretical foundations and requirements for technical solutions. Comparative analysis and systematization were applied to study the capabilities of leading vulnerability management platforms and to determine their advantages and disadvantages. The classification method was used to structure the stages of the vulnerability management process according to the SANS VMMM model. The expert assessment method was used to analyze the functionality of Tenable SC. The systematic approach ensured the alignment of methodological and technical aspects of implementing the complete vulnerability management cycle in practice.

Field of application. The developed approaches can be used for planning, implementing, and improving the vulnerability management process in the context of strengthening the overall state of information security.

Keywords: VULNERABILITY, VULNERABILITY MANAGEMENT, VULNERABILITY MANAGEMENT METHODOLOGY, TENABLE SC, TENABLE SECURITY CENTER.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ 10
ВСТУП 11
РОЗДІЛ 1 УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ЯК ВАЖЛИВИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ 13
1.1 Загальна характеристика поняття «вразливість» 13
1.1.1 Поняття та небезпеки вразливостей 13
1.1.2 Методика оцінки вразливостей CVSS 14
1.1.3 Поняття CVE: мета, джерела формування, користь 16
1.2 Дослідження процесу управління вразливостями 18
1.2.1 Історія, причини та актуальність процесу управління вразливостями 18
1.2.2 Управління вразливостями в міжнародних стандартах 20
1.2.3 Основні принципи управління вразливостями 23
1.3 Огляд моделей управління вразливостями 27
1.3.1 Модель NIST (Vulnerability Management Lifecycle) 27
1.3.2 Модель SANS (PIACT) 28
1.3.3 Модель Tenable (Cyber Exposure Lifecycle) 29
1.3.4 Переваги та недоліки моделей управління вразливостями 31
Висновки до розділу 1 33
РОЗДІЛ 2 ТЕХНІЧНІ ЗАСОБИ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ: РОЛЬ, ВАЖЛИВІСТЬ, АНАЛІЗ РІШЕНЬ 35
2.1 Роль та призначення технічних засобів управління вразливостями 35
2.2 Порівняльний аналіз провідних платформ управління вразливостями 38
2.2.1 Огляд провідних рішень 40
2.2.2 Аналіз переваг і недоліків платформ 43
2.2.3 Обґрунтування вибору платформи Tenable SC для дослідження 47
2.3 Важливість методики управління вразливостями 48
Висновки до розділу 2 52

РОЗДІЛ 3 МЕТОДИКА УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ З ВИКОРИСТАННЯМ TENABLE SC 54
3.1 Prepare (Підготовка) 54
3.1.1 Створення та налаштування політики сканування 54
3.1.2 Створення та налаштування сканування 55
3.1.3 Створення та налаштування груп активів 58
3.2 Identify (Виявлення) 60
3.3 Analyze (Аналіз) 61
3.3.1 Перегляд результатів сканування 61
3.3.2 Аналіз вразливостей за VPR, критичністю та експлуатованістю 63
3.4 Communicate (Комунікація) 66
3.4.1 Створення звітності 66
3.4.2 Створення дашбордів 69
3.4.3 Створення завдань та сповіщень 71
3.5 Treat (Усунення) 74
Висновки до розділу 3 76
ВИСНОВКИ 78
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 80

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ОС	Операційна система
ПЗ	Програмне забезпечення
CISO	Chief Information Security Officer
CVSS	Common Vulnerability Scoring System
CVE	Common Vulnerabilities and Exposures
EPSS	Exploit Prediction Scoring System
IP	Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator
Qualys VMDR	Qualys Vulnerability Management, Detection and Response
SANS VMMM	SANS Vulnerability Management Maturity Model
SLA	Service Level Agreement
SIEM	Security Information and Event Management
Tenable SC	Tenable Security Center
VM	Vulnerability Management
VPR	Vulnerability Priority Rating

ВСТУП

Актуальність теми. В умовах стрімкого зростання кількості кіберзагроз та збільшення площини атаки сучасних організацій управління вразливостями набуває критичного значення для забезпечення належного рівня кіберстійкості. Статистика свідчить, що понад 90 % успішних атак здійснюються через вже відомі, але не усунуті вразливості. Водночас кількість зареєстрованих уразливостей щороку перевищує десятки тисяч записів у базі CVE, що створює значні виклики щодо їхньої ефективної обробки та пріоритизації.

Однією з провідних платформ для централізованого управління вразливостями є Tenable Security Center (SC), яка надає розширені можливості для повного циклу робіт — від виявлення до усунення. Проте для досягнення високої ефективності важливо мати чітку методику застосування цієї платформи з урахуванням кращих міжнародних практик.

Таким чином, розроблення прикладної методики управління вразливостями з використанням Tenable SC є актуальним науковим завданням для підвищення кіберзахисту організацій, оптимізації процесів реагування та забезпечення відповідності сучасним вимогам безпеки.

Мета роботи полягає у визначенні методики управління вразливостями з використанням Tenable SC.

Об’єкт дослідження – процес управління вразливостями.

Предмет дослідження – методика управління вразливостями з використанням Tenable SC.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Проаналізувати основи та цикл процесу управління вразливостями.
2. Дослідити технічні засоби спрямовані на процес управління вразливостями та їх роль у ньому.
3. Визначити методику застосування Tenable SC у рамках управління вразливостями.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використано комплекс наукових методів, зокрема методи аналізу та синтезу, порівняльного аналізу, систематизації та класифікації, моделювання, експертної оцінки та системного підходу до управління інформаційною безпекою.

Практичне значення одержаних результатів. Застосування напрацювань дасть змогу здійснити обґрунтований вибір методів і інструментів формування обізнаності й навчання персоналу як важливого елемента управління інформаційною безпекою відповідно до цілей бізнесу, можливостей та ресурсів підприємства.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції “Стратегії кіберстійкості: управління ризиками та безперервність бізнесу” 27 лютого 2025 року.

Розділ 1 УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ ЯК ВАЖЛИВИЙ ЕЛЕМЕНТ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

1.1 Загальна характеристика поняття «вразливість»

1.1.1 Поняття та небезпеки вразливостей.

Вразливістю називають слабке місце в апаратному чи програмному забезпеченні, яке може бути використане зловмисником для порушення конфіденційності, цілісності або доступності системи [1]. Інакше кажучи, це дефект або хиба безпеки, експлуатація якої призводить до негативних наслідків для інформаційних ресурсів.

Небезпека вразливостей полягає в тому, що через них зловмисники можуть отримати несанкціонований доступ до даних, виконати шкідливий код чи вивести системи з ладу. Зафіксовано численні інциденти, коли використання відомих вразливостей спричиняло масштабні кібератаки. Наприклад, уразливість Log4Shell (CVE-2021-44228) у популярній Java-бібліотеці Log4j дала змогу виконувати довільний код на мільйонах систем по всьому світу, що вимагало екстрених заходів з оновлення ПЗ [2].

Загалом щороку виявляються десятки тисяч нових уразливостей: так, у 2022 році було зареєстровано понад 25 тис. уразливостей CVE, а станом на серпень 2024 року кількість нових CVE сягнула ~52 тис. [3].

Якщо вразливості вчасно не усунути, вони залишають «лазівки» для нападників. Дослідження показують, що близько 60% витоків даних безпосередньо спричинені невстановленими патчами для відомих вразливостей [4]. Таким чином, вразливості є одним з ключових факторів ризику кіберінцидентів, і їх своєчасна ідентифікація та усунення має критичне значення для забезпечення кібербезпеки.

1.1.2 Методика оцінки вразливостей CVSS.

Кожну вразливість можна охарактеризувати низкою параметрів, що визначають її небезпечність та пріоритет усунення. Для забезпечення стандартизації методу оцінювання було створено CVSS (Common Vulnerability Scoring System) – загальноприйняту методику якісної оцінки небезпеки вразливостей за шкалою 0–10.

Версія 3.1 CVSS (оприлюднена у 2019 р.) наразі широко використовується у спільноті кібербезпеки для визначення рейтингу вразливостей.

CVSS v3.1 складається з трьох груп метрик: Base, Temporal та Environmental, кожна з яких складається з набору метрик (рис. 1.1).

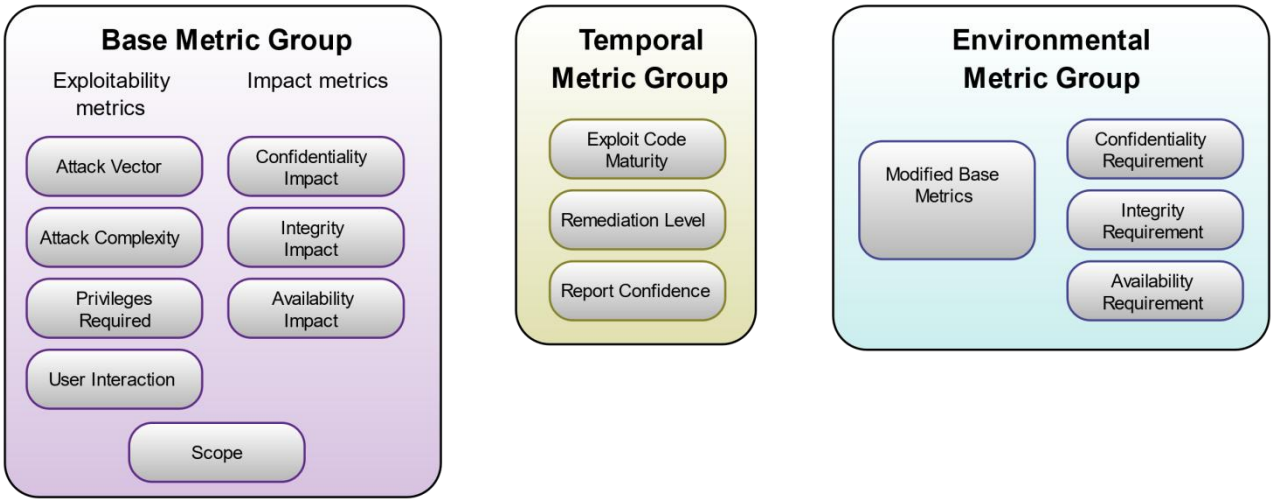


Рис. 1.1. Групи метрик CVSSv3.1 [5]

Оскільки наразі найбільш широко використовуються показники базової (Base) оцінки CVSS v3.1, ми розглянемо саме її метрики детальніше.

До основних підгруп параметрів CVSS належать метрики оцінки експлуатації (Exploitability), охоплення (Scope) та впливу (Impact).

1) *Метрики експлуатації* відображають характеристики вразливого компонента. Таким чином, кожна з перелічених нижче метрик експлуатації повинна бути оцінена відносно вразливого компонента і відображати властивості вразливості, які призводять до успішної атаки.

1.1) Вектор атаки (Attack Vector, AV) – визначає, з якої дистанції або способу може здійснюватися експлуатація вразливості. Чим більш віддалений (наприклад, через мережу Інтернет) доступ потрібен для атаки,

тим небезпечнішою є уразливість (AV:N – мережевий вектор має найвищий ризик). Локальні вразливості (AV:L) вимагають попереднього доступу до системи й оцінюються нижче.

1.2) Складність атаки (Attack Complexity, AC) – описує умови, які повинен подолати атакувальник для успішної експлуатації. Якщо додаткових складних умов не потрібно (AC:L – низька складність), вразливість отримує вищий бал небезпечності. Висока складність (AC:H) знижує рейтинг, оскільки потребує рідкісних умов або спеціальних знань для атаки.

1.3) Необхідні привілеї (Privileges Required, PR) – мінімальний рівень прав у системі, який мусить мати атакувальник до експлуатації уразливості. Вразливості, що не потребують автентифікації (PR:N), є більш критичними, ніж ті, для яких потрібен, скажімо, обліковий запис користувача (PR:L) чи адміністратора (PR:H).

1.4) Взаємодія з користувачем (User Interaction, UI) – вказує, чи потрібні дії легітимного користувача для успішної атаки. Якщо жодної взаємодії не потрібно (UI:N), ризик більший. У випадку, коли потрібна участь користувача (UI:R), наприклад відкриття файлу чи запуск макросу, вразливість оцінюється як менш небезпечна.

2) *Метрика охоплення* (Scope, S) – показує, чи виходить вплив експлуатації за межі враженого компонента. Якщо компрометація однієї системи дає змогу атакувати інші системи чи ресурси за її межами (S:Changed), це збільшує критичність. Якщо вплив обмежується тільки межами початкової системи (S:Unchanged), ризик нижчий.

3) *Метрики впливу* фіксують вплив успішно використаної вразливості на компонент, який зазнає найгіршого результату, що найбільш безпосередньо і передбачувано пов'язаний з атакою. Аналітики повинні обмежити вплив до розумного кінцевого результату, якого, на їхню думку, може досягти зловмисник.

3.1) Вплив на конфіденційність (Confidentiality, C) – ступінь, до якого порушується конфіденційність даних у разі успішної атаки. Повний витік або доступ до всіх даних (C:High) означає максимальний негативний вплив, частковий – середній (C:Low), відсутність впливу – (C:None).

3.2) Вплив на цілісність (Integrity, I) – характеризує наслідки для цілісності інформації або систем. Повне порушення цілісності (наприклад, можливість змінити всі дані) оцінюється як високий вплив (I:High), часткове – як середній (I:Low), відсутність впливу – (I:None).

3.3) Вплив на доступність (Availability, A) – визначає, наскільки експлуатація вразливості порушує доступність сервісів чи ресурсів. Повна відмова в обслуговуванні (A:High) є найгіршим випадком, часткова деградація продуктивності – середнім (A:Low), а відсутність впливу – (A:None).

Кожна з цих характеристик впливає на підсумковий бал CVSS: чим легше експлуатувати уразливість (наприклад, AV: мережевий, AC: низька, PR: не потрібні, UI: не потрібна) та чим сильніше вона впливає на конфіденційність, цілісність або доступність (C/I/A: високий), тим вищим буде її рівень небезпеки. На основі комбінації значень метрик обчислюється базова оцінка CVSS (0–10), що класифікує вразливість як низьку, середню, високу чи критичну за ступенем ризику [6].

Таким чином, наведені характеристики дозволяють стандартизовано описати потенціал експлуатації і наслідки кожної уразливості, що є основою для її пріоритизації в процесі управління вразливостями.

1.1.3 Поняття CVE: мета, джерела формування, користь.

Ефективне управління вразливостями потребує уніфікованої системи ідентифікації, щоби різні сторони могли однозначно посилатися на одну й ту саму вразливість. Саме таку роль виконує система CVE (Common Vulnerabilities and Exposures) – «Загальний перелік уразливостей та експозицій». Програма CVE була започаткована у 1999 році корпорацією MITRE з метою створити

спільну мову для опису вразливостей [7]. До впровадження CVE різні виробники та дослідники могли використовувати власні назви для одних і тих самих проблем безпеки, що спричиняло плутанину. Натомість CVE призначає кожній вразливості унікальний ідентифікатор у форматі CVE-PPPP-XXXX, завдяки чому дві чи більше сторін можуть впевнено говорити про ту саму уразливість, використовуючи спільний CVE-ID.

Мета CVE – ідентифікувати, каталогізувати та публічно описати всі відомі уразливості, щоб полегшити обмін інформацією про них у спільноті. Як зазначено в місії програми CVE, завдання – «ідентифікувати, визначити та каталогізувати публічно відомі вразливості». CVE не містить детальної технічної інформації чи способів експлуатації – вона радше служить індексом або довідником, що перелічує уразливості. Деталі про конкретну вразливість (опис, оцінки CVSS, рішення тощо) зазвичай публікуються в інших базах (NVD, SecurityFocus, тощо) з посиланням на CVE-ID.

Наповнення списку CVE здійснюється через мережу партнерів – CVE-нумеруючих органів (CNA). CNAs включають виробників програмного та апаратного забезпечення, дослідницькі групи та інші організації, що виявляють або отримують інформацію про нові уразливості. Кожна така організація може зарезервувати CVE-ідентифікатор для нової уразливості і після публічного розголошення опису внести запис до каталогу CVE. Усі записи перевіряються та ведуться MITRE (у співпраці з організацією FIRST) на офіційному сайті cve.org. На початок 2025 року в списку CVE зареєстровано понад 277 тисяч записів [8], причому щорічно додаються десятки тисяч нових (як згадувалось, понад 50 тис. за 2024 рік). Таким чином, CVE охоплює надзвичайно широкий спектр вразливостей у продуктах різних виробників за останні десятиліття.

Не можна не зазначити, що стандарт CVE став фундаментом для більшості засобів та процесів керування вразливостями.

По-перше, наявність CVE-ID дозволяє легко об’єднувати дані з різних джерел: консультативні бюлетені від виробників, бази експлойтів, сканери вразливостей – всі оперують єдиними CVE-кодами. Це усуває двозначність: як

зазначено вище, CVE забезпечує, що різні сторони мають на увазі ту саму уразливість.

По-друге, CVE полегшує обмін інформацією про уразливості між фахівцями та організаціями. Наприклад, національна база даних NVD (National Vulnerability Database, США) імпортує всі CVE-записи та доповнює їх аналізом – без CVE таке агрегування було б неможливим.

По-третє, CVE стимулювала розвиток інструментів автоматизації: завдяки CVE з’явилися стандартизовані формати обміну (OVAL, SCAP), що дозволяють системам управління вразливостями автоматично отримувати дані про нові загрози.

Таким чином, CVE стала «кореневим довідником» у галузі кібербезпеки. Сьогодні важко уявити бюлетень безпеки чи звіт сканування, в яких не використовуються CVE-ідентифікатори. Спільнота отримала завдяки CVE єдиний базис для координації зусиль у боротьбі з уразливостями, і ця система довела свою ефективність за більш ніж 20 років існування.

1.2 Дослідження процесу управління вразливостями

1.2.1 Історія, причини та актуальність процесу управління вразливостями.

Практика систематичного управління вразливостями сформувалася поступово на початку 2000-х років, хоча окремі її елементи з’явилися ще раніше. У 90-х роках адміністрування вразливостей зводилось переважно до ручного встановлення патчів постачальників, часто – після появи перших експлойтів чи інцидентів. Зі зростанням кількості вразливостей (у 1990-х їх публікувалось лише декілька сотень на рік, проти десятків тисяч сьогодні) та поширенням мережевих черв’яків і атак, виникла потреба в більш проактивному підході. На рубежі 2000-х з’являються автоматизовані сканери вразливостей (наприклад, Nessus, SATAN), що дозволили виявляти вразливі системи в мережах. Це ознаменувало перехід від одиничного «латання дір» до

процесу постійної оцінки безпеки систем. У наступні роки концепція розвивалась: у 2010-х набувають популярності моделі безперервного моніторингу і проактивного пошуку вразливостей. Сьогодні управління вразливостями – це безперервний процес у циклі кібербезпеки організації, що все більше опирається на автоматизацію, машинне навчання та інтеграцію в процеси розробки (DevSecOps).

Головною рушійною силою розвитку управління вразливостями стали реальні кіберзагрози. Напади типу worms/черв'яків (наприклад, Code Red у 2001 р., що використовував уразливість у IIS-сервері) показали, що експлуатація вразливостей може відбуватися масово та швидко після їх оприлюднення. Відомий інцидент – атака WannaCry (2017), коли шифрувальне ПЗ використало уразливість Windows (протокол SMB, CVE-2017-0144) для зараження десятків тисяч комп'ютерів по всьому світу; при цьому виправлення для цієї уразливості було випущене Microsoft за кілька місяців до атаки. Цей випадок засвідчив критичну необхідність вчасно встановлювати патчів. Таким чином, збільшення частоти та масштабів кібератак через відомі уразливості стало однією з причин виокремлення управління вразливостями в самостійний процес.

Іншою причиною є зростання кількості самих уразливостей – жодна велика організація не в змозі реагувати хаотично на кожне нове повідомлення; потрібні наперед сплановані процедури моніторингу, аналізу та усунення вразливостей. До того ж, час між публікацією інформації про вразливість та появою перших експлойтів стрімко скоротився: за статистикою, близько 80% експлойтів стають доступними ще до офіційного випуску CVE-запису, у середньому з випередженням у 23 дні. Отже, без проактивного виявлення вразливостей захисники часто відстають від зловмисників.

Важливим фактором актуальності є також регуляторні вимоги та стандарти. Яскравий приклад – стандарт PCI DSS для компаній, що обробляють платіжні картки: він вимагає проводити регулярне сканування на вразливості та оперативно застосовувати патчі, під загрозою штрафів за невідповідність.

Аналогічно, нормативні акти у сферах охорони здоров'я (HIPAA), захисту персональних даних (GDPR) тощо прямо або опосередковано спонукають організації мати процедури управління технічними вразливостями.

Отже, історично управління вразливостями пройшло шлях від епізодичного встановлення патчів до стратегічно спланованого циклічного процесу, підкріпленого автоматизованими сканерами і регламентованого внутрішніми політиками та міжнародними стандартами. На його актуальність вказують як невпинно високий рівень загрози, так і вимоги регуляторів та бізнесу забезпечити належний захист інформаційних систем. За даними Verizon, частка інцидентів, де початковим вектором було експлуатацію вразливостей, зростає: у 2022–2023 рр. їх кількість як причини витоків даних збільшилась на 180% [9-11]. У цих умовах зрілі процеси vulnerability management є необхідним елементом кіберстійкості сучасної організації.

1.2.2 Управління вразливостями в міжнародних стандартах.

Ефективне управління вразливостями закріплено в низці міжнародних стандартів та рекомендацій з кібербезпеки. Розглянемо найважливіші з них.

ISO/IEC 27002:2022 – містить керівництво з реалізації заходів безпеки в системах менеджменту інформаційної безпеки (доповнення до стандарту ISO 27001). У новій редакції 2022 року в розділі 8 «Технологічні контролі» виділено контроль 8.8 «Management of technical vulnerabilities» (Управління технічними вразливостями). Вимога цього контролю формулюється так: «Необхідно отримувати інформацію про технічні вразливості інформаційних систем, оцінювати експозицію організації до цих вразливостей і вживати відповідних заходів». Тобто ISO 27002 визначає загальну потребу мати процес відстеження і реагування на уразливості. У роз'ясненні до контролю 8.8 наводяться основні етапи такого процесу: сканування на наявність відомих уразливостей у системах та мережах; оцінка вразливостей – аналіз потенційного впливу знайдених вразливостей і пріоритизація їх за рівнем небезпеки; усунення вразливостей – розробка і реалізація плану щодо їх виправлення (встановлення

патчів, оновлень, зміна конфігурації або впровадження додаткових засобів захисту). Також наголошується на важливості мати формалізований план управління вразливостями та регулярно його переглядати, включно з проведенням повторних сканувань і оцінок [12].

Фактично, ISO 27002:2022 встановлює високорівневий вимір: організація повинна мати безперервний процес відстеження технічних уразливостей і оперативно реагувати на них, виходячи з оцінки ризиків. Стандарт не диктує конкретних інструментів чи строків, але задає принципи проактивності, своєчасності та пріоритезації, що мають бути відображені у внутрішніх процедурах.

NIST Special Publication 800-40 Rev.4 (2022) – це спеціальне видання Національного інституту стандартів і технологій (NIST, США) під назвою “Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology”. NIST SP 800-40 визначає рамки організаційної програми управління виправленнями: це процес виявлення, пріоритизації, отримання, встановлення і перевірки встановлення патчів у масштабах підприємства. На практиці дана модель включає: ведення актуального переліку активів і програмного забезпечення; моніторинг інформації про нові уразливості та доступні виправлення (з бюлетенів постачальників, баз даних тощо); оцінку критичності вразливостей і вирішення, які патчі слід встановити першочергово (з урахуванням оцінки CVSS, наявності експлойтів, важливості системи); планування та розгортання патчів – організація тестування оновлень, їх поетапне розгортання на середовища (спочатку тестові, потім продуктивні системи), мінімізація простоїв; та аудит/верифікація – перевірка, що патчі успішно застосовані на всіх потрібних вузлах (наприклад, повторне сканування). NIST акцентує, що patch management має розглядатись як «вартість ведення бізнесу» та невід’ємна частина забезпечення місії організації. Документ обговорює типові проблеми (розбіжність пріоритетів між IT-підрозділом та бізнесом, вікна простою для оновлень тощо) і рекомендує

виробити стратегію на рівні підприємства задля спрощення та систематизації процесу патчінгу [13].

Таким чином, NIST SP 800-40 доповнює високорівневі вимоги ISO конкретнішим керівництвом щодо організації циклу оновлень безпеки. Цей стандарт орієнтовано переважно на державні установи США, але його положення (наприклад, щодо пріоритетного встановлення патчів на критичні вразливості протягом визначеного часу) стали де-факто найкращою практикою і в комерційному секторі по всьому світу.

CIS Critical Security Controls – відомий набір з 18 базових контролів кібербезпеки, розроблений Center for Internet Security (CIS, раніше – SANS Institute). В актуальній версії CIS Controls v8 один з ключових контролів (номер 7) називається “Continuous Vulnerability Management” – безперервне управління вразливостями. Він вимагає від організацій “розробити план для постійної оцінки та відстеження вразливостей на всіх активах підприємства з метою своєчасного усунення та мінімізації вікна можливостей для атакуючих”. Зокрема, рекомендується моніторити зовнішні джерела інформації (публічні й галузеві) щодо нових загроз і вразливостей, щоб швидко дізнаватись про релевантні уразливості.

CIS Control 7 конкретизується через низку підконтролів, наприклад: 7.1 – “Впровадити процес управління вразливостями та підтримувати його”; 7.2 – “Проводити регулярне сканування вразливостей на всіх пристроях і системах”; 7.3 – “Визначати пріоритети виправлення вразливостей на основі оцінки ризиків (враховуючи оцінки CVSS, наявність експлойтів, критичність активів)”; 7.5 – “Виконувати виправлення або інші заходи пом’якшення вразливостей у встановлені строки (наприклад, протягом 14 днів для критичних)” тощо [14].

CIS Controls є стислим практичним керівництвом, тому не дають детальних процедур, але чітко фокусуються на проактивності та безперервності: сканування повинно виконуватися регулярно (постійно), дані про вразливості мають централізовано збиратися і аналізуватися, а закриття вразливостей – здійснюватися в якнайстисліші терміни. Даний контроль

узгоджується з вимогами ISO/NIST, але формулює їх у більш прикладному ракурсі. У багатьох компаніях саме впровадження CIS Control 7 стає початковою точкою побудови процесу vulnerability management.

З характеристики вищерозглянутих стандартів можна зробити висновок, що вони доповнюють один одного: ISO 27002 задає що потрібно робити (отримувати інформацію, оцінювати, усувати), NIST SP 800-40 заглиблюється як планувати та реалізувати процес (з акцентом на патчі як превентивну міру), а CIS Controls визначає пріоритетність і частоту дій (безперервність сканувань, оперативність виправлень).

1.2.3 Основні принципи управління вразливостями.

Аналіз стандартів і найкращих практик дозволяє виділити кілька базових принципів, на яких ґрунтується ефективне управління вразливостями, а саме:

- проактивність;
- пріоритизація на основі ризику;
- безперервність процесу;
- комплексність та всеохопність;
- документованість і відслідковуваність.

Проактивність. Організація повинна наполегливо випереджати зловмисників, виявляючи та усуваючи вразливості до того, як ними скористаються. Це означає, що управління вразливостями має носити превентивний характер, а не реактивний. Замість чекати інциденту або повідомлення від третіх осіб, слід самостійно шукати слабкі місця. Проактивність досягається за рахунок регулярного сканування систем на наявність відомих уразливостей, аналізу вихідного коду на вразливості ще на етапі розробки тощо. Проактивний підхід зменшує «вікно ризику» – час, протягом якого організація залишається вразливою. Згідно з визначенням, управління вразливостями – це саме безперервний проактивний процес ідентифікації та усунення вразливостей.

Пріоритизація на основі ризику. Оскільки ресурси завжди обмежені, а кількість вразливостей може бути дуже великою, критично важливо правильно визначати, на чому зосередити зусилля першочергово. Принцип пріоритизації означає оцінку кожної вразливості з точки зору ризику, який вона становить для організації, і впорядкування черги виправлень за цією оцінкою. Поширеною практикою є категоризація вразливостей за критичністю (оцінка CVSS та відповідний рівень загрози – Critical/High/Medium/Low). Проте сучасний підхід виходить за рамки суто CVSS: враховується контекст активу (його роль, цінність даних), поточна обстановка вразливості (чи є в наявності експлойт, чи використовують дану уразливість реальні зловмисники), доступність засобів пом’якшення тощо.

У 2021 р. Агентство з кібербезпеки і інфраструктур США (CISA) започаткувало каталог Known Exploited Vulnerabilities (KEV) – список уразливостей, щодо яких достеменно відомо про активну експлуатацію у реальних атаках [15]. Рекомендовано використовувати такі дані при ранжуванні робіт з виправлення: вразливості з каталогу KEV мають виправлятись у першочерговому порядку. Ще один інструмент – метрика EPSS (Exploit Prediction Scoring System), яка оцінює ймовірність експлуатації конкретної уразливості в найближчі 30 днів на основі статистичних моделей [16]. Поєднання CVSS (технічна важливість) з EPSS (ймовірність атаки) та даними про наявність експлойтів дозволяє реалізувати принцип Risk-Based Vulnerability Management, тобто управління вразливостями, орієнтоване на ризик. У підсумку, організація повинна проактивно усувати ті уразливості, які становлять найбільший сумарний ризик – навіть якщо їх формальна критичність може бути не найвищою. Пріоритизація також стосується черговості охоплення систем: спочатку захищаються найкритичніші сервіси (наприклад, інтернет-портали, бази даних з конфіденційною інформацією), а вже потім другорядні вузли.

Безперервність процесу. Управління вразливостями має бути постійним циклом, інтегрованим у повсякденну діяльність підрозділів IT та інформаційної

безпеки. Це не одноразовий проект (скажімо, сканування раз на рік для аудиту), а безупинна послідовність етапів: сканування – аналіз – виправлення – моніторинг – знову сканування і далі по колу. Нові вразливості з'являються щодня, змінюється середовище (розгортання нових систем, зміни конфігурацій), тому тільки постійний моніторинг може забезпечити актуальність картини. Принцип безперервності закріплений у самих формулюваннях стандартів: «безперервне управління вразливостями» (CIS Control 7), «постійне превентивне обслуговування» (NIST 800-40). Практично це означає, що сканування вразливостей слід виконувати на регулярній основі (щонайменше щомісяця, а за можливості – постійно за розкладом або агентами в реальному часі).

Також безперервність передбачає своєчасність застосування виправлень: організація встановлює внутрішні SLA – наприклад, виправити критичні уразливості протягом 1–2 тижнів з моменту виявлення. Після завершення чергового раунду патчів потрібно знову сканувати системи, щоб впевнитись, що нові вразливості не виникли або не були пропущені.

Комплексність та всеохопність. Цей принцип означає, що програма управління вразливостями повинна охоплювати всі рівні і всі активи організації. Не можна обмежуватися лише серверами чи лише мережевим обладнанням – вразливими можуть бути й користувацькі пристрої, мобільні додатки, хмарні сервіси, IoT-тощо. Тому необхідно мати повний реєстр IT-активів і відповідні інструменти для їх сканування. Стандарти (як-от CIS Control 7.1) рекомендують створити процес виявлення нових активів та додавання їх до зони дії управління вразливостями. Наприклад, при підключенні нового сервера він автоматично має ставати на облік та скануватися. Також комплексність стосується видів уразливостей – процес має враховувати як технологічні вразливості (помилки програмного коду, некоректні налаштування), так і процедурні (наприклад, відсутність сегментації мережі, слабкі паролі). Крім того, слід координувати цей процес з суміжними: управління конфігураціями (Configuration Management) та управління змінами

(Change Management), аби виправлення вразливостей не порушували роботу систем і відповідали політикам конфігурації.

Документованість і відслідковуваність. Хоча цей аспект часто недооцінюють, він важливий для масштабного впровадження. Потрібно мати чітко визначені ролі й відповідальність за кожен етап (сканування виконує, наприклад, відділ безпеки; аналіз результатів – спільно з IT-адміністраторами; затвердження черги виправлень – комітет з ризиків тощо).

Усі дії та рішення мають протоколюватися: які вразливості виявлено, який ризик присвоєно, коли і яким способом усунуто. Це дозволяє контролювати прогрес (метрики на кшталт % закритих вразливостей) і проводити ретроспективний аналіз інцидентів (чи була дана уразливість відома до атаки, чому не усунута). Більш зрілі підходи включають звітність для керівництва – наприклад, періодичні звіти про стан вразливостей у підрозділах, що мотивує відповідальних осіб приділяти увагу цьому питанню. SANS-методологія PIACT містить окремий етап Communicate, підкреслюючи необхідність доводити інформацію про ризики від уразливостей до керівництва і власників бізнес-активів [17]. Без належної комунікації навіть технічно ефективний процес може натрапити на перепони (наприклад, відмова підрозділів відключати системи для встановлення патчів). Тому принцип полягає в тому, щоб зробити управління вразливостями прозорим процесом, зрозумілим на всіх рівнях, з відповідним документуванням і звітуванням.

Підсумовуючи, ефективна система управління вразливостями будується на проактивному, безперервному виявленні слабких місць, їх оцінці за ризиком та пріоритетному усуненні, охоплює всю IT-інфраструктуру і підкріплена внутрішньою політикою та процесами контролю. Дотримання цих принципів дозволяє організації значно знизити спектр можливих дій для зловмисника і своєчасно протидіяти новим загрозам.

1.3 Огляд моделей управління вразливостями

Хоча основні етапи управління вразливостями загалом зрозумілі, різні організації та експерти описують життєвий цикл цього процесу через власні моделі. Розглянемо кілька відомих моделей циклу управління вразливостями:

- NIST (Vulnerability Management Lifecycle);
- SANS (PIACT);
- Tenable (Cyber Exposure Lifecycle);

1.3.1 Модель NIST (Vulnerability Management Lifecycle).

NIST не виділяє окремого офіційного циклу під такою назвою, проте в своїх публікаціях (зокрема SP 800-40, SP 800-137) описує процес у вигляді логічної послідовності дій.

1) Підготовка та пріоритизація – створення інвентаря активів, визначення відповідальних, налаштування засобів сканування, оцінка критичності різних систем.

2) Виявлення вразливостей – регулярне сканування і збір інформації про нові вразливості (наприклад, моніторинг повідомлень від постачальників, розсилок CERT тощо).

3) Аналіз та оцінка ризику – присвоєння знайденим вразливостям рейтингу ризику (CVSS, контекст активу, наявність експлойтів).

4) Розробка плану реагування – визначення, які вразливості коли і як будуть усунені (встановлення патчів, чи застосування обхідних рішень, чи прийняття ризику).

5) Усунення вразливостей – реалізація запланованих заходів: тестування патчів, розгортання оновлень, зміна налаштувань, впровадження додаткових засобів захисту.

6) Перевірка та моніторинг – повторне сканування для підтвердження закриття уразливостей, контроль журналів і SIEM на відсутність ознак

експлуатації, складання звітності; після чого цикл повторюється з нового раунду сканування.

Такий підхід узгоджується з загальним циклом безпеки PDCA (Plan-Do-Check-Act). У моделі NIST наголос робиться на етапі планування і інтеграції з управлінням змінами – щоб виправлення вразливостей не порушувало стабільність роботи. Також NIST рекомендує паралельно вести процес моніторингу загроз: відстежувати чи не з'явилися нові методи обходу захисту, нові експлойти, що можуть вплинути на пріоритети в поточному циклі.

1.3.2 Модель SANS (PIACT).

Інститут SANS запропонував просту для запам'ятовування модель з п'яти фаз, позначену абревіатурою PIACT – Prepare, Identify, Analyze, Communicate, Treat. Ця модель описана, зокрема, в роботах фахівців SANS та в навчальних матеріалах [18]. Розглянемо її етапи.

1) Prepare (Підготовка). На цій фазі вибудовуються основи програми управління вразливостями. Визначаються цілі та обсяг – які системи і мережі охоплено, яка періодичність сканувань; формуються команди та призначаються відповідальні; збирається початкова інформація про активи і їх критичність; затверджуються політики (наприклад, політика застосування патчів). Якісна підготовка забезпечує успіх подальших кроків, не допускаючи пропуску критичних вузлів чи дублювання зусиль.

2) Identify (Виявлення). Фаза ідентифікації передбачає власне сканування систем на наявність відомих вразливостей та збір відповідних даних. Вона включає використання автоматизованих сканерів, ручний аудит, тестування безпеки – всього, що потрібно, аби скласти повний перелік актуальних вразливостей на кожному активі.

3) Analyze (Аналіз/Оцінка). На цьому етапі зібрану інформацію аналізують: фахівці з безпеки оцінюють ризик від кожної вразливості, групують їх, визначають причини. Важливо зрозуміти, які з виявлених уразливостей найбільш небезпечні для бізнесу. Тут застосовуються згадані принципи

пріоритизації – оцінки CVSS, контекст активів, дані про наявні експлойти тощо. Результатом аналізу є впорядкований список уразливостей, що потребують усунення, із зазначенням пріоритетів (наприклад, критичні – негайно, середні – протягом місяця тощо).

4) Communicate (Комунікація). SANS виділяє окремо цей аспект: результати аналізу мають бути донесені до відповідних стейкхолдерів. У рамках цієї фази команди безпеки готують звіти для IT-підрозділів (конкретний перелік систем і патчів, які треба встановити), для керівництва (агреговані показники ризику, статус відповідності політикам), а також проводять зустрічі з власниками систем для узгодження плану дій. Ефективна комунікація гарантує, що всі задіяні сторони розуміють серйозність проблеми і згодні виділити ресурси на виправлення. Без цього етапу процес може гальмуватися – наприклад, якщо IT-команда не усвідомить пріоритетності певного патча, він може бути відкладений.

5) Treat (Усунення). Фаза реалізації заходів – фактичне усунення вразливостей. Це може включати встановлення оновлень програмного забезпечення, зміни конфігурацій (відключення небезпечних сервісів, увімкнення додаткових опцій безпеки), впровадження компенсаційних заходів (WAF – Web Application Firewall, IPS – Intrusion Prevention System для захисту до патча) або навіть ізоляцію/виведення з експлуатації застарілих уразливих систем. На цьому етапі важлива співпраця між відділами: адміністратори виконують зміни, а фахівці з безпеки консультують щодо пріоритету (які системи виправляти першими) і перевіряють результати. Після завершення усунення цикл переходить знову до Phase 1 (Prepare) наступного ітераційного кола, де коригуються плани, оновлюється інвентар активів і т.д.

1.3.3 Модель Tenable (Cyber Exposure Lifecycle).

Компанія Tenable, розробник відомого сканера Nessus, просуває концепцію “життєвого циклу кіберекспозиції”, тісно пов’язаного з управлінням уразливостями. Ця модель складається з п’яти основних етапів: Discover,

Assess, Analyze, Fix, Measure – Виявлення, Оцінка, Аналіз, Усунення, Вимірювання. По суті, Tenable розширює технічну частину процесу й додає етап вимірювання ефективності:

1) Discover (Виявлення активів і вразливостей). Спочатку організація повинна виявити всі активи у своєму цифровому просторі та зібрати інформацію про відомі уразливості на них. Tenable наголошує на важливості динамічної інвентаризації: в сучасних умовах (хмара, контейнери, віддалені працівники) активи можуть з’являтися і зникати дуже швидко. Тому необхідні інструменти для постійного виявлення нових вузлів. Після виявлення активів виконується сканування на вразливості – таким чином збирається початковий перелік проблем.

2) Assess (Оцінка). Другий крок – оцінити отримані результати. Це включає і технічну оцінку (CVSS бал, параметри конфігурацій), і бізнес-контекст. Tenable, наприклад, об’єднує в понятті “Assess” як пошук уразливостей, так і виявлення неправильних конфігурацій, недотримання політик безпеки тощо [19]. Результатом етапу Assess є повна «карта» кіберекспозиції: розуміння, які активи наскільки вразливі.

3) Analyze (Аналіз ризику). На цьому етапі виконується кореляція та пріоритизація. Tenable інтегрує в аналіз дані про загрози: наприклад, чи є вразливість частиною відомої ланцюжка атак, чи використовується у поточних кампаніях зловмисників. Враховується критичність активу для бізнесу за допомогою особливих метрик Tenable. Мета – визначити, на які слабкості слід реагувати насамперед, а які можуть почекати. Саме на цьому етапі часто застосовуються сучасні інструменти, як згаданий EPSS, а також експертні знання аналітиків.

4) Fix (Усунення). Далі – усунути виявлені вразливості згідно з розставленими пріоритетами. Цей етап аналогічний фазі Treat у SANS-моделі. Особливість сучасного підходу – орієнтація на швидкість і автоматизацію. Наприклад, Tenable пропонує інтеграцію з системами управління виправленнями, щоб автоматично генерувати завдання на встановлення патчів

для IT-відділу. Також часто будуються конвеєри типу “виявлено – створено завдання на усунення – відслідковано виконання – повторно просканово”. У випадку критичних вразливостей, які не можуть бути негайно пропатчені, на етапі Fix реалізують тимчасові рішення: змінюють ACL, відключають уразливий сервіс, налаштовують WAF з правилом для блоку експлойту і т.д.

5) Measure (Вимірювання). Завершальний етап – виміряти ефективність виконаної роботи і залишковий ризик. Тут здійснюється побудова метрик: скільки уразливостей усунено, скільки залишилось відкритими (і чому), середній час виправлення, відсоток систем з актуальними патчами тощо. Також формується зворотний зв’язок для циклу – результати вимірювань використовуються при плануванні наступного циклу (Phase Discover/Assess). Наприклад, якщо виявлено, що певний тип систем стабільно відстає по патчах, це може означати проблему в процесі (відсутність відповідального чи слабкий контроль) – цю інформацію треба врахувати у фазі Prepare наступного циклу, призначивши додаткові ресурси.

1.3.4 Переваги та недоліки моделей управління вразливостями.

Розглянуті моделі мають багато спільного, проте відрізняються акцентами і рівнем деталізації, що впливає на їх застосовність у різних організаціях. Виокремимо їх сильні та слабкі сторони.

Модель NIST.

Переваги:

- комплексний системний підхід та прив’язка до загального управління ризиками.

Недоліки:

- відносна повільність і реактивність;
- перевантаженість формалізованими процесами.

Модель SANS PIACT.

Переваги:

- простота і зрозумілість;

- змістовне представлення планування процесу.

Недоліки:

- відсутність деталізації, необхідність спиратися на додаткові керівництва.

Модель Tenable (Cyber Exposure Lifecycle).

Переваги:

- орієнтація на сучасні динамічні середовища і автоматизацію;
- хороша інтеграція з інструментальними рішеннями;
- стимулює практику постійного вдосконалення і демонстрування прогресу.

Недоліки:

- складність і вимогливість до ресурсів;
- спрямування моделі під власні продукти;
- зосередження майже виключно на технічних аспектах.

Загалом, можна сказати, що моделі SANS і Tenable є двома кінцями спектру: перша – більш концептуальна і організаційна, друга – більш технічна і автоматизована. Модель NIST знаходиться посередині, збалансовуючи організаційні і технічні аспекти, але, можливо, поступається гнучкістю в дуже динамічних сценаріях. Вибір моделі залежить від масштабу та зрілості організації: невеликі компанії можуть почати з простого циклу PIACT, поступово вбудовуючи його в безперервний процес і додаючи інструменти (рух у бік Tenable-підходу); великі ж підприємства часто комбінують – використовують автоматизовані сканери і системи (Tenable), проте в рамках формального процесу з ролями та політиками (NIST/SANS).

Таким чином, у сучасних організаціях оптимальним є комплексний підхід, що поєднує сильні сторони різних моделей. Було обґрунтовано вибір оптимальної моделі як безперервного управління вразливостями, орієнтованого на ризик. Така модель передбачає постійний ітеративний цикл (на зразок моделі CIS/Tenable) – з регулярним скануванням і виправленням, – але під контролем

чіткої організаційної структури (як рекомендує SANS/NIST) та з використанням даних про актуальні загрози для пріоритизації (відповідно до найкращих сучасних практик). Оптимальна модель включає: налагоджений процес виявлення всіх активів і їх вразливостей (CMDB + сканери), автоматизоване надсилання сповіщень та створення завдань на усунення, закріплені SLA на виправлення вразливостей за категоріями критичності, регулярний моніторинг експлуатації вразливостей у світі та коригування пріоритетів на його основі, а також постійне відстеження ефективності через KPI.

Враховуючи усе вищезазначене, можна зробити висновок, що впровадження безперервного циклу управління вразливостями з акцентом на пріоритизацію ризиків є необхідною умовою кібербезпеки сучасної організації.

Висновки до розділу 1

Розглянуто ключові характеристики вразливостей (метрики CVSS), які визначають їх вплив та критичність. Це створює основу для стандартизованої пріоритизації вразливостей при їх усуненні.

Розкрито сутність системи CVE (Common Vulnerabilities and Exposures) як централізованого каталогу уразливостей. Наведено історію створення CVE, описано механізм наповнення бази CVE через партнерську мережу CNA (органи, що присвоюють CVE-ID) та вигоди для спільноти від використання CVE.

Досліджено процес управління вразливостями: простежено його еволюцію від ручного патч-менеджменту 1990-их до сучасних інтегрованих програм. Показано, що необхідність формалізованого процесу зумовлена зростанням загроз (хронічне використання зловмисниками відомих уразливостей, скорочення інтервалу між публікацією CVE та появою експлойтів) та вимогами регуляторів і стандартів.

Зазначено стандарти та проведено порівняння їх підходів: висновок полягає у їх взаємодоповнюваності (ISO задає що робити, NIST як планувати, CIS як підтримувати безперервність і швидкість), а загальна картина зводиться до проактивного, регулярного та ризик-орієнтованого процесу.

Виділено основні принципи управління вразливостями: проактивність (випереджувальне виявлення і усунення); пріоритизація за ризиком (фокус на найбільш небезпечних уразливостях першочергово); безперервність (циклічність процесу); комплексність (охоплення всіх елементів інфраструктури); документованість та контроль (формування політик, регламентів, контроль метрик, звітність). Дотримання цих принципів дозволяє будувати зрілу програму управління вразливостями.

Проведено огляд моделей життєвого циклу управління вразливостями від різних джерел: розглянуто підхід NIST (як послідовність етапів від підготовки до перевірки, інтегровану в загальний Risk Management Framework), модель SANS PIACT (Prepare, Identify, Analyze, Communicate, Treat), що акцентує на підготовчій та комунікаційній складових, та модель Tenable Cyber Exposure Lifecycle (Discover, Assess, Analyze, Fix, Measure), яка підкреслює безперервність та використання автоматизації і метрик. Порівняно переваги й недоліки цих моделей.

Розділ 2 ТЕХНІЧНІ ЗАСОБИ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ: РОЛЬ, ВАЖЛИВІСТЬ, АНАЛІЗ РІШЕНЬ

2.1 Роль та призначення технічних засобів управління вразливостями

Сучасні IT-середовища містять безліч компонентів (операційні системи, застосунки, бази даних, мережеве обладнання, хмарні сервіси тощо), кожен з яких потенційно може мати вразливості. Тому організаціям необхідна екосистема технічних засобів для автоматизації процесу управління вразливостями, що забезпечує безперервну видимість слабких місць та спрощує їх пріоритизацію й усунення [20-21].

Технічні засоби управління вразливостями – це програмні й апаратні рішення, призначені для сканування мереж, систем і застосунків з метою виявлення вразливих місць та допомоги у їх подальшому усуненні. На відміну від засобів захисту типу міжмережевих екранів чи систем виявлення вторгнень (IDS), які реагують на атаки в режимі реального часу, засоби VM працюють проактивно – вони шукають потенційні проблеми безпеки наперед і пропонують кроки для їх виправлення, щоб запобігти атакам до їх здійснення. По суті, інструменти VM виконують роботу за IT-підрозділ: відстежують хости та їх конфігурації, визначають застаріле ПЗ, відсутні виправлення та неправильні налаштування, а також перевіряють відповідність політикам безпеки. Якщо сканування виявляє слабкі місця, програмне забезпечення генерує сповіщення та рекомендації щодо усунення, а інколи навіть автоматизує застосування виправлень. Таким чином, ці інструменти знижують імовірність успішної атаки, даючи змогу закрити знайдені прогалини до того, як ними скористаються зловмисники.

Загалом можна виділити такі категорії та класифікації засобів VM.

1) *За підходом до сканування*: активні сканери (виконують перевірку систем по мережі), пасивні сканери (моніторять мережевий трафік для виявлення потенційно уразливих служб), агентні рішення (встановлюють

програмні агенти на хости для збору даних про вразливості) або комбіновані підходи. Більшість сучасних платформ VM підтримують як активне мережеве сканування, так і встановлення агентів на критичні вузли для безперервного моніторингу.

2) *За середовищем використання*: засоби для сканування мережевої інфраструктури та серверів; засоби для оцінки вразливостей веб-застосунків; інструменти для контейнерів і хмарних середовищ; спеціалізовані рішення для OT/SCADA систем тощо. Повноцінна програма VM охоплює різні рівні – від мережевого обладнання і операційних систем до веб-додатків та баз даних [22].

3) *За способом розгортання*: автономне ПЗ (on-premise) для встановлення у внутрішній інфраструктурі; хмарні сервіси (Software-as-a-Service, SaaS). Усі ці моделі фактично виконують схожі функції сканування, відмінність полягає у місці розміщення та моделі підтримки. Наприклад, платформа Qualys VMDR працює як SaaS-рішення з хмарною консоллю управління, Rapid7 InsightVM пропонує хмарну аналітику з локальними сканерами, а Tenable Security Center (Tenable SC) розгортається у мережі замовника як сервер управління скануваннями [23].

4) *За функціональним призначенням у процесі VM*: засоби виявлення та інвентаризації активів (для побудови повного переліку систем, що підлягають скануванню); сканери вразливостей (ядро процесу – виконують перевірку систем на наявність відомих уразливостей); засоби аналізу та пріоритизації (накладають контекст ризику – наприклад, використовують дані про критичність активів, наявність експлойтів, актуальність загроз тощо для визначення пріоритетів виправлення); інструменти управління виправленнями (patch management), які можуть автоматично або напівавтоматично застосовувати патчі та оновлення; засоби звітування і відстеження прогресу (для контролю метрик, формування звітів про стан безпеки, відповідність стандартам та ін.). Сучасні інтегровані VM-платформи намагаються охопити усі ці аспекти в одному рішенні або через тісні інтеграції з суміжними продуктами.

Незалежно від конкретного типу рішення, технічні засоби VM відіграють ключову роль в екосистемі управління вразливостями.

По-перше, без автоматизованих сканерів неможливо масштабувати процес виявлення вразливостей у великих мережах – ручні перевірки є надто трудомісткими і неефективними. Як зазначається в дослідженнях, організації, що не мають автоматизованого ПЗ для VM, змушені діяти “наосліп”: вони встановлюють виправлення хаотично і лише реагують на інциденти, що є нераціональним підходом [24].

По-друге, інструменти VM забезпечують безперервність процесу – регулярні сканування (щоденні, щотижневі або постійний моніторинг агентами) дозволяють своєчасно виявляти нові вразливості, що з’являються внаслідок змін у системах чи появи нових загроз [25].

По-третє, ці засоби додають структурованості та об’єктивності в процес: вони надають оцінки ризику (бали CVSS або власні рейтинги ризику), що допомагає обрати, на які проблеми звернути увагу в першу чергу, а також фіксують всі виявлені вразливості в центральній базі даних для подальшого відстеження прогресу виправлення.

Важливою функцією технічних засобів є інтеграція з іншими компонентами кібербезпеки. Дані сканерів вразливостей можуть автоматично передаватися в системи управління інцидентами (SIEM) та оркестрації (SOAR - Security Orchestration Automation and Response) для кореляції з іншими подіями, до засобів керування конфігураціями (наприклад, для виявлення відхилень від політик безпеки) чи в системи управління IT-активами. Також часто впроваджується інтеграція з сервіс-десками (ITSM) – наприклад, виявлена критична вразливість може автоматично створювати завдання на її усунення у команді IT. Таким чином, технічні засоби VM є сполучною ланкою між виявленням проблеми та її практичним вирішенням, вбудовуючи управління вразливостями у загальні процеси забезпечення кібербезпеки та IT-експлуатації.

Отже, значення технічних засобів в екосистемі VM полягає в тому, що вони дозволяють зробити процес управління вразливостями систематичним, безперервним і контрольованим. Без належних інструментів навіть наявність політики та обізнаного персоналу не гарантує успіху, адже масштаб сучасних IT-інфраструктур і динаміка появи нових загроз вимагають автоматизації. У наступному розділі проведено аналіз провідних сучасних платформ VM, які інтегрують в собі описані функції, – це рішення компаній Tenable, Qualys та Rapid7, що здобули визнання експертної спільноти та займають лідерські позиції на ринку.

2.2 Порівняльний аналіз провідних платформ управління вразливостями

Сьогодні існує декілька десятків комерційних і відкритих інструментів для управління вразливостями, утім ринок корпоративних VM-рішень очолює відносно невелика група вендорів. Незалежні галузеві аналізи та рейтинги послідовно відзначають серед лідерів компанії Tenable, Qualys та Rapid7. Згідно з дослідженням IDC, сукупна частка цих трьох постачальників становить понад 60% світового ринку рішень для управління вразливостями пристроїв [26-28]. Зокрема, компанія Tenable у 2023 році посідає перше місце з приблизно 29% ринку (рис. 2.1), випереджаючи Qualys (≈19%) та Rapid7 (≈14%).

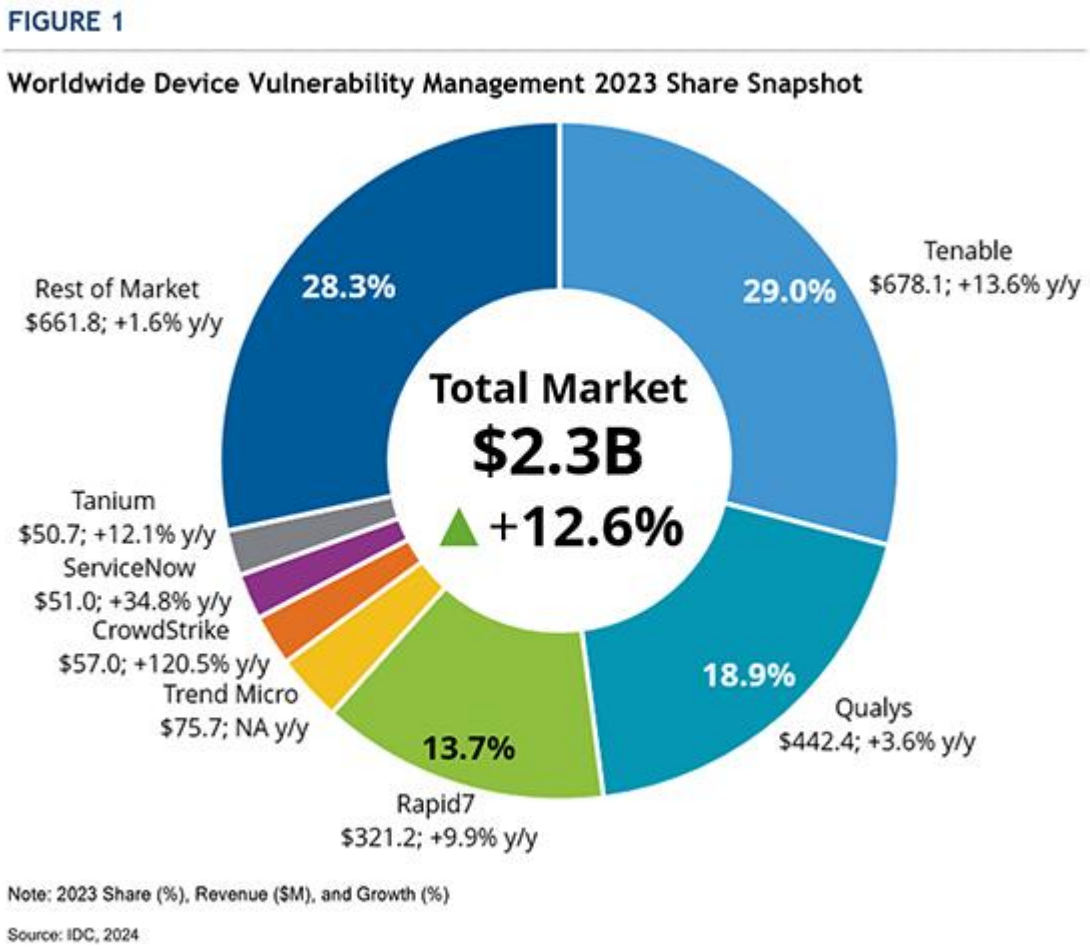


Рис. 2.1. Розподіл ринку VM-рішень за даними IDC станом на 2023р. [29]

Водночас у згаданому сегменті зростає конкуренція з боку інших гравців – таких як Microsoft (Defender Vulnerability Management), Palo Alto Networks, Trend Micro, а також нових платформ, що фокусуються на пріоритезації ризиків (наприклад, Kenna Security від Cisco, Skybox Security, Balbix, Vulcan Cyber тощо). Проте рішення Tenable Security Center (засноване на сканерах Nessus), Qualys VMDR та Rapid7 InsightVM продовжують залишатися еталонами у сфері VM і часто фігурують у порівняльних оглядах як основні альтернативи один одному [30].

2.2.1 Огляд провідних рішень.

Tenable Security Center (Tenable SC) – це корпоративна платформа від компанії Tenable, яка забезпечує централізоване управління вразливостями на основі сканерів Nessus. Tenable засновано у 2002 р., і її продукт Nessus був одним із перших популярних сканерів вразливостей (початково випущений ще у 1998 р. як вільне ПЗ). Tenable SC (раніше відомий як Tenable.sc або Nessus Enterprise) є локально встановлюваним рішенням (on-premise) і зазвичай розгортається у мережі організації: одна або кілька серверних інстанцій SC виконують роль консолі, а розподілені сканери Nessus проводять перевірку активів. Tenable SC надає єдиний веб-інтерфейс для планування сканувань, перегляду результатів, формування звітів та відстеження показників ризику. Архітектурно платформа підтримує активне сканування (через Nessus) та пасивний моніторинг мережі (через модуль Tenable Nessus Network Monitor) для виявлення нових пристроїв і трафіку, що може свідчити про наявність уразливих служб. Також Tenable пропонує хмарне рішення Tenable VM та комплексну платформу Tenable One, утім у цьому дослідженні робиться акцент на версії Security Center як основній для великого корпоративного середовища.

Qualys VMDR (Vulnerability Management, Detection and Response) – хмарна платформа від компанії Qualys, яка є піонером у сфері VM-сервісів (Qualys засновано у 1999 р. і вона була однією з перших, хто запропонував сканування вразливостей за моделлю SaaS). Рішення Qualys VMDR надається користувачам повністю у хмарному форматі: Qualys Cloud Platform забезпечує веб-інтерфейс та аналітику, а сканери розгортаються у середовищі замовника у вигляді віртуальних машин або агентів (Qualys Cloud Agent) на самих хостах. VMDR – це комплексний набір модулів, що включає власне управління вразливостями, а також функції виявлення активів, розширений аналіз загроз та навіть базові засоби реагування (застосування патчів). Сканери Qualys можуть постійно працювати у мережі, проводячи безперервну оцінку стану систем і негайно повідомляючи про знайдені критичні проблеми. У базі Qualys – одна з найбільших бібліотек перевірок вразливостей (більше 100 тис. підписів), що

охоплює широкий спектр ОС, СУБД – Система Управління Базами Даних, мережевих пристроїв та застосунків. Платформа також пропонує засоби автоматичного розставлення пріоритетів на основі поєднання CVSS-балу, наявності експлойтів, активності зловмисників (через інтегровані стрічки Threat Intelligence) та критичності активу. Слово “Response” у назві VMDR означає, що Qualys інтегрувала можливості реагування – зокрема, модуль Patch Management, який може автоматично завантажувати та встановлювати патчі на уразливі системи безпосередньо з консолі Qualys [31].

Rapid7 InsightVM – рішення компанії Rapid7, що продовжує лінійку продуктів Nexpose (перейменоване на InsightVM з додаванням хмарних аналітичних можливостей). Rapid7 вийшла на ринок VM у 2009 році, придбавши проект Metasploit – відому платформу для експлуатації вразливостей, – що згодом стало її конкурентною перевагою. InsightVM за архітектурою є гібридним рішенням: локальні сканери Nexpose здійснюють перевірку мережевих активів, а зібрані дані передаються до хмарної платформи Rapid7 Insight для глибокого аналізу та побудови інтерактивних панелей моніторингу. Користувачі взаємодіють через веб-інтерфейс Insight, який надає розширені можливості аналітики, дашборди, відстеження прогресу та інші модулі (зокрема, інтеграцію з SIEM InsightIDR, SOAR InsightConnect тощо). Особливістю Rapid7 InsightVM є гнучка система оцінки ризиків: окрім стандартних балів CVSS, платформа розраховує власний показник ризику для кожної знайденої вразливості – так званий Real Risk score у діапазоні 1–1000, що враховує ймовірність експлуатації, наявність шкідливих кампаній, важливість хоста та інші фактори. Це дозволяє краще ранжувати виявлені проблеми та фокусуватися на дійсно критичних загрозах, а не лише на номінально високих CVSS. InsightVM також тісно інтегрований з Metasploit: користувачі можуть напряму перевірити, чи можлива експлуатація певної вразливості, запустивши модуль Metasploit з консолі – це допомагає відсіяти хибнопозитивні (false-positive) результати і побачити реальний “шлях атаки”. Для розширення охоплення Rapid7 пропонує агенти Insight Agent, які

встановлюються на кінцеві точки та збирають дані про вразливості навіть на пристроях, що не завжди в мережі, доповнюючи тим самим традиційне сканування.

Для узагальнення характеристик платформ, наведемо стандартизований технічний профіль Tenable SC, Qualys VMDR та Rapid7 InsightVM за рядом ключових критеріїв у табл. 2.1.

Таблиця 2.1

Порівняння характеристик провідних платформ управління вразливостями Tenable SC, Qualys VMDR, Rapid7 InsightVM

Критерій	**Tenable Security Center**	**Qualys VMDR**	**Rapid7 InsightVM**
Модель розгортання	Локально (on-premise)	Хмарна (SaaS)	Гібридна
Охоплення середовищ	• Мережеві пристрої; • ОС (Windows, Linux, macOS); • веб-застосунки.	• Мережеві пристрої; • ОС (Windows, Linux, macOS); • веб-застосунки; • хмарні сервіси; • мобільні пристрої; • контейнери.	• Мережеві пристрої; • ОС (Windows, Linux, macOS).
Методи сканування	• Активне; • пасивне; • агентне.	• Активне; • агентне.	• Активне; • агентне.
Пріоритизація ризиків	• CVSS; • власні метрики для оцінки загроз та критичності активів.	• CVSS; • власні метрики для оцінки загроз та критичності активів.	• CVSS; • власні метрики для оцінки загроз та критичності активів.
Звітування та аналітика	Гнучкий функціонал створення дашбордів та звітів.	Гнучкий функціонал створення дашбордів та звітів.	Обмеженість функціоналу створення дашбордів та звітів.

Продовження таблиці 2.1

Критерій	Tenable Security Center	Qualys VMDR	Rapid7 InsightVM
Інтеграції та сумісність	• Гарно задокументоване REST API; • існують готові конектори; • підтримує імпорт даних з різних джерел.	• Обмежене у кількості запитів API (SOAP/XML та REST); • існують готові конектори.	• RESTful API; • існують готові конектори.
Унікальні особливості	• Велика спільнота користувачів (Tenable Community); • розвиток передової концепції Exposure Management; • інтеграція з іншими рішеннями екосистеми Tenable.	• Інтегроване рішення застосування патчів безпеки.	• Унікальна інтеграція з Metasploit; • консоль має вбудований сканер; • інтеграція з іншими рішеннями екосистеми Rapid7.

2.2.2 Аналіз переваг і недоліків платформ.

Кожна з розглянутих платформ має свої сильні сторони і недоліки, які важливо врахувати при виборі рішення для конкретної організації. Спираючись на незалежні огляди та відгуки користувачів, нижче представлено детальний аналіз переваг та слабких місць Tenable SC, Qualys VMDR та Rapid7 InsightVM.

Tenable Security Center.

Переваги:

- гнучкість налаштувань і можливість глибокої кастомізації сканувань під потреби організації;

- потужні сканера Nessus з високою точністю та глибиною перевірок (Tenable багато років утримує одну з найбільших баз сигнатур вразливостей і регулярно оновлює її);
- підтримка унікального пасивного аналізу мережі для виявлення “тіньових” активів;
- інтеграція з екосистемою Tenable: забезпечення додаткових можливостей у разі наявності екосистеми через інтеграції з іншими додатками (Tenable OT, Tenable VM, Tenable WAS тощо);
- активна спільнота та велика кількість матеріалів для навчання й сертифікації фахівців (Nessus є фактичним стандартом де-факто серед сканерів).

Недоліки:

- менш інтуїтивний порівняно з сучасними хмарними конкурентами;
- наявність кількох продуктів у лінійці Tenable може заплутати – Nessus, Tenable.sc, Tenable.io, Tenable One – організаціям треба чітко обрати свій шлях, що інколи викликає складнощі з точки зору стратегії (хмарне чи локальне рішення).

Qualys VMDR.

Переваги:

- надзвичайно широке покриття технологій;
- низькі вимоги до інфраструктури через модель розгортання SaaS;
- єдина платформа для всіх модулів – управління вразливостями, інвентаризація, моніторинг конфігурацій і застосування патчів працюють комплексно;
- автоматизація: багато процесів можуть виконуватися без участі людини (постійна робота агентів, автоматичне завантаження патчів тощо), що зменшує навантаження на персонал.

Недоліки:

- доволі стрімкий поріг навчання – незважаючи на якісний інтерфейс, продукт містить дуже багато функцій, модулів і налаштувань, через що нові користувачі відзначають круту криву освоєння;
- “хмарність” може бути проблемою для деяких – платформа залежить від постійного інтернет-з’єднання з серверами Qualys, що не завжди прийнятно для організацій із жорсткими вимогами до ізоляції мереж (відсутність повної on-prem версії);
- обмеження на API – користувачі повідомляють про ліміти на кількість API-запитів на добу, що може ускладнювати інтеграції при великому масштабі;
- модель ліцензування і ціноутворення – Qualys історично не є дешевим рішенням, а окремі функції (як-от сканування певних типів активів) можуть вимагати додаткових ліцензій, що підвищує загальну вартість.

Rapid7 InsightVM.

Переваги:

- можливість проводити сканування “з коробки” через вбудований сканер;
- відкритий проект Metasploit забезпечує швидку появу експлойтів для перевірки;
- інтеграція з екосистемою Rapid7: тісний зв’язок з модулем поведінкового аналізу UserInsight, SIEM InsightIDR тощо, що дає переваги комплексного підходу у разі наявності екосистеми;

Недоліки:

- дещо застарілий інтерфейс користувача;
- частина функцій (наприклад, деякі види сканувань на перевірку відповідності чи контекстного аналізу) менш розвинені, ніж у конкурентів – Rapid7 більше фокусується саме на аспекті ризиків і інтеграції з власними продуктами, тоді як Qualys має перевагу в глибині політик відповідності, а Tenable – в широті охоплення завдяки стороннім модулям;

- іноді зустрічаються хибнопозитивні результати – сканер може вказати на можливу уразливість, якої насправді немає, хоча це певною мірою притаманно всім інструментам VM;
- обмеженість у створенні дашбордів та звітності, зокрема через відсутність певних нестандартних фільтрів або потреба писати складні SQL-подібні запити для вибірки даних.

Узагальнені висновки також зведено у табличну форму (табл. 2.2) для наочності [32-33].

Таблиця 2.2

Основні переваги та недоліки провідних VM-платформ

Платформа VM	**Переваги**	**Недоліки**
Tenable SC	- Гнучкість налаштувань; - еталонний сканер Nessus; - унікальний тип сканування; - можливість інтеграції з екосистемою Tenable; - велика та активна спільнота.	- Менш інтуїтивний інтерфейс; - ускладнення вибору платформи поміж схожих продуктів Tenable.
Qualys VMDR	- Широке покриття; - SaaS; - унітарність управління платформи; - висока базова автоматизація процесів.	- Стрімка крива навчання; - SaaS; - висока вартість, складна модель ліцензування; - обмеження на API.
Rapid7 InsightVM	- Сканування «з коробки»; - вбудована інтеграція з Metasploit; - можливість інтеграції з екосистемою Rapid7.	- Дещо застарілий інтерфейс - обмеженість у створенні звітів та дашбордів; - частіше виникають хибнопозитивні результати сканування, ніж у конкурентів; - деякий функціонал сканування менш розвинутий.

З наведеного аналізу можна зрозуміти, що жодна платформа не є ідеальною і вибір залежить від пріоритетів та контексту організації. Tenable SC підходить тим, хто бажає повного контролю on-premise та цінує глибину сканування; Qualys VMDR приваблює широкою функціональністю “все в одному” та мінімальними вимогами до підтримки інфраструктури; Rapid7 InsightVM вирізняється інноваційним підходом до оцінки ризику та інтеграцією з іншими інструментами захисту.

2.2.3 Обґрунтування вибору платформи Tenable SC для дослідження.

Беручи до уваги результати порівняння, для глибинного дослідження в рамках цієї кваліфікаційної роботи обрано платформу Tenable Security Center як основну. Це рішення обґрунтовується сукупністю факторів.

Лідерство на ринку та визнання експертів. Tenable протягом кількох років поспіль посідає перше місце за часткою світового ринку VM-рішень та отримує високі оцінки в незалежних рейтингах (наприклад, Forrester Wave 2019 назвав Tenable серед лідерів ринку поряд з Qualys і Rapid7, а у Forrester Wave 2023 платформа Tenable знов очолила категорію завдяки стратегії та широкому охопленню ризиків [34-35]). Така репутація свідчить про зрілість технології та довіру до неї з боку спільноти безпеки.

Відповідність потребам великої організації. Tenable SC як on-premise рішення добре пасує для середовищ, де важливо зберігати всі дані про вразливості всередині контуру безпеки компанії (без передачі у хмару). Багато підприємств з секторів фінансів, урядових установ, оборони обирають Tenable саме з міркувань контролю даних та гнучкості налаштування під власні процеси. Наша подальша мета – дослідити методику управління вразливостями у прив’язці до конкретного інструмента; Tenable SC надає всі необхідні гвинтики для гранулярного налаштування процесу, що дозволяє продемонструвати взаємозв’язок між функціоналом платформи і організаційними практиками.

Широка інтегрованість та розширюваність. Tenable SC легко інтегрується з зовнішніми рішеннями (як-от ServiceNow для управління виправленнями або Splunk для кореляції інцидентів), а також підтримує імпорт/експорт даних зі сторонніх сканерів. Таким чином, на базі Tenable SC можна реалізувати повний цикл управління вразливостями, включаючи виявлення, аналіз, виправлення і контроль, що відповідає цілям дослідження.

Практичний досвід впровадження. Додатково, вибір Tenable SC зумовлений наявністю практичного досвіду використання цієї платформи в рамках переддипломної практики автора. Це дозволяє провести прикладний експеримент чи дослідження певного випадку на реальних даних, що підсилює наукову цінність роботи.

Отже, Tenable Security Center обрано як базову платформу для подальших розробок методики управління вразливостями у розділі 3. На цьому етапі важливо підкреслити, що впровадження будь-якого з розглянутих рішень має розглядатися крізь призму організаційних процесів. Далі буде обґрунтовано, чому наявність навіть найпотужнішого інструмента не гарантує успіху без належної методології, і як можливості платформи Tenable SC можуть бути ефективно використані в рамках зрілого процесу VM.

2.3 Важливість методики управління вразливостями

Впровадження платформи управління вразливостями – необхідний, але недостатній крок для побудови дієвої системи кіберзахисту. Практика показує, що результати залежать не тільки від вибору інструменту, а й від методики його використання, зрілості процесів та компетенції команди. Як влучно зауважив експерт SANS Джон Ріето: «Ви не можете перемогти в управлінні вразливостями. Ви можете лише дозріти та стати кращими в цьому», маючи на увазі, що це безперервна діяльність, успіх якої вимірюється покращенням показників з часом [36-37]. Таким чином, після вибору платформи постає питання: як вибудувати процес управління вразливостями навколо цього

інструменту, щоби максимально реалізувати його потенціал і підвищити зрілість програми VM?

Методика управління вразливостями – це формалізований набір політик, процедур і кроків, що визначають хто, коли і як виконує завдання виявлення, аналізу, усунення та моніторингу вразливостей. Правильно розроблена методика враховує можливості конкретної VM-платформи, вписуючи її в загальний робочий процес. Взаємозв'язок між функціоналом платформи та процесною зрілістю організації двосторонній: з одного боку, зрілі процеси дозволяють отримати максимальну користь з інструменту (наприклад, налагоджений процес управління активами забезпечить актуальний інвентар, який сканер буде перевіряти, а налагоджений процес патч-менеджменту гарантує швидке реагування на звіти платформи); з іншого боку, сучасні платформи надають функції (автоматизацію, оркестрацію, аналітику), що можуть "підняти" зрілість процесів на новий рівень, якщо їх впровадити правильно.

Розглянемо декілька аспектів, чому методика, прив'язана до платформи VM, є критично важливою.

Повнота охоплення (scope) та етап Підготовка. Базовий рівень зрілості VM-програми починається з чіткого визначення периметру сканування та регулярності перевірок. Платформа Tenable SC надає засоби імпорту даних з CMDB та автоматичного виявлення нових хостів (через пасивний моніторинг). Методика повинна регламентувати використання цих можливостей: наприклад, процедура онбордингу нових активів може включати автоматичне додавання їх до політики сканування Tenable SC і встановлення на них агента Nessus (якщо це передбачено). На етапі Prepare за моделлю SANS VMMM організація забезпечує наявність актуального інвентарю та необхідних доступів для сканера – і тут інтеграція CMDB з Tenable SC чи регулярний імпорт даних про хости є процесним рішенням, що випливає з можливостей платформи.

Оцінка та пріоритезація (етап Аналіз). Сучасні VM-інструменти пропонують розвинені механізми рейтингу ризиків (як обговорювалося,

наприклад, VPR у Tenable, Threat Priority у Qualys, Risk Score у Rapid7). Але без методології існує ризик, що ці рейтинги залишаться невикористаними належним чином. Організація повинна розробити політику: які пороги ризику встановлюються для реагування, в які терміни мають виправлятися вразливості різних критичностей, як обробляти винятки (false positives, або вразливості, що не можуть бути виправлені з об'єктивних причин). Методика може встановлювати, що, скажімо, всі вразливості з VPR ≥ 9.0 мають бути виправлені протягом 7 днів, з 7.0–8.9 – протягом 30 днів, а нижче 7.0 – за рішенням ризик-менеджера. Наявність в Tenable SC функції тегування активів і вразливостей дозволяє процесно реалізувати ці правила (наприклад, автоматично тегувати "Overdue" вразливості, які перевищили дедлайн, і генерувати для них звіт для керівництва). Таким чином, можливості платформи (оцінка ризику, тегування, нотифікації) мають бути відображені в регламентах роботи команди безпеки.

Ремедіація (етап Усунення/Treat). Найважливіший елемент – виправлення знайдених уразливостей – виходить за межі самої VM-платформи, охоплюючи IT-відділ, девопсів тощо. Тут методика критично необхідна для забезпечення спільної роботи підрозділів. Платформа може допомогти: Tenable SC, наприклад, може відправляти результати сканування напряму в ServiceNow для створення завдань на усунення. Методика повинна визначати, як саме використовується цей функціонал: чи створюються завдання автоматично для кожної критичної уразливості, чи команда безпеки спочатку переглядає та групує їх; хто відповідає за моніторинг завдань та оновлення їх статусу; як проводиться повторне сканування після виправлення. Від процесної зрілості на цьому етапі залежить реальна ефективність всієї програми VM – як зазначає огляд JetPatch, багато традиційних VM-інструментів «виявляють вразливості, але залишають подальшу роботу на вашу команду». Тому розробка методики, що накриває "останню милю" (від звіту про уразливість до встановлення патчу), з використанням можливостей платформи (автоматизації, інтеграцій) є обов'язковою умовою успіху. Якщо Tenable SC пропонує API, методика може

передбачати написання скриптів для масового підтвердження виправлення (щоб закривати десятки елементів після патчу автоматично) тощо.

Комунікація та звітність (eman Communicate). Зрілість процесу також визначається тим, як результати VM-програми доносяться до зацікавлених сторін – керівництва, аудиторів, команд-винуватців (asset owners). Тут можливості платформи (генерація звітів, дашборди) є лише інструментом, який слід правильно застосувати. Методика може встановлювати щомісячні звіти різного рівня деталізації: операційний звіт для IT з переліком конкретних систем і патчів; управлінський KPI-звіт для CISO із метриками (кількість критичних вразливостей, середній час виправлення тощо). Tenable SC дозволяє налаштувати обидва, але методика визначає які саме метрики важливі організації та на які показники орієнтуватися. Наприклад, якщо організація впровадила модель зрілості VM (як у SANS VMMM чи подібну [38]), то може відстежувати прогрес: перехід зі Stage 2 (де багато неотриманого контексту) до Stage 3 (пріоритезація за ризиком) можна побачити у вигляді зменшення "завалу" невиправлених вразливостей низького ризику тощо. Платформа надасть цифри, але інтерпретація їх покладається на процес (правильні KPI, регулярні огляди тощо).

Підсумовуючи, методика управління вразливостями, яка будується навколо можливостей VM-платформи, дозволяє підняти програму з рівня простого реагування на рівень проактивного та керованого процесу. Взаємодія між інструментом і процесом можна порівняти з взаємодією між аптечкою і лікарем: найсучасніше обладнання буде мало корисним без протоколу лікування, але й найкращий лікар, не маючи інструментів, буде обмежений у допомозі. Тому успішні організації інвестують і в технології VM, і в розробку рамок та політик їх використання.

Зокрема, Tenable пропонує клієнтам рекомендації з побудови програми VM, наголошуючи на необхідності поєднання кращих практик (best practices) та функціоналу продукту. У їх "Complete Guide" підкреслюється, що для підвищення зрілості потрібно будувати міцний фундамент процесів і

оптимізувати їх [39]. Такі ж тези знаходять підтвердження у незалежних джерелах: дослідження eSecurityPlanet зазначає, що багато команд зменшують “розпорошеність” інструментів, обираючи одну платформу, але обов’язково інтегрують її з іншими засобами та вписують у загальний цикл безпеки [40].

Отже, у розділі 3 буде детальніше розглянуто методику управління вразливостями, що враховує можливості Tenable Security Center і спрямована на підвищення зрілості процесу VM. Будуть описані кроки процесу (від підготовки до усунення і контролю), роль відповідальних осіб на кожному етапі, приклади використання функцій платформи для автоматизації чи оптимізації, а також запропоновано метрики для оцінки ефективності методики.

Висновки до розділу 2

У цьому розділі проведено дослідження технічних засобів управління вразливостями та їх ролі в процесі VM. Результати можна підсумувати наступними основними положеннями.

Технічні засоби є невід’ємною частиною екосистеми управління вразливостями. Вони забезпечують автоматизацію ключових етапів – виявлення вразливостей шляхом сканування, допомагають у їх оцінці та пріоритезації, надають інструменти для відстеження виправлення та формування звітності. Без таких засобів масштабна програма VM в сучасній великій IT-інфраструктурі практично неможлива.

Лідерами серед VM-рішень на ринку є Tenable Security Center, Qualys VMDR та Rapid7 InsightVM. Ці платформи отримали визнання як з боку користувачів, так і в аналітичних звітах (Forrester, IDC тощо), займаючи сумарно понад половину світового ринку VM. Проведений порівняльний аналіз показав, що кожна з них пропонує широкий набір функцій (сканування різних типів активів, власні механізми оцінки ризику, інтеграції, звітність), при цьому маючи свої переваги та недоліки, які варто враховувати (від особливостей інтерфейсу до ліцензійних нюансів).

Для подальшого поглибленого дослідження було обрано платформу Tenable Security Center (Tenable SC). Це обрання обґрунтоване її лідерською позицією та відповідністю умовам використання (on-premise розгортання, гнучкі налаштування, широкий спектр підтримуваних технологій). Важливо, що Tenable SC не розглядається як “краще” рішення абсолютно для всіх випадків – проте, воно містить усі типові компоненти VM-платформи, і висновки дослідження будуть релевантними і для інших подібних продуктів.

Наголошено на важливості методики управління вразливостями, тісно пов’язаної з використанням VM-платформи. Технологія без належного процесу може бути малоефективною: наприклад, просто впровадити сканер недостатньо – потрібно визначити регламенти сканування, обробки результатів, відповідальності та строки виправлення. Зрілість програми VM оцінюється не лише наявністю інструментів, а й тим, наскільки вони вбудовані в щоденні операції і стратегічне планування безпеки. Розглянуто взаємозалежність: платформа Tenable SC надає функціонал (пріоритезація VPR, інтеграція з тикет-системами, дашборди KPI тощо), який слід закріпити у політиках і процедурах. Тільки таким чином організація може перейти на високі рівні зрілості VM – коли процеси Prepare, Identify, Analyze, Communicate, Treat (за моделлю SANS VMMM) виконуються послідовно і безперервно, значною мірою автоматизовано засобами платформи.

У наступних розділах сформовані висновки будуть використані для практичного моделювання методики VM на основі Tenable SC, що продемонструє, як теорія втілюється у практичні кроки. Завдяки цьому можна буде оцінити ефективність запропонованого підходу та визначити рекомендації щодо впровадження його в реальних умовах.

Розділ 3 МЕТОДИКА УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ З ВИКОРИСТАННЯМ TENABLE SC

3.1 Prepare (Підготовка)

3.1.1 Створення та налаштування політики сканування.

На етапі Prepare організація впроваджує необхідні політики й процедури для підтримки ефективного процесу управління вразливостями [41]. Згідно з моделлю SANS, це включає розробку внутрішніх стандартів сканування та налаштування середовища до початку виявлення вразливостей. Політика сканування визначає, що і як сканувати, забезпечуючи узгодженість процесу з обраними стандартами безпеки.

Функціонал Tenable Security Center. Політика сканування – це перелік налаштувань і плагінів для сканера, які застосовуються до майбутніх перевірок мережі [42].Таким чином, політики сканування дозволяють стандартизувати параметри перевірки у масштабі організації (наприклад, глибину сканування, рівень «агресивності» тестів, перевірку на відомі вразливості тощо) відповідно до прийнятих політик безпеки.

Покрокова інструкція. Процес налаштування нової політики сканування в Tenable.sc включає декілька кроків.

1) Вхід у розділ політик. Увійти до Tenable Security Center з обліковим записом адміністратора. Перейти в меню Scanning > Policies (для адміністратора; для організаційного користувача – Scans > Policies). Відкриється сторінка керування політиками [43].

2) Створення політики. Натиснути кнопку Add (Додати) для створення нової політики. Відкриється майстер створення політики сканування (рис. 3.1). Спочатку обрати тип політики: або один з наявних шаблонів Tenable (наприклад, “Basic Network Scan”, “Credentialed Patch Audit” тощо), або режим Advanced Scan для повного налаштування з нуля.

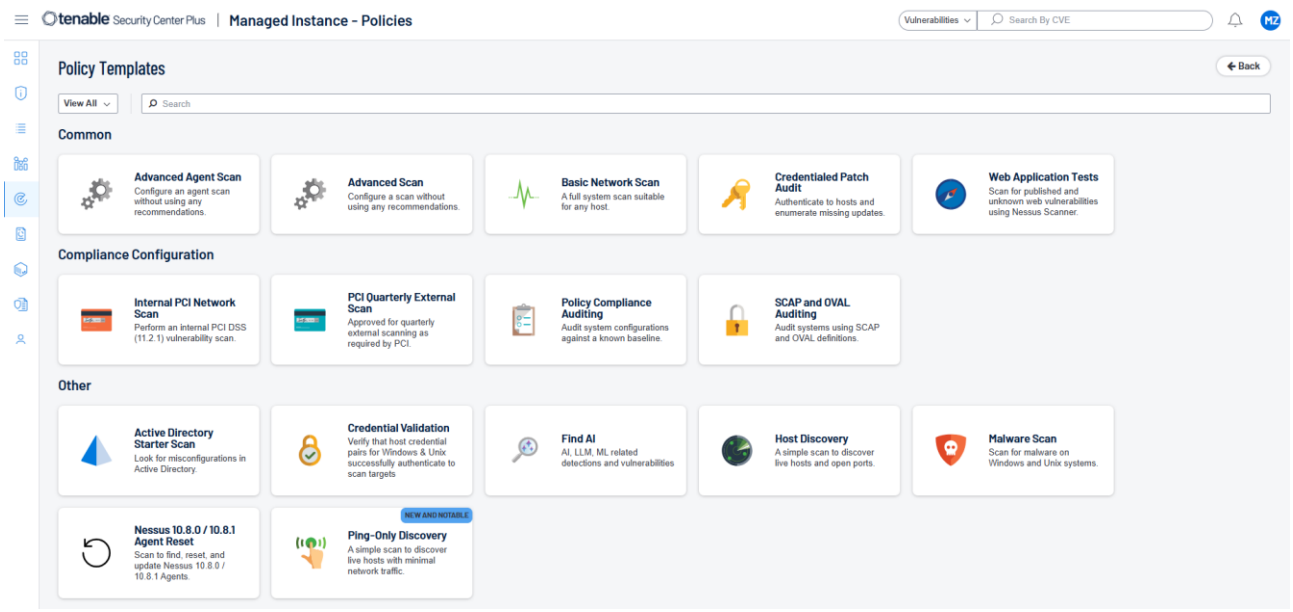


Рис. 3.1. Вибір політики сканування

3) Налаштування параметрів. Вказати основні параметри політики: ім’я (Name) та опис (для чого призначена політика). Далі налаштувати опції сканування – наприклад, діапазон плагінів, рівень перевірок, параметри продуктивності, автентифікації тощо – згідно з обраним шаблоном або в розширених налаштуваннях. На цьому етапі доступні всі опції, аналогічні налаштуванням Nessus.

4) Збереження політики. Після завершення конфігурації натиснути Submit (Зберегти). Новостворена політика з’явиться у списку та стане доступною для використання при запуску сканувань.

Вплив на зрілість процесу. Розробка власних політик сканування підвищує стандартизацію та передбачуваність процесу виявлення вразливостей. Впровадження чітких, задокументованих політик на основі галузевих практик виводить програму на визначений рівень зрілості (Level 3 – Defined) за моделлю SANS.

3.1.2 Створення та налаштування сканування.

Наступним кроком етапу Prepare є планування безпосереднього процесу сканування. Визначення методів і графіків сканування всіх релевантних активів організації – критично важливе підґрунтя перед переходом до етапу Identify.

SANS VMMM наголошує на необхідності стандартизованих засобів виявлення вразливостей: організація повинна заздалегідь обрати інструменти та методи сканування, якими вона буде користуватися постійно [44]. На практиці це означає затвердження розкладу регулярних перевірок, охоплення всіх груп IT-ресурсів і визначення відповідальних осіб ще до запуску перших сканувань.

Функціонал Tenable Security Center. У Tenable Security Center конфігурація безпосереднього сканування здійснюється через створення об’єкта типу Active Scan (активне сканування). Active Scans визначають конкретне завдання сканування – які активи сканувати, за якою політикою, коли саме запускати перевірку, куди зберігати результати тощо. Кожне створене сканування можна запускати вручну або за розкладом. Таким чином, на етапі Prepare адміністратор налаштовує декілька регулярних сканувань, що охоплюють усі необхідні сегменти інфраструктури.

Покрокова інструкція. Приклад налаштування нового сканування в Tenable.sc наведено нижче.

1) Створення сканування. У консолі Tenable Security Center перейти до Scans > Active Scans і натиснути Add для додавання нового сканування. Відкриється форма конфігурації Active Scan [45].

2) Основні параметри. На вкладці General (рис. 3.2) вказати Name (назву сканування) та при потребі опис. У полі Policy вибрати раніше створену політику сканування, яка буде використана для цього завдання. За необхідності задати розклад (Schedule): наприклад, щотижневе автоматичне виконання.

3) Додаткові налаштування. Перейти на вкладку Settings. Тут можна вибрати зону сканування (Scan Zone, якщо в інфраструктурі декілька сканерів), репозиторій для імпорту результатів (Import Repository), налаштувати час очікування та поведінку при перевищенні тривалості сканування (Scan Timeout Action), а також опції повтору/перенесення сканування.

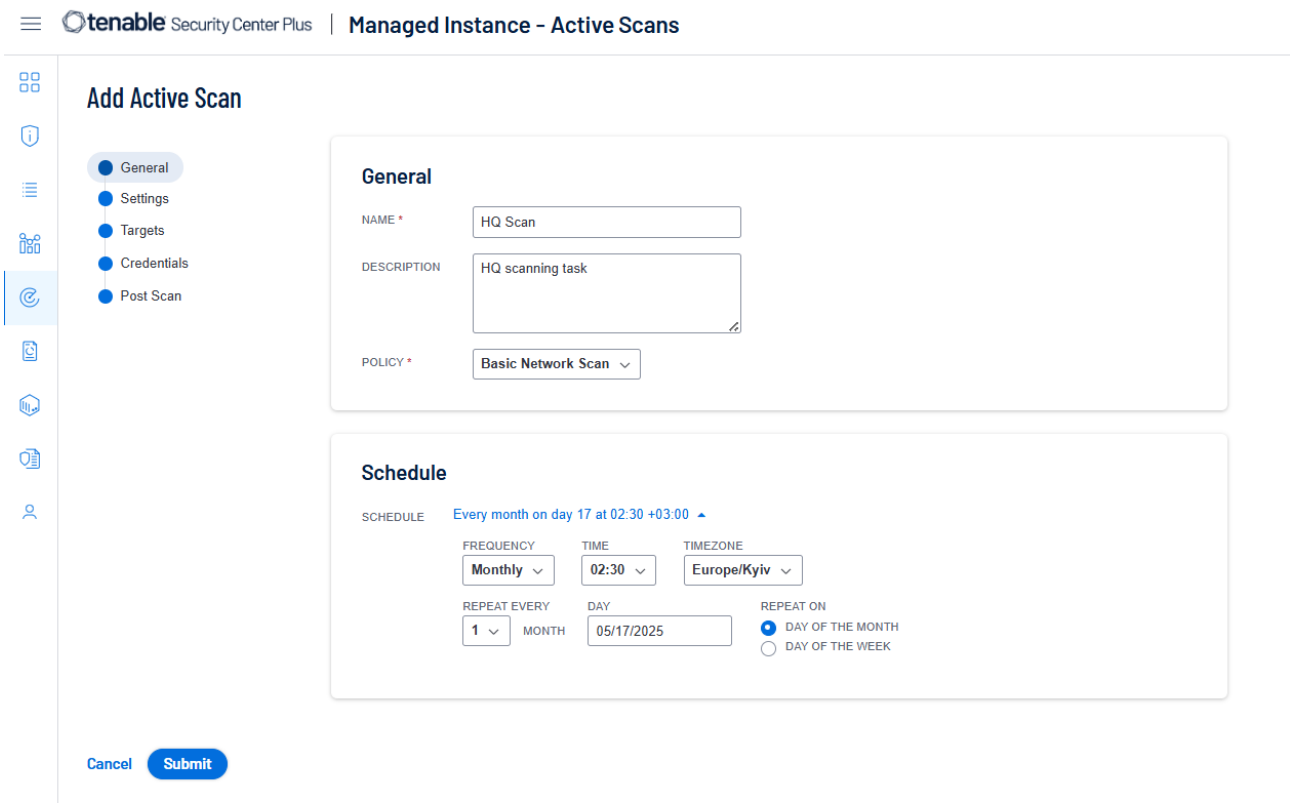


Рис. 3.2. Налаштування вкладки General сканування

4) Цільові активи. На вкладці Targets вибрати тип цілей сканування (Target Type). Tenable.sc дозволяє вказати конкретні IP-адреси або доменні імена, або ж вибрати заздалегідь створені групи активів зі списку. Додати один або кілька діапазонів IP / DNS, або вибрати потрібні Asset Lists, щоб визначити охоплення сканування.

5) Збереження і запуск. Після налаштування всіх параметрів натиснути Submit для збереження сканування. Новий Active Scan з’явиться у списку доступних завдань. Його можна запускати вручну одразу або чекати автоматичного запуску за розкладом.

Вплив на зрілість процесу. Налаштування регулярних повних сканувань усіх важливих активів організації є ключовою умовою переходу від хаотичного до керованого процесу виявлення вразливостей. Організація, яка забезпечила автоматизоване регулярне сканування із заданою періодичністю, демонструє «визначений» рівень зрілості за напрямком Identify у моделі SANS.

3.1.3 Створення та налаштування груп активів.

Останній компонент етапу Prepare – забезпечення контексту для сканування, тобто розуміння того, що саме ми захищаємо. SANS визначає підчас Prepare також напрям Context, що включає інвентаризацію та класифікацію активів. Формування повного переліку IT-активів організації та розбиття його на логічні групи (за підрозділами, критичністю, типом систем тощо) є дуже важливим. Зріла програма управління вразливостями спирається на постійне виявлення та ведення обліку активів – це фундамент, на якому будується решта процесів.

Функціонал Tenable Security Center. Tenable.sc надає гнучкий механізм керування переліком активів через Asset Lists (списки активів). Assets в Tenable.sc – це по суті групи пристроїв, що відповідають заданим критеріям [46]. Після створення такі групи активно використовуються при конфігурації сканування: замість того щоб кожного разу вводити сотні адрес, інженер просто вибирає відповідний Asset List.

Покрокова інструкція. Створення групи активів (Asset List) у Tenable.sc відбувається наступним чином.

1) Доступ до розділу активів. У консолі Tenable Security Center перейти до Assets > Assets. Відкриється сторінка зі списком раніше створених груп активів [47].

2) Додавання нового списку. Натиснути Add. Відобразиться сторінка вибору шаблону активу (рис. 3.3). Можна обрати один з попередньо визначених Tenable шаблонів у категорії Common. Такі шаблони оновлюються автоматично і спрощують створення типових груп. Якщо ж потрібна користувацька група, в секції Other обрати тип: Static, Dynamic, Combination тощо.

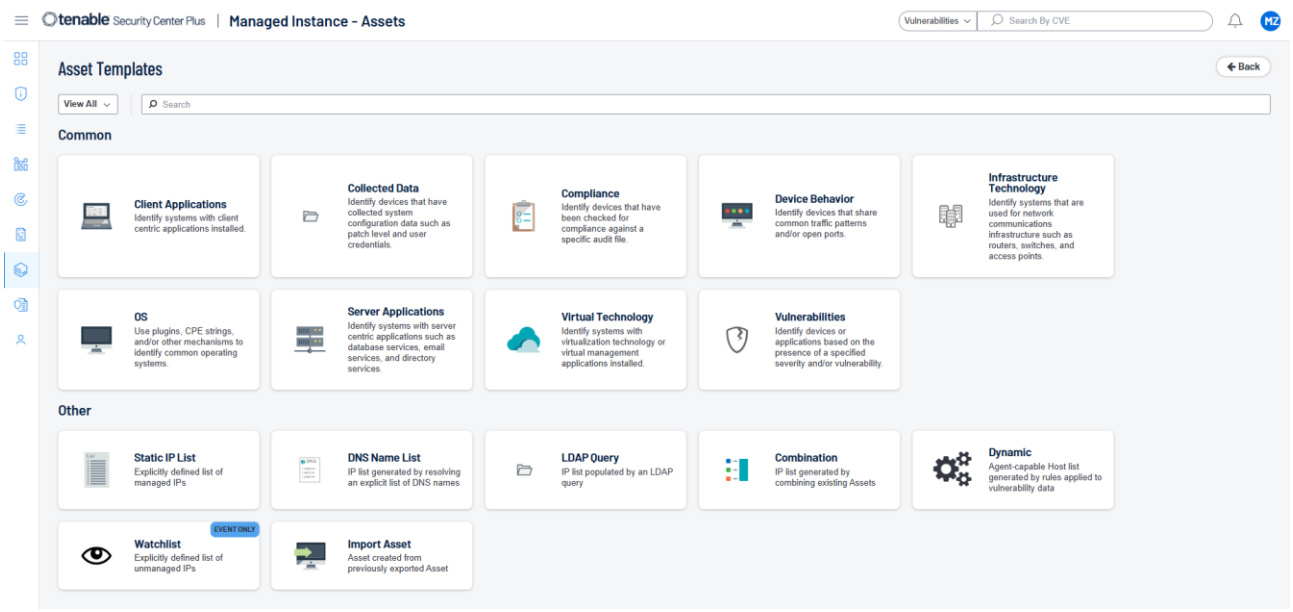


Рис. 3.3. Вибір шаблону групи активів

3) Налаштування групи. Після вибору типу відобразиться форма конфігурації. Задати Name (назву групи) та Description (опціонально, для зручності розуміння призначення). Далі залежно від типу вказати інші параметри.

4) Збереження активу. Після задання потрібних критеріїв натиснути Submit. Створена група з’явиться у списку Assets. За потреби її можна редагувати чи доповнювати. Після наступного сканування Tenable.sc автоматично віднесе знайдені хости до відповідних динамічних груп згідно з їх характеристиками.

Вплив на зрілість процесу. Ведення структурованого інвентаря активів безпосередньо підсилює контекстну обізнаність при управлінні вразливостями. Поділ систем на групи за критичністю та функціями дозволяє фокусувати зусилля на найбільш важливих ресурсах [48] і відстежувати прогрес усунення вразливостей у розрізі цих груп. За рекомендаціями Tenable, безперервне виявлення, оцінка і управління активами є базисом зрілої програми VM. Таким чином, впровадження практики керування групами активів підвищує зрілість процесу до рівня, коли Identify та подальші етапи виконуються з урахуванням повного контексту бізнес-активів.

3.2 Identify (Виявлення)

Етап Identify моделі SANS VMMM присвячений безпосередньому виявленню вразливостей у середовищі організації. Основне питання, на яке відповідає цей етап: «Які вразливості існують в наших системах і як ми їх шукаємо?». Згідно з підходом SANS, ідентифікація включає три напрямки: автоматизоване сканування, ручні перевірки та зовнішні джерела. Tenable Security Center забезпечує реалізацію автоматизованого компонента – регулярні сканування мережі з використанням налаштувань, підготовлених на попередньому етапі.

Функціонал Tenable Security Center. Після того як сканування налаштовано, його необхідно запустити і при необхідності контролювати. У Tenable.sc керування скануваннями відбувається через розділ Active Scans – тут відображаються всі створені завдання з їх статусами. Адміністратор може запускати сканування негайно, ставити їх на паузу або зупиняти, якщо потрібно, та переглядати результати. Завершені сканування автоматично зберігають результати у розділі Scan Results, де їх можна переглянути, відфільтрувати та експортувати.

Покрокова інструкція. Для запуску та моніторингу сканувань у Tenable.sc виконайте дії нижче.

1) Запуск сканування. Відкрийте список активних сканувань (Scans > Active Scans). Встановіть прапорець біля потрібного завдання сканування та натисніть Launch. Вибране сканування відразу перейде в стан Running і розпочнеться його виконання [49]. Якщо для сканування був налаштований розклад, його можна також дочекатися – Tenable.sc запустить його автоматично у вказаний час.

2) Пауза/відновлення (опціонально). Під час виконання сканування система відображає його прогрес. При необхідності (наприклад, якщо сканування спричиняє надмірне навантаження на мережу чи потрібно тимчасово призупинити перевірку) можна поставити його на паузу: для цього

також відмітити завдання і натиснути Pause. Сканер призупинить роботу, а пізніше його можна відновити повторним натисненням Launch (продовжити).

3) Перегляд результатів. Після завершення сканування його статус зміниться на Completed. Щоб переглянути підсумки, перейдіть до Scans > Scan Results (рис. 3.4). На цій сторінці відображається список усіх сесій сканувань із позначенням часу, статусу (успішно чи з помилками), кількості знайдених вразливостей тощо [50].

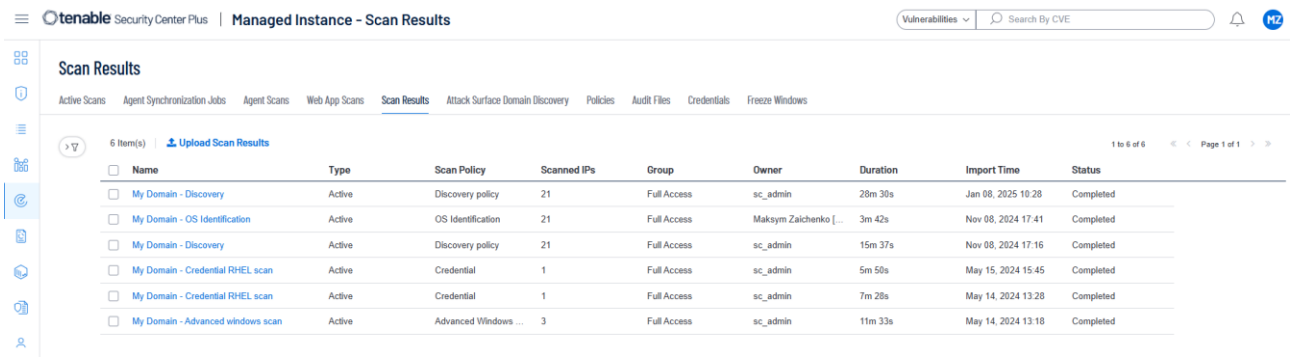


Рис. 3.4. Сторінка Scan Results

Вплив на зрілість процесу. Послідовне виконання сканувань і оперативне отримання їх результатів – головна мета етапу Identify. Організація, яка налагодила регулярне автоматизоване сканування з мінімальними перервами і повним охопленням, знаходиться на високому рівні зрілості цього етапу. Таким чином, реалізація етапу Identify через Tenable Security Center (з використанням підготовлених політик, розкладів та груп активів) дозволяє організації поступово перейти до проактивного та керованого процесу управління вразливостями.

3.3 Analyze (Аналіз)

3.3.1 Перегляд результатів сканування.

На етапі Analyze організація опрацьовує дані, отримані зі сканування, щоб визначити пріоритети виправлення вразливостей. За моделлю SANS VMMM фаза Analyze покликана «категоризувати та пріоритизувати виявлені вразливості». Це критично для переходу від простого виявлення проблем до

розуміння їхнього ризику. Належний аналіз забезпечує фокусування ресурсів на найбільш небезпечних уразливостях, що підвищує ефективність програми управління вразливостями.

Функціонал Tenable Security Center. Платформа Tenable.sc надає зручні засоби перегляду та фільтрації результатів сканування. Кожен результат містить загальні відомості (назва, час початку/завершення, кількість просканованих хостів тощо) і дозволяє переглянути знайдені вразливості [51].

Покрокова інструкція. Для перегляду результатів сканування в Tenable.sc необхідно виконати дії нижче.

1) Відкриття списку сканувань. Перейдіть до меню Scans > Scan Results. На сторінці відобразиться таблиця з виконаними скануваннями.

2) Вибір потрібного сканування. Знайдіть у списку рядок із цікавим вам скануванням (за назвою або датою). Клацніть правою кнопкою миші по цьому рядку (або встановіть прапорець поруч).

3) Відкриття деталей. У контекстному меню натисніть View – відкриється сторінка деталізації результату сканування. На ній доступні вкладки з інформацією про сканування та перелік виявлених уразливостей.

4) Перегляд вразливостей. Переключіться на розділ зі списком виявлених уразливостей (звичайно під таблицею або у вкладці). Ви побачите кожну уразливість, знайдену сканером на вибраних хостах, із зазначенням її критичності, кількості хостів, ідентифікатора CVE тощо.

5) Фільтрація (за потреби). За допомогою панелі фільтрів можна відсіяти результати за певними критеріями (рис. 3.5).

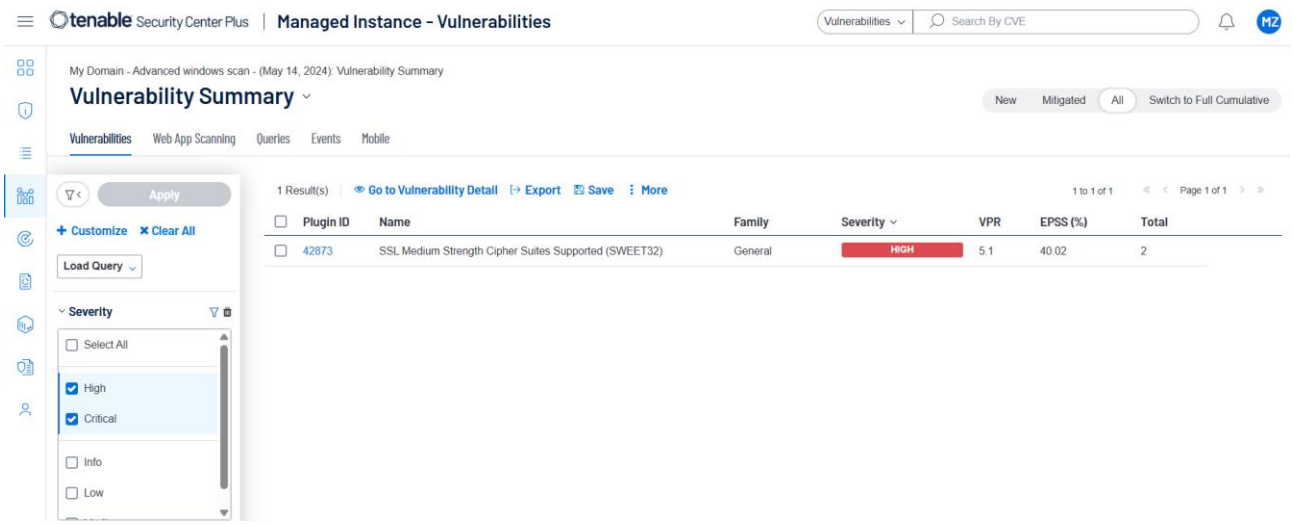


Рис. 3.5. Фільтрація результатів сканувань за критеріями

Вплив на зрілість процесу. Систематичний перегляд та документування результатів сканування є ознакою керованого підходу (рівень Managed або вище за SANS VMMM). Запровадження регламентованого перегляду (наприклад, після кожного сканування результати розглядаються відповідальними особами) підвищує прозорість та контроль. Це створює базу для подальшого глибокого аналізу: команда знає, де знайти потрібні дані, і впевнена, що жодна знайдена уразливість не залишиться без уваги. Таким чином, організація переходить від початкового рівня зрілості (reactive) до керованого процесу, закладаючи основу для більш зрілого аналізу та пріоритизації вразливостей.

3.3.2 Аналіз вразливостей за VPR, критичністю та експлуатованістю.

Окрім простого перелічення уразливостей, зріла програма вимагає оцінки кожної знахідки за ступенем ризику. Модель SANS наголошує, що необхідно враховувати контекстні фактори: не лише CVSS-бали, але й наявність експлойтів, критичність активів, першопричини проблем тощо. Такий підхід (який відповідає підфазі Prioritization в моделі VMMM) дозволяє обрати з «багатьох тисяч проблем ті, з яких слід почати в першу чергу».

Функціонал Tenable Security Center. Платформа пропонує декілька метричних показників та інструментів для оцінки ризику вразливостей [52-53].

- CVSS Severity (Критичність за CVSS): Класичний показник, що відображає базову оцінку небезпеки уразливості (версія CVSSv2 або CVSSv3). Tenable.sc позначає вразливості рівнями Low/Medium/High/Critical відповідно до діапазону CVSS.
- VPR (Vulnerability Priority Rating). Динамічний рейтинг пріоритету від Tenable, що оновлюється щоденно з урахуванням актуальної обстановки загроз. VPR також вимірюється по шкалі 0.1–10 і поділяється на категорії Low/Medium/High/Critical. На відміну від статичного CVSS, VPR враховує ймовірність експлуатації вразливості, тенденції появи експлойтів, активність уразливості у злочинному середовищі тощо.
- Дані про експлойти та експлуатованість. Tenable.sc відображає для кожної вразливості інформацію про наявні відомі експлойти, коди експлойтів або факти використання вразливості в атаках. Також інтегровано метрику EPSS.

Покрокова інструкція. Аналіз та пріоритизація в Tenable.sc здійснюється за наступними кроками.

1) Відкриття сторінки аналізу. У Tenable.sc перейдіть до Analysis > Vulnerabilities. За замовчуванням відкриється узагальнений список уразливостей з базовими стовпцями.

2) Вибір представлення даних. У верхній частині сторінки є випадаючий список «Analysis Tools». Виберіть, наприклад, Vulnerability Detail List для детального перегляду або Vulnerability Summary для згрупованого перегляду за плагінами. Примітка: У Detail List доступні всі метрики (CVSS, VPR, експлойти і т.д.) поруч з кожною уразливістю.

3) Застосування фільтрів. Розгорніть панель Filters. Додайте умови фільтрації, що відповідають вашим пріоритетам.

4) Аналіз списку. Після застосування фільтрів таблиця оновиться. Розгляньте отриманий список вразливостей. Для кожного запису зверніть увагу

на колонки CVSS Score, VPR, Exploit Info та кількість залучених хостів. Це дасть розуміння, наскільки небезпечна уразливість і наскільки широко вона розповсюджена в мережі.

5) Детальний огляд вибраної вразливості (за потреби). Ви можете клацнути на назву уразливості (або plugin ID) для переходу на сторінку деталей конкретної уразливості на конкретному хості (рис. 3.6). Там буде приведено опис, рекомендації з усунення (Solution), метрики ризику та ключові драйвери VPR.

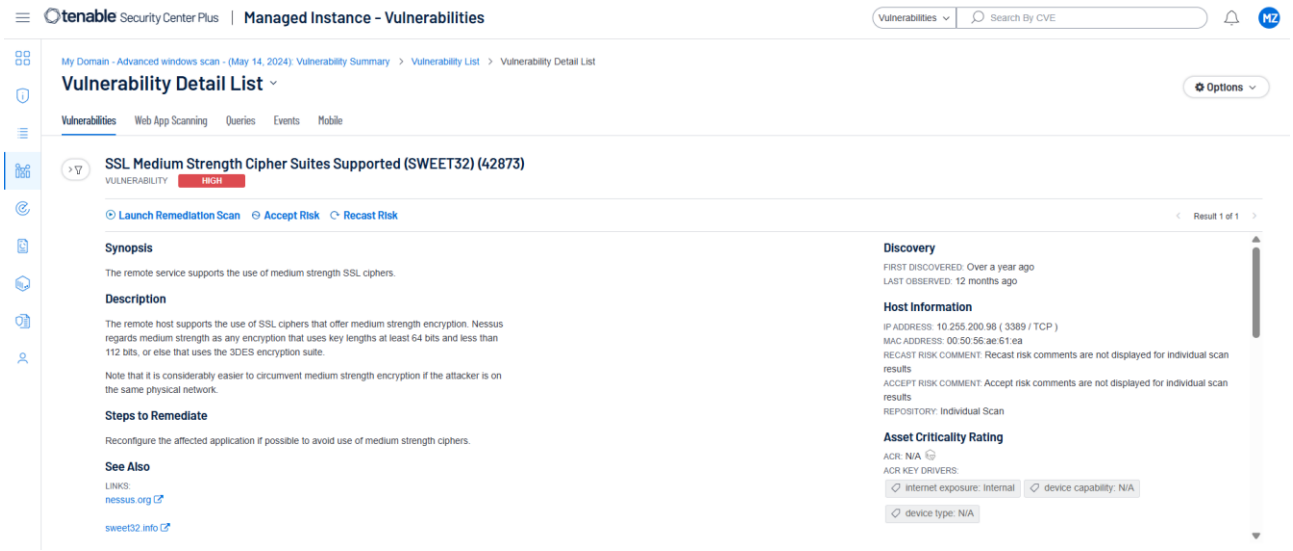


Рис. 3.6. Детальний огляд вибраної вразливості

Вплив на зрілість процесу. Згідно SANS VMMM, вже на рівні 2 (Managed) впроваджується врахування доступності експлойтів при пріоритизації. У нашому випадку – Tenable.sc надає ці дані «з коробки», тож підключення метрик експлуатованості до робочого процесу забезпечує вищий рівень зрілості. Далі, інтеграція бізнес-контексту (критичності активів, розташування) відповідає рівню 3 (Defined) і вище. Таким чином, систематичний аналіз за VPR та експлуатованістю свідчить, що програма переходить від реагування на “всі критичні однаково” до ризик-орієнтованого підходу. Це покращує показники середнього часу до виправлення найбільш небезпечних уразливостей і знижує загальний ризик для організації.

3.4 Communicate (Комунікація)

3.4.1 Створення звітності.

Виявити та проаналізувати вразливості недостатньо – необхідно донести цю інформацію до зацікавлених сторін у зручному форматі. Етап Communicate у SANS VMMM підкреслює важливість метрик та звітності і оповіщень. Регулярна звітність забезпечує прозорість: керівництво, технічні команди, замовники повинні розуміти стан безпеки. Отже, створення звітів – ключовий компонент комунікації, який перетворює «сирі дані» сканування на інформацію для прийняття рішень.

Функціонал Tenable Security Center. Платформа має потужний модуль Reporting, який дозволяє генерувати кастомізовані звіти про вразливості у різних форматах (HTML, PDF, CSV тощо). Звіти можуть бути як шаблонними (вбудовані шаблони для типових випадків), так і повністю налаштованими під потреби організації. Звіт у Tenable.sc – це документ, що може складатися з декількох розділів (chapters), містити таблиці, графіки, діаграми, текстові пояснення [54-55].

Покрокова інструкція: Створення звіту в Tenable.sc здійснюється наступним чином.

1) Відкриття модуля звітів. У лівому меню інтерфейсу Tenable.sc перейдіть до Reporting > Reports. Відкриється сторінка управління звітами, де відображаються вже наявні визначення звітів (Report Definitions).

2) Створення нового звіту. Натисніть кнопку Add у верхній частині сторінки. Відкриється сторінка вибору шаблону звіту (Report Template).

3) Вибір типу або шаблону. Tenable.sc запропонує вибрати тип звіту. Існують шаблони (наприклад, “Executive Summary”, “Compliance Report” тощо) – вони згруповані за категоріями у вигляді плиток. Ви можете:

a. обрати один з Tenable-provided templates у розділі Common чи інших категоріях. Після вибору шаблону система автоматично налаштує структуру звіту;

b. або обрати порожній шаблон (розділ Custom), щоб самому зібрати звіт з нуля.

4) Налаштування параметрів звіту. Після вибору шаблону відкриється форма налаштування. Вкажіть назву звіту та опис (за потреби). Також визначте, які дані має охоплювати звіт: у полі Targets можна вибрати конкретні репозиторії, діапазони IP чи групи активів, про які генеруватиметься звіт. Це зручно, якщо, наприклад, ви робите окремий звіт для різних підрозділів.

5) Конфігурація змісту звіту (рис. 3.7). Залежно від вибраного шаблону, Tenable.sc може автоматично додати типові розділи (наприклад, короткий огляд, детальний список уразливостей, графіки). Якщо ви створюєте користувацький звіт, потрібно додати розділи вручну. Для цього після створення структури звіту використовуйте опцію Edit report outline або додавання розділів.

a. Add Chapter – додати розділ (наприклад, таблицю вразливостей, графік розподілу за CVSS тощо). Tenable.sc дозволяє додавати як шаблонні розділи (визначені компоненти), так і вручну створені (де ви самі вибираєте колонки, критерії).

b. Add Element – налаштувати елемент всередині розділу, наприклад, матрицю, діаграму або таблицю з конкретним запитом фільтрації.

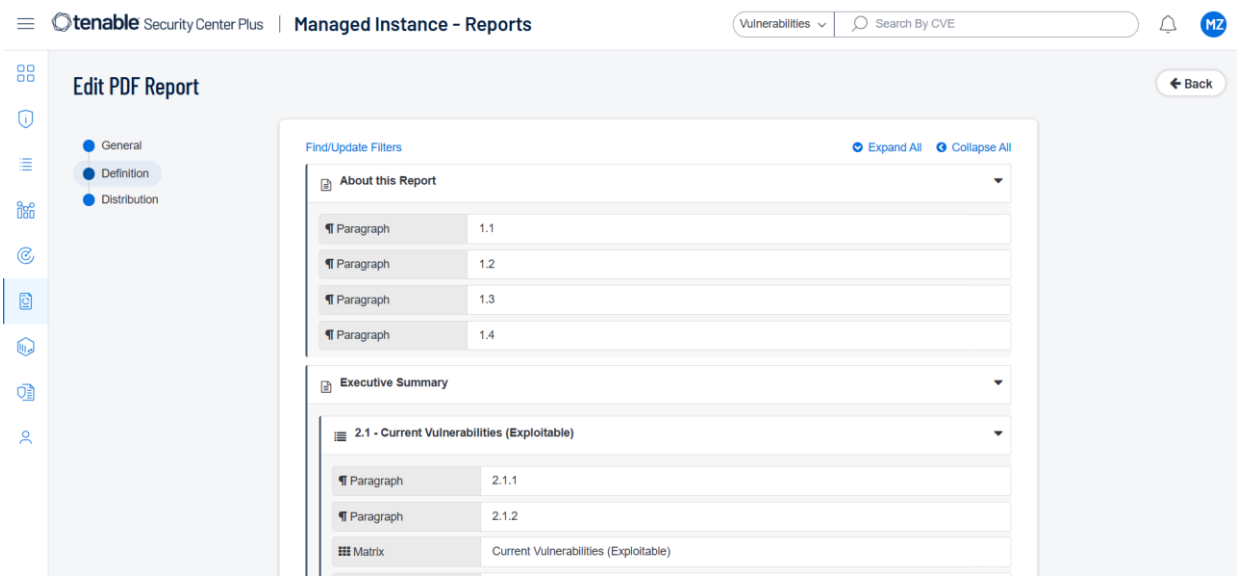


Рис. 3.7. Конфігурація розділів звіту

6) Збереження та генерація звіту. Після налаштування всіх розділів натисніть Submit для збереження визначення звіту. Створений звіт з’явиться у списку визначень. Для його виконання (генерації документа) – виберіть звіт у таблиці та натисніть Launch (запустити звіт) або встановіть розклад (Schedule) для автоматичної генерації за розкладом.

7) Перегляд та експорт. Після запуску звіту готовий результат можна переглянути через інтерфейс (вбудований перегляд PDF/HTML) або завантажити файл. Звіти зберігаються, історію їх виконань можна також переглядати в розділі Report Results.

Вплив на зрілість процесу. Наявність формалізованої звітності – ознака зрілого процесу. На початковому етапі (рівень Initial за VMMM) інформація про уразливості може доноситись хаотично (через неформальні канали, без сталій періодичності). Впровадження регулярних звітів (тижневих, місячних) із чітко визначеними метриками переводить процес на рівень Defined: встановлено стандарти, що і кому доповідається. Наприклад, SANS рекомендує відстежувати кількість критичних уразливостей, середній час виправлення, покриття сканування тощо як ключові метрики програми. Отже, створення звітності підвищує прозорість і підзвітність процесу, що характерно для вищих рівнів зрілості (Quantitatively Managed) – коли рішення приймаються на основі чітко виміряних показників.

3.4.2 Створення дашбордів.

Окрім періодичної звітності, зрілі програми впроваджують інтерактивні дашборди (інформаційні панелі) для моніторингу ключових показників в режимі реального часу. Дашборди – це частина комунікації, що забезпечує Alerting/Monitoring: різні користувачі (CISO, менеджери, інженери) можуть щоденно відстежувати стан безпеки без необхідності генерувати звіт. SANS VMMM відносить оперативне інформування та оповіщення до фокусу Communicate, оскільки це дає можливість своєчасно реагувати на зміни (наприклад, появу нових критичних уразливостей). Різні ролі мають різні

потреби: керівництво цікавлять узагальнені ризики й тренди, технічний персонал – конкретні деталі по їх зонах відповідальності.

Функціонал Tenable Security Center. Платформа має розділ Dashboard, де користувачі можуть додавати та налаштовувати будь-яку кількість дашбордів [56-57]. Tenable надає бібліотеку готових шаблонів дашбордів на різні тематики – від оглядових панелей ризику до специфічних (наприклад, «Endpoint Vulnerabilities», «Patch Compliance» тощо). Кожен дашборд складається з компонентів – графіків, таблиць, матриць – які відображають дані з певного запиту чи метрики. Дашборди легко кастомізувати: можна створювати власні компоненти, визначати їх оформлення, налаштовувати фільтри.

Покрокова інструкція. Створення дашборду в Tenable.sc відбувається наступним чином:

1) Відкриття розділу дашбордів. З головного меню перейдіть до Dashboard > Dashboard. Відкриється сторінка, на якій відображається поточний дашборд та опції перемикання дашбордів.

2) Додавання нового дашборду. У правому верхньому куті клацніть меню Options і виберіть Add Dashboard. Система запропонує або вибрати шаблон, або створити порожній дашборд.

3) Вибір шаблону або порожнього дашборду (рис. 3.8). Якщо ви хочете скористатися готовим шаблоном Tenable, на сторінці Dashboard Templates оберіть категорію (наприклад, Executive, Compliance, Operations) і конкретний шаблон дашборду зі списку доступних. Для повного контролю можна обрати створення порожнього дашборду (Custom Dashboard).

4) Налаштування дашборду. Після створення дашборду (шаблонного чи порожнього) ви можете змінити його назву та опис відповідно до ролі. Для цього використовуйте пункт Edit (наприклад, перейменуйте дашборд на "Вразливості – Огляд для CISO").

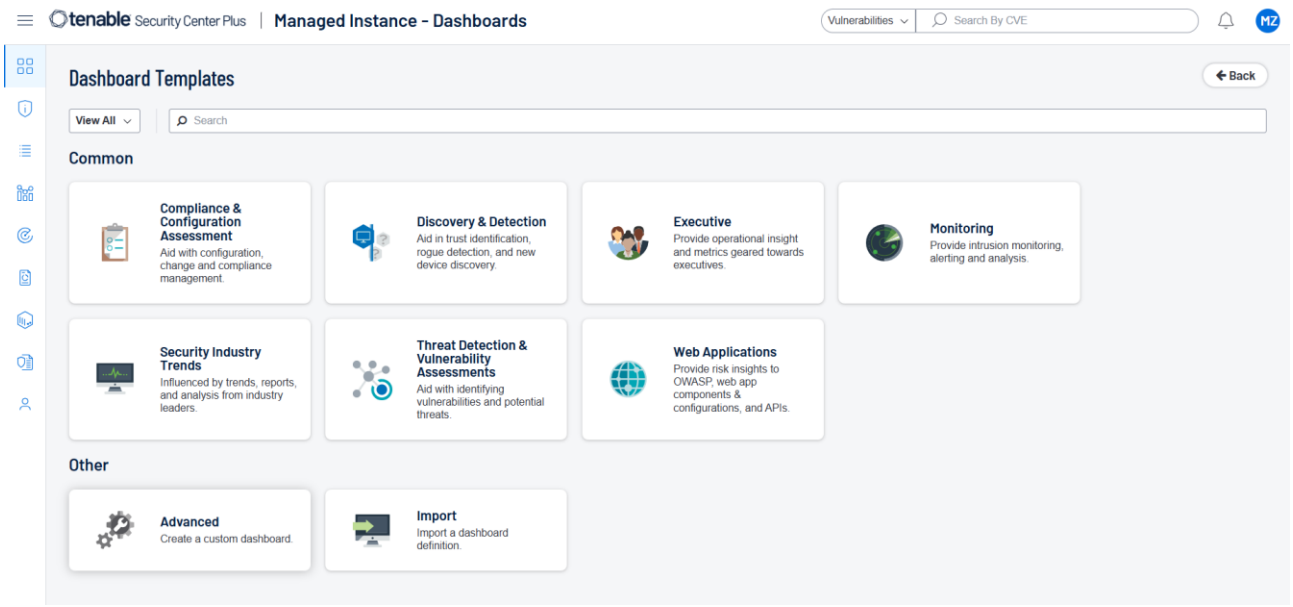


Рис. 3.8. Вибір шаблону дашборду

5) Додавання компонентів. Головна цінність – додати до дашборду компоненти з даними [58]. Якщо ви обрали готовий шаблон, певні компоненти вже будуть присутні. Їх можна редагувати або додавати нові. Для додавання натисніть Options > Add Component. Відкриється бібліотека компонентів:

a. Можна вибрати тип компонента – таблиця, стовпчиковий графік, колова діаграма тощо.

b. Оберіть потрібний тип і налаштуйте його: задайте назву, критерії фільтрації даних, що відображатимуться, метрики. Наприклад, компонент типу matrix може відображати перехресну таблицю «Відділи vs Кількість критичних уразливостей».

c. Якщо використовуєте шаблон, багато компонентів вже налаштовано – ви можете лише підправити фільтри (наприклад, щоб дашборд відображав дані лише по певній групі активів, якщо це панель для конкретного підрозділу).

6) Збереження дашборду та перемикання. Після додавання всіх необхідних компонентів збережіть дашборд. Ви можете створити декілька різних дашбордів для різних цілей/ролей. Перемикатися між ними можна через випадаючий список Switch Dashboard у верхньому куті сторінки дашбордів.

Вплив на зрілість процесу. Налаштування різнорівневих дашбордів демонструє, що процес комунікації знаходиться на високому рівні. Організація не лише збирає дані, але й оперативно відстежує ключові показники. Це дозволяє своєчасно виявляти відхилення (наприклад, раптове зростання кількості критичних уразливостей) і реагувати до того, як проблема стане критичною. Таким чином, комунікація стає проактивною: інформація завжди під рукою, а не лише у вигляді статичних звітів раз на місяць. Це відповідає переходу від рівня Defined до Quantitatively Managed, коли процес оцінюється і покращується на основі постійного моніторингу метрик.

3.4.3 Створення завдань та сповіщень.

Ефективна комунікація – це не лише планові звіти, але й оперативні сповіщення та інтеграція з процесом роботи команди. Якщо виявлено критичну вразливість, яка потребує негайної уваги, система повинна автоматично повідомити відповідальних. Так само, потрібен механізм відстеження виконання виправлень – постановки завдань та контролю статусу. На рівні Communicate модель SANS передбачає підфокус Alerting: своєчасні попередження про інциденти чи значні вразливості, щоб ніщо не «прослизнуло» повз увагу.

Функціонал Tenable Security Center. У платформі реалізовано вбудований workflow для управління знайденими вразливостями [59]. Основні можливості наведені нижче.

- Alerts (Сповіщення): налаштування правил, які автоматично виконують певні дії при заданих умовах. Tenable.sc може надсилати email-повідомлення, показувати повідомлення в інтерфейсі, створювати завдання повторно запускати сканування чи звіти або генерувати syslog повідомлення при спрацьовуванні сповіщення.
- Tickets (Завдання): система дозволяє призначати вразливості до виконання, створюючи записи задач. Наприклад, аналітик може прямо зі списку

уразливостей відкрити Ticket і призначити його конкретній особі або групі. Таким чином, ведеться облік – які вразливості взяті в роботу, ким і коли.

Покрокова інструкція. Налаштування Alert для автоматичного сповіщення здійснюється наступним чином:

1) Перейдіть у меню Workflow > Alerts (може бути у розділі Workflow або окремо) – відкриється сторінка списку правил сповіщень.

2) Натисніть Add Alert. Система запропонує задати умови спрацювання. Виберіть тип події: наприклад, Vulnerability (виявлення вразливості). Задайте фільтр умови: наприклад, Severity = Critical. Налаштуйте частоту: разово при кожному скані, або раз на день.

3) Виберіть Alert Actions – що робити при спрацюванні (рис. 3.9).

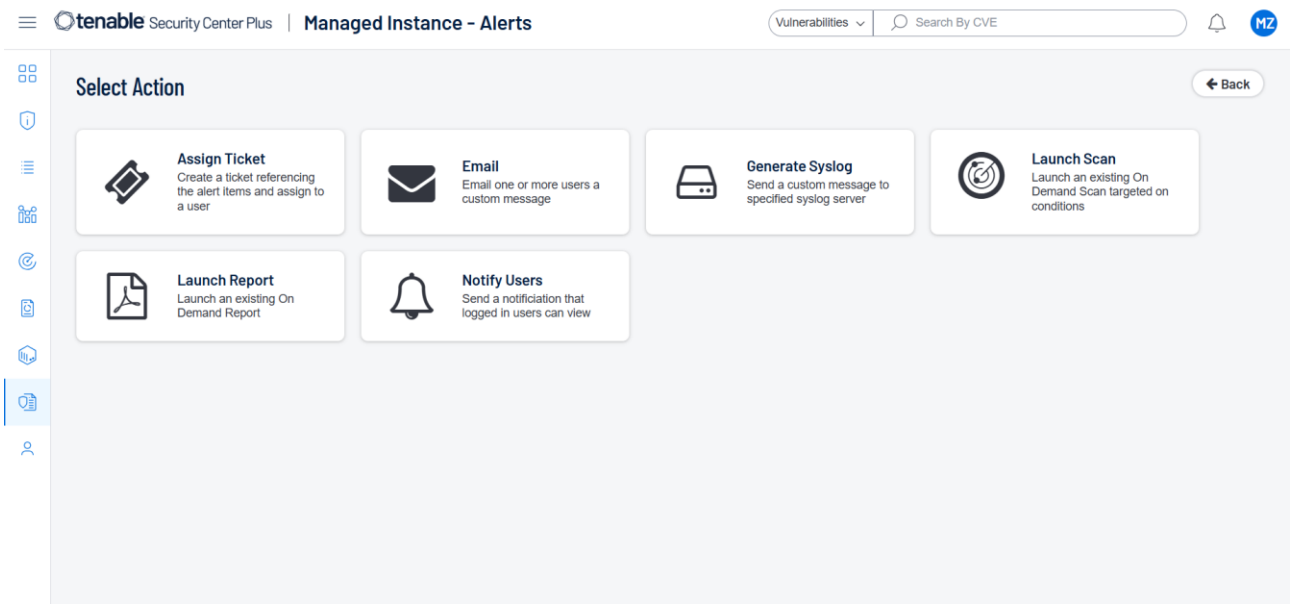


Рис. 3.9 – Перелік дій, що виконує alert

4) Збережіть правило Alert. У результаті, при настанні умови (наприклад, нове сканування виявило критичну уразливість), Tenable.sc автоматично надішле сповіщення. Наприклад, адміністратор отримає email із деталями вразливості.

Створення та використання Tickets (завдань) реалізовується наступним чином.

1) Відкрийте сторінку аналізу Analysis > Vulnerabilities і знайдіть уразливість, яку треба призначити на виправлення.

2) Правим кліком по рядку уразливості виберіть Open Ticket (Відкрити завдання). Відкриється форма створення завдання.

3) Заповніть поля завдання: назва (за замовчуванням буде щось на кшталт “Vuln [ID] on [Host]”), опис (можна вказати що треба зробити, наприклад, “Оновити бібліотеку OpenSSL до останньої версії”), призначте відповідального користувача або групу.

4) Задайте пріоритет і дедлайн, якщо потрібно. Це допоможе відслідкувати прострочені завдання.

5) Збережіть завдання. Тепер ця уразливість відображатиметься як призначена. Відповідальний отримує повідомлення (через email або в системі – за налаштуваннями), і в розділі Workflow > Tickets він побачить цей запис.

6) Закрийте завдання. Після того, як уразливість буде виправлено і підтверджено (наприклад, повторне сканування не знаходить її), завдання можна закрити.

Вплив на зрілість процесу. Впровадження workflow-компонентів переводить управління вразливостями на рівень операційного процесу. Це ознака переходу від просто Defined до Quantitatively Managed/Optimizing. Автоматичні оповіщення гарантують, що критична інформація не загубиться – тобто, знижується залежність від людського фактору, підвищується своєчасність реагування. Використовуючи вбудований Workflow Tenable.sc або інтегруючи його з зовнішніми системами, організація досягає високого рівня зрілості, коли виправлення вразливостей стає частиною рутинних операцій. На рівні Optimizing керівництво може аналізувати ефективність цього процесу і вносити покращення. Отже, завдяки сповіщенням і завданням процес управління вразливостями набуває керованості, вимірюваності та здатності до постійного покращення.

3.5 Treat (Усунення)

Етап Treat – це завершальний і найважливіший етап – фактичне виправлення знайдених вразливостей. Стадія Treat у моделі SANS фокусується на застосуванні змін: патчів, конфігураційних виправлень, або інших заходів для усунення ризиків. Від якості виконання цього етапу залежить реальне зниження ризику. Важливо також визначити оптимальні методи усунення: часто один патч може закрити одразу багато уразливостей, тому пріоритизація рішень (а не лише самих уразливостей) підвищує ефективність.

Функціонал Tenable Security Center. Платформа допомагає не тільки знайти вразливості, але й підказує, як саме їх виправити [60]. Можна виокремити наступні основні можливості.

- У деталях кожної вразливості є секція Solution, де надається рекомендація від Tenable щодо усунення. Зазвичай це опис патчу чи необхідної зміни конфігурації. Ця інформація береться з плагіна сканера і часто містить посилання на відповідні патчі чи статті виробника.
- Remediation Summary (Solutions) – спеціальний інструмент аналізу в Tenable.sc, який агрегує виявлені уразливості за рішеннями. Згідно з документацією, Remediation Summary «надає список дій з усунення, які можна виконати, щоб максимально знизити кількість вразливостей». Метрики в Remediation Summary включають: кількість хостів, яких торкнеться дія; кількість вразливостей, що вона виправить; відсоток зниження сумарного балу ризику в мережі тощо. Це дає можливість порівняти, які патчі найбільш «вигідні» з точки зору зниження ризику.

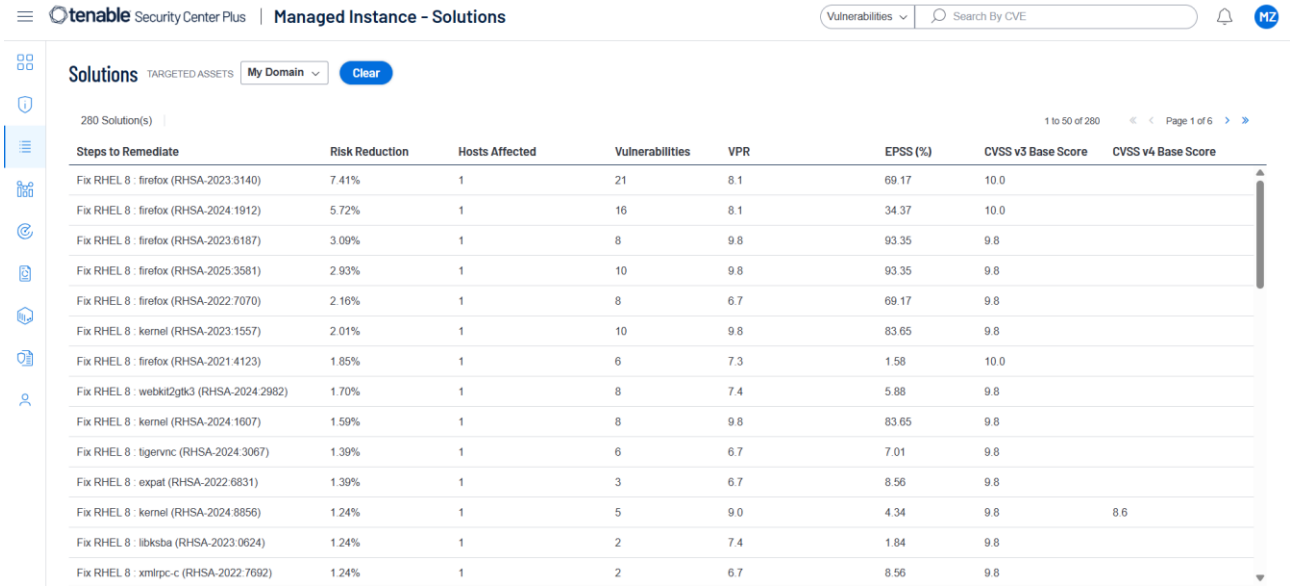
Покрокова інструкція. Використання Remediation Summary в Tenable.sc здійснюється наступним чином.

1) Формування вибірки. Перейдіть до Analysis > Vulnerabilities. Щоб скористатися інструментом Remediation Summary, спочатку бажано звузити вибірку уразливостей до тих, які ви плануєте розглядати (наприклад, всі

відкриті уразливості на поточний момент або за певним сегментом мережі). Встановіть необхідні фільтри (можна залишити “всі”).

2) Вибір інструменту Remediation Summary. У випадаючому меню Analysis Tool виберіть опцію Remediation Summary (іноді вона доступна після вибору певного виду таблиці). Після цього Tenable.sc покаже окремий перегляд – список рекомендацій (рішень).

3) Аналіз списку рішень. Ви побачите таблицю, де кожен рядок – це конкретне рішення/патч (рис. 3.10).



Steps to Remediate	Risk Reduction	Hosts Affected	Vulnerabilities	VPR	EPSS (%)	CVSS v3 Base Score	CVSS v4 Base Score
Fix RHEL 8 : firefox (RHSA-2023:3140)	7.41%	1	21	8.1	69.17	10.0	
Fix RHEL 8 : firefox (RHSA-2024:1912)	5.72%	1	16	8.1	34.37	10.0	
Fix RHEL 8 : firefox (RHSA-2023:6187)	3.09%	1	8	9.8	93.35	9.8	
Fix RHEL 8 : firefox (RHSA-2025:3581)	2.93%	1	10	9.8	93.35	9.8	
Fix RHEL 8 : firefox (RHSA-2022:7070)	2.16%	1	8	6.7	69.17	9.8	
Fix RHEL 8 : kernel (RHSA-2023:1557)	2.01%	1	10	9.8	83.65	9.8	
Fix RHEL 8 : firefox (RHSA-2021:4123)	1.85%	1	6	7.3	1.58	10.0	
Fix RHEL 8 : webkit2gtk3 (RHSA-2024:2982)	1.70%	1	8	7.4	5.88	9.8	
Fix RHEL 8 : kernel (RHSA-2024:1607)	1.59%	1	8	9.8	83.65	9.8	
Fix RHEL 8 : tigervnc (RHSA-2024:3067)	1.39%	1	6	6.7	7.01	9.8	
Fix RHEL 8 : expat (RHSA-2022:6831)	1.39%	1	3	6.7	8.56	9.8	
Fix RHEL 8 : kernel (RHSA-2024:8856)	1.24%	1	5	9.0	4.34	9.8	8.6
Fix RHEL 8 : libksba (RHSA-2023:0624)	1.24%	1	2	7.4	1.84	9.8	
Fix RHEL 8 : xmlrpc-c (RHSA-2022:7692)	1.24%	1	2	6.7	8.56	9.8	

Рис. 3.10. Перелік рішень для усунення вразливостей

4) Пріоритизація та планування. На основі цього списку ви можете планувати виправлення. Tenable.sc не автоматизує сам процес установки патчів, але надає інформацію для прийняття рішень. З цього списку варто почати з дій з найвищим Risk Reduction (особливо якщо вони мають відносно малу кількість залучених хостів – тобто легко виконуються).

5) Використання деталей рішення. Якщо клацнути на конкретний рядок (рішення), можна отримати деталі – які саме уразливості включені, на яких хостах. Це корисно для передачі в команду IT: вони отримають перелік систем і відповідний патч для застосування.

Вплив на зрілість процесу. Застосування підходу, орієнтованого на рішення, а не просто на окремі уразливості, відображає високий рівень зрілості

процесу усунення. Організація оптимізує процес виправлення, приділяючи увагу патчам з найбільшим впливом. Tenable.sc надає інформаційну підтримку цьому – що вже значно вище базового рівня зрілості. Отримуючи такі підказки (список “top patches”), команда виправлення може швидше знизити сукупний ризик, витрачаючи менше зусиль – це показник ефективності процесу. Зрештою, ефективне виправлення великої кількості уразливостей з мінімальними простоями і витратами є метрикою зрілості етапу Treat.

Висновки до розділу 3

У межах третього розділу досліджено практичну реалізацію етапів моделі SANS Vulnerability Management Maturity Model (VMMM) засобами платформи Tenable Security Center. Проведений аналіз дозволив продемонструвати, що Tenable SC є комплексним технічним інструментом, здатним забезпечити всі ключові компоненти зрілої програми управління вразливостями.

На етапі Prepare виявлено, що платформа дозволяє створювати стандартизовані політики сканування, ефективно управляти обліковими даними для автентифікованого сканування та будувати динамічні групи активів на основі актуальної інформації з мережі. Це забезпечує системний підхід до підготовки процесу виявлення вразливостей з урахуванням специфіки інфраструктури організації.

Етап Identify реалізується в Tenable SC через запуск активних сканувань з використанням раніше визначених політик та груп активів. Інструмент забезпечує повний цикл управління скануваннями, включно з плануванням, моніторингом виконання та збереженням результатів для подальшого аналізу.

На етапі Analyze платформа надає аналітичні можливості для глибокої оцінки виявлених уразливостей за такими критеріями, як CVSS, VPR, наявність експлойтів і рівень експлуатаційної активності. Завдяки цьому забезпечується ризик-орієнтована пріоритизація, що дозволяє зосередити ресурси на найкритичніших загрозах.

Етап Communicate реалізується через модулі звітності та дашбордів, що дає змогу доносити інформацію про поточний стан безпеки до різних зацікавлених сторін. Додатково реалізовано механізми сповіщення та управління завданнями, що дозволяє інтегрувати процес управління вразливостями в операційну діяльність організації.

Нарешті, етап Treat підтримується через функціонал Remediation Summary для вибору найбільш ефективних дій з усунення вразливостей.

Загалом, Tenable Security Center повністю відповідає вимогам зрілої програми управління вразливостями відповідно до моделі SANS VMMM і дозволяє організаціям забезпечити безперервний, контрольований та вимірюваний процес зниження ризиків. Реалізація всіх етапів у комплексі сприяє досягненню високого рівня процесної зрілості, що є запорукою ефективного кіберзахисту сучасного підприємства.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи досягнуто поставлених завдань – здійснено комплексне дослідження основ, методології та технічних засобів процесу управління вразливостями. Теоретичне та практичне опрацювання тематики дозволило обґрунтувати значущість управління вразливостями як одного з фундаментальних напрямів забезпечення кібербезпеки організацій.

У першому розділі проаналізовано сучасне розуміння поняття «вразливість», її характеристики та класифікації. Досліджено міжнародні підходи до вимірювання критичності вразливостей, зокрема методології CVSS v3.1, а також розглянуто роль системи CVE як глобального реєстру уразливостей. На основі аналізу нормативних документів і моделей, зокрема ISO/IEC 27002:2022, NIST SP 800-40r4 та SANS VMMM, обґрунтовано ключові принципи та етапи ефективного управління вразливостями.

Другий розділ присвячено дослідженню технічних платформ управління вразливостями. Проведено порівняльний аналіз рішень Tenable Security Center, Qualys VMDR та Rapid7 InsightVM. На основі аналітичних оглядів і технічного порівняння визначено, що Tenable Security Center є найбільш повнофункціональною платформою для комплексного впровадження процесу управління вразливостями в організаціях з великою кількістю активів. Платформа забезпечує широкі можливості інтеграції, гнучкість налаштувань і підтримку зрілих процесів управління ризиками.

У третьому розділі запропоновано методику реалізації етапів моделі SANS VMMM із використанням Tenable Security Center. Відповідно до етапів Prepare, Identify, Analyze, Communicate та Treat описано практичні кроки налаштування політик сканування, запуску сканувань, аналізу результатів, формування звітності та організації процесу виправлення вразливостей. Особливу увагу приділено інструментам пріоритизації ризиків (VPR, Exploitability), управлінню робочими процесами.

Таким чином, у роботі підтверджено, що ефективне управління вразливостями потребує поєднання методологічної бази, технологічної підтримки та зрілого процесного підходу. Реалізація всіх компонентів наведеної в роботі методики дозволяє організаціям забезпечити безперервне виявлення, оцінку, пріоритизацію та усунення вразливостей, що є важливим фактором зниження кіберризиків та підвищення стійкості до кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. NIST National Vulnerability Database (NVD). Vulnerabilities – CVE definition. URL: https://nvd.nist.gov/vuln (дата звернення: 12.05.2025).

2. NRI Secure Technologies. How to Build a Proactive Vulnerability Management Strategy. URL: https://www.nri-secure.com/blog/how-to-build-a-proactive-vulnerability-management-strateg (дата звернення: 12.05.2025).

3. Statista. Number of new CVEs per year, 2024. URL: https://www.statista.com/statistics/ (дата звернення: 12.05.2025).

4. Astra Security. 35 Cyber Security Vulnerability Statistics, Facts in 2025. URL: https://www.getastra.com/blog/security-audit/cyber-security-vulnerability-statistics (дата звернення: 12.05.2025).

5. FIRST.org. CVSS v3.1 Metric Groups diagram. URL: https://www.first.org/cvss/v3-1/media/MetricGroups.svg (дата звернення: 12.05.2025).

6. FIRST.org. Understanding CVSS v3.1: A Comprehensive Guide. URL: https://codethem.com/insight/understanding-cvss-v3 (дата звернення: 12.05.2025).

7. SentinelOne. The History of Vulnerability Management: Key Milestones. URL: https://www.sentinelone.com/cybersecurity-101/history-of-vulnerability-management (дата звернення: 12.05.2025).

8. MITRE CVE Program. Mission of the CVE® Program. URL: https://cve.mitre.org (дата звернення: 12.05.2025).

9. Poireault K. DBIR: Vulnerability Exploits Triple as Initial Access Point for Data Breaches. Infosecurity Magazine, 01.05.2024. URL: https://www.infosecurity-magazine.com/news/dbir-vulnerability-exploits-triple/ (дата звернення: 12.05.2025).

10. Verizon. 2023 Data Breach Investigations Report (DBIR). URL: https://www.verizon.com/business/resources/reports/dbir/ (дата звернення: 12.05.2025).

11. Ikeda S. 2025 Verizon DBIR: Cyber Attacks Increasingly Driven by Vulnerability Exploitation. CPO Magazine, 07.2025. URL:

https://www.cpomagazine.com/cyber-security/2025-verizon-dbir-cyber-attacks-vulnerability-exploitation (дата звернення: 12.05.2025).

12. ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls. Київ: ДСТУ ISO/IEC 27002:2022, 2022. Section 8.8 – Management of technical vulnerabilities.

13. Souppaya M., Scarfone K. NIST SP 800-40 Rev.4: Guide to Enterprise Patch Management Planning. Gaithersburg, MD: NIST, 04.2022. URL: https://csrc.nist.gov (дата звернення: 12.05.2025).

14. Center for Internet Security (CIS). CIS Critical Security Control 7 – Continuous Vulnerability Management. URL: https://www.cisecurity.org/controls/continuous-vulnerability-management (дата звернення: 12.05.2025).

15. Cybersecurity & Infrastructure Security Agency (CISA). Known Exploited Vulnerabilities Catalog. URL: https://www.cisa.gov/known-exploited-vulnerabilities-catalog (дата звернення: 12.05.2025).

16. FIRST.org. Exploit Prediction Scoring System (EPSS) – Mission & Model. URL: https://www.first.org/epss/ (дата звернення: 12.05.2025).

17. Tripwire. Steps for Successful Vulnerability Management: Lessons from the Pitch. URL: https://www.tripwire.com/state-of-security/successful-vulnerability-management (дата звернення: 12.05.2025).

18. Palmaers T. Implementing a Vulnerability Management Process: whitepaper. SANS Institute, 04.2013. 17 p. URL: https://www.sans.org (дата звернення: 12.05.2025).

19. Phonsa V. Vulnerability Management Fundamentals: Cyber Exposure Lifecycle. Tenable Blog, 2019. URL: https://www.tenable.com/blog/vulnerability-management-fundamentals-what-you-need-to-know (дата звернення: 12.05.2025).

20. BlueVoyant. Vulnerability Management: Complete Guide to Process and Tools. URL: https://www.bluevoyant.com/knowledge-center/vulnerability-management-complete-guide-to-process-and-tools (дата звернення: 12.05.2025).

21. Aqua Security. Vulnerability Management: Definition, Process, and Tools. 2021. URL: https://www.aquasec.com/cloud-native-academy/vulnerability-management/vulnerability-management/ (дата звернення: 12.05.2025).

22. JetPatch. Comparing Qualys, Tenable, Rapid7 – and the remediation missing link. Блог, 2020. URL: https://jetpatch.com/blog/patch-management/comparing-qualys-tenable-rapid7-and-the-remediation-missing-link/ (дата звернення: 12.05.2025).

23. Cynet. Top 5 Vulnerability Management Tools. 2024. URL: https://www.cynet.com/initial-access-vectors/top-5-vulnerability-management-tools/ (дата звернення: 12.05.2025).

24. Prasad M. 5 Stages of Vulnerability Management Maturity Model. SecPod Blog, 11.03.2022. URL: https://www.secpod.com/blog/vulnerability-management-maturity-model/ (дата звернення: 12.05.2025).

25. Rapid7. The Ultimate Guide to Vulnerability Management. URL: https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning/ (дата звернення: 12.05.2025).

26. Bricker D. Top 10 Risk-Based Vulnerability Management Tools for 2022. VentureBeat, 05.2022. URL: https://venturebeat.com/security/top-10-risk-based-vulnerability-management-vm-tools-for-2022/ (дата звернення: 12.05.2025).

27. Bricker D. Zero Trust: The New Security Paradigm. VentureBeat, 2022. URL: https://venturebeat.com (дата звернення: 12.05.2025).

28. IDC. Worldwide Security and Vulnerability Management Market Shares, 2021. IDC Market Analysis, 2022. 25 p.

29. IDC. Worldwide Device Vulnerability Management Report, 2023: Analyst Report. URL: https://www.tenable.com/sites/default/files/thumb-AnalystReport-IDC_Worldwide_Device_Vulnerability_Management_Report_2023.png (дата звернення: 12.05.2025).

30. IDC. Worldwide Device Vulnerability Management 2023 Market Share Snapshot. IDC, 2024. URL: https://www.tenable.com/analyst-research/idc-

worldwide-device-vulnerability-management-market-share-report-2023 (дата звернення: 12.05.2025).

31. SC Media. 2022 SC Awards – Best Vulnerability Management Solution: Qualys. SC Media, 2022. URL: https://www.scmagazine.com (дата звернення: 12.05.2025).

32. UpGuard. Rapid7 vs Qualys. UpGuard Blog, 2023. URL: https://www.upguard.com/blog/rapid7-vs-qualys (дата звернення: 12.05.2025).

33. PeerSpot. Qualys VMDR vs Rapid7 InsightVM vs Tenable Security Center. 2025. URL: https://www.peerspot.com/products/comparisons/qualys-vmdr_vs_rapid7-insightvm_vs_tenable-security-center (дата звернення: 12.05.2025).

34. Novinson M. Tenable, Vulcan Cyber Lead Vulnerability Management Rankings. BankInfoSecurity, 18.10.2023. URL: https://www.bankinfosecurity.com/tenable-vulcan-cyber-lead-vulnerability-management-rankings-a-23349 (дата звернення: 12.05.2025).

35. Forrester. The Forrester Wave™: Vulnerability Risk Management, Q3 2023. Forrester Research Report. Cambridge (MA), 2023. 27 p.

36. Risto J. Vulnerability Management Maturity Model (Part I). SANS Institute Blog, 2019. URL: https://www.sans.org/blog/vulnerability-management-maturity-model/ (дата звернення: 12.05.2025).

37. Nucleus Security. What Is Vulnerability Management Maturity?. Nucleus Blog, 11.01.2024. URL: https://www.nucleussec.com (дата звернення: 12.05.2025).

38. Sanchez A. What Is Vulnerability Management? Process & Use Cases. Fortra Blog, 23.07.2024. URL: https://www.fortra.com/blog/what-is-vulnerability-management-process-use-cases (дата звернення: 12.05.2025).

39. Tenable. Vulnerability Management: The Complete Guide. Tenable Cybersecurity Guide, 2025. URL: https://www.tenable.com/source/vulnerability-management (дата звернення: 12.05.2025).

40. Hiter S. Vulnerability Management: Definition, Process & Tools. eSecurityPlanet, 02.03.2023. URL:

https://www.esecurityplanet.com/networks/vulnerability-management/ (дата звернення: 12.05.2025).

41. Cronin B. Vulnerability Management Program Overview. LinkedIn. URL: https://www.linkedin.com/pulse/vulnerability-management-program-overview-brendan-cronin (дата звернення: 12.05.2025).

42. Tenable, Inc. Tenable Security Center 6.5.x User Guide: Scan Policies. 2025. URL: https://docs.tenable.com/security-center/Content/ScanPolicies.htm (дата звернення: 12.05.2025).

43. Tenable, Inc. Tenable Security Center 6.5.x User Guide: Add a Scan Policy. 2025. URL: https://docs.tenable.com/security-center/Content/AddScanPolicy.htm (дата звернення: 12.05.2025).

44. Cybersecurity and Infrastructure Security Agency (CISA). CRR Supplemental Resource Guide. Vol. 4: Vulnerability Management. 2018. URL: https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-VM_0.pdf (дата звернення: 12.05.2025).

45. Tenable, Inc. Tenable Security Center 6.5.x User Guide: Add an Active Scan. 2025. URL: https://docs.tenable.com/security-center/Content/AddActiveScan.htm (дата звернення: 12.05.2025).

46. Tenable, Inc. Tenable Security Center 6.5.x User Guide: Assets. 2025. URL: https://docs.tenable.com/security-center/Content/Assets.htm (дата звернення: 12.05.2025).

47. Tenable, Inc. Tenable Security Center 6.5.x User Guide: Add a Custom Asset. 2025. URL: https://docs.tenable.com/security-center/6_4/Content/AddCustomAsset.htm (дата звернення: 12.05.2025).

48. Aaron L. Writing Reports in Tenable’s Security Center (Asset Lists). Medium, 29.01.2024. URL: https://medium.com/@AaronLJ/writing-reports-in-tenable-s-security-center-asset-lists-1da340c0c1db (дата звернення: 12.05.2025).

49. Tenable, Inc. Tenable Security Center 6.5.x User Guide: Start or Pause a Scan. 2025. URL: https://docs.tenable.com/security-center/Content/StartPauseScan.htm (дата звернення: 12.05.2025).

50. Tenable, Inc. Tenable Security Center 6.5.x User Guide: Manage Scan Results. 2025. URL: https://docs.tenable.com/security-center/Content/ManageScanResults.htm (дата звернення: 12.05.2025).

51. Tenable, Inc. Tenable Security Center 6.5.x User Guide: View Scan Result Details. 2025. URL: https://docs.tenable.com/security-center/Content/ViewScanResultDetails.htm (дата звернення: 12.05.2025).

52. Tenable, Inc. Tenable Security Center 6.5.x User Guide: Vulnerability Analysis Tools. 2025. URL: https://docs.tenable.com/security-center/Content/VulnerabilityAnalysisTools.htm (дата звернення: 12.05.2025).

53. Tenable, Inc. Tenable Security Center 6.5.x User Guide: CVSS vs. VPR (Risk Metrics). 2025. URL: https://docs.tenable.com/security-center/Content/RiskMetrics.htm (дата звернення: 12.05.2025).

54. Tenable, Inc. Tenable Security Center 6.5.x User Guide: Create a Custom Report. 2025. URL: https://docs.tenable.com/security-center/Content/Reports/CreateCustomReport.htm (дата звернення: 12.05.2025).

55. Tenable, Inc. Tenable Security Center 6.5.x User Guide: Manage Reports. 2025. URL: https://docs.tenable.com/security-center/Content/Reports/ManageReports.htm (дата звернення: 12.05.2025).

56. Weiss J. Outstanding Remediations Tracking – SC Dashboard. Tenable Blog, 29.01.2024. URL: https://www.tenable.com/sc-dashboards/outstanding-remediations-tracking (дата звернення: 12.05.2025).

57. Tenable, Inc. Tenable Security Center 6.5.x User Guide: Add a Template-Based Dashboard. 2025. URL: https://docs.tenable.com/security-center/Content/AddTemplateDashboard.htm (дата звернення: 12.05.2025).

58. Tenable, Inc. Tenable Security Center 6.5.x User Guide: Add a Custom Dashboard Component. 2025. URL: https://docs.tenable.com/security-center/Content/AddCustomDashboardComponent.htm (дата звернення: 12.05.2025).

59. Tenable, Inc. Tenable Security Center 6.5.x User Guide: Alerts (Workflow Actions). 2025. URL: https://docs.tenable.com/security-center/Content/Alerts.htm (дата звернення: 12.05.2025).

60. Tenable, Inc. Tenable Security Center 6.5.x User Guide: View Vulnerability Instance Details. 2025. URL: https://docs.tenable.com/security-center/Content/ViewVulnerabilityInstanceDetails.htm (дата звернення: 12.05.2025).