ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА БАЗІ IBM QRADAR VULNERABILITY MANAGER»

Виконав студент 4 курсу, групи БСД-431
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Голубовський А.П.
(прізвище та ініціали)
Керівник Собчук А.В.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БД – база даних

ОС – операційна система

КІС – корпоративна інформаційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

APIs – Application Programming Interfaces

APT – Advanced Persistent Threat

CVSS – Common Vulnerability Scoring System

DNS – Domain Name System

IDS – Intrusion Detection System

IoT – Internet of Things

IP – Internet Protocol

IPsec – IP security

NGFW – Next Generation Firewall

OVAL – Open Vulnerability and Assessment Language

SaaS – Software as a Service

SIEM – Security Information and Event Management

VPN – Virtual Private Networks

QVM –QRadar Vulnerabilite Manager

ВСТУП

Актуальність дослідження. Управління вразливістю – це процес виявлення, оцінки, усунення та складання звітів про вразливості безпеки в системах та програмному забезпеченні, яке на них працює. Реалізоване з іншими безпековими тактиками, життєво важливо для організацій, щоб розставити пріоритети для можливих загроз і мінімізувати «поверхню атаки».

Вразливість безпеки, відноситься до технологічних недоліків і помилок, які дозволяють зловмисникам скомпрометувати інформаційні системи та дані, що оброблюються (міститься) в них.

Програмне забезпечення для управління вразливістю автоматизує цей процес, використовуючи сканер вразливостей, а іноді й агентів у кінцевих точках, щоб провести інвентаризацію різних систем у мережі та знайти у них вразливості.

Системи IBM QRadar SIEM та IBM QRadar Vulnerability Manager є признаними світовими лідерами в збиранні, обробці та візуалізації даних про вразливості корпоративних інформаційних систем.

Після виявлення вразливостей оцінюється ризик, який вони представляють, у різних контекстах, щоб можна було прийняти рішення про те, як краще їх виправляти (усувати). Перевірка вразливості – ефективний спосіб контекстуалізації реальної серйозності проблеми.

Від правильного визначення умов функціонування корпоративної інформаційної системи, вибору та обґрунтування складу методів та засобів управління вразливостями корпоративної інформаційної системи та ефективного їх застосування залежить ефективність забезпечення її кібербезпеки.

Вищесказане визначає актуальність теми даної бакалаврської роботи, основний зміст якої становлять дослідження методів та засобів управління вразливостями корпоративних інформаційних систем.

Об’єкт дослідження – управління вразливостями корпоративної інформаційної системи.

Предмет дослідження – методи та засоби управління вразливостями на прикладі IBM QRadar Vulnerability Manager.

Мета роботи – розробити рекомендації щодо застосування методів та засобів управління вразливостями в корпоративній інформаційній системі.

Наукові завдання:

дослідити проблему управління вразливостями корпоративних інформаційних систем;

дослідити зміст управління вразливостями корпоративної інформаційної системи;

проаналізувати існуючі методи та засоби управління вразливостями на прикладі IBM QRadar Vulnerability Manager;

розглянути варіанти побудови системи управління вразливостями корпоративної інформаційної системи з використанням IBM QRadar Vulnerability Manager.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів полягає в розробці рекомендацій щодо застосування методів та засобів управління вразливостями корпоративних інформаційних систем.

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

1.1. Дослідження проблеми управління вразливостями корпоративних інформаційних систем

Останні кілька років були далекі від звичайних, як для кібербезпеки, так і для бізнесу в цілому. Пандемія COVID-19 назавжди змінила спосіб ведення бізнесу, і кіберзлочинці пристосувалися до цих змін, адаптуючи свою тактику до нової реальності [2].

Хоча 2020 і 2021 роки були винятковими роками для кібератак, мало вказівок на те, що в 2023 році все повернеться до «нормального стану». Актори кіберзагроз випробували нові тактики та методи, виявили, що вони є успішними, і додали їх до свого основного арсеналу [2].

У 2021 році кілька кампаній кібератак і суб'єктів кіберзагроз стали загальновідомими, оскільки наслідки кібератак відчувалися далеко за межами цільових компаній. Сучасний ландшафт загроз складається з більш масштабних, яскравіших і потужних атак, оскільки кіберзлочинність стає все більш професіоналізованою, а суб'єкти кіберзагроз прагнуть отримати максимальну цінність або вплив від своїх атак [2].

Щороку певні загрози швидко зростають, оскільки кіберзлочинці зосереджують свої зусилля на особливо ефективній або прибутковій техніці атаки, наприклад, програмі-вимагачі або криптоджекінг. Однак однією з найбільш тривожних тенденцій у 2021 році було зростання кіберзлочинності в усіх сферах.

У 2021 році загальна кількість кібератак зросла на 50% за рік. Однак певні райони постраждали сильніше, ніж інші, оскільки освіта, наукові установи та охорона здоров'я несуть основний тягар збитку. Це свідчить про те, що суб'єкти кіберзагроз зосереджені на сферах, які швидко стають все більш залежними від технологій і найменш готовими до захисту від кіберзагроз [2].

Таке швидке зростання атак віщує біду до 2023 року. Оскільки суб'єкти кіберзагроз удосконалюють свої методи та використовують машинне навчання й автоматизацію, кількість і наслідки атак, ймовірно, тільки зростатимуть.

В [1] зазначається, що з січня 2023 року з програмним забезпеченням-вимагачем було пов'язано 22 нові вразливості та 9 нових слабких місць.

141 відомих використаних вразливостей CISA (Known Exploited Vulnerabilities, KEV) використовуються операторами програм-вимагачів, у тому числі 18 нещодавно виявлених у цьому кварталі.

11 вразливостей, пов'язаних із програмним забезпеченням-вимагачем, не виявлені популярними сканерами.

3 нові групи APT (Exotic Lily, APT 35, DEV-0401) і 4 нові сімейства програм-вимагачів (AvosLocker, Karma, BlackCat, Night Sky) використовують програму-вимагач для атаки своїх цілей.

Прогалини даних у CWE, CAPEC (Common Attack Pattern Enumeration and Classification) та MITRE про вразливості заважають дослідникам безпеки, водночас дають змогу зловмисникам потай проникати в організаційні мережі, які нічого не підозрюють [1].

Оператори програм-вимагачів стали невблаганними і використовують вразливості швидше, ніж будь-коли, для досягнення своїх цілей. Нові вразливості включають три критичного ступеня тяжкості та вісімнадцять високого рівня за стандартом CVSS V3.

Кількість популярних вразливостей зросла на 6,8%, оскільки оператори програм-вимагачів продовжують шукати слабкі місця, які можуть створити максимальний збій і вплив на їхні цілі.

Деякі з найпопулярніших сканерів не виявляють кілька ключових вразливостей програм-вимагачів. В [1] досліджено, що понад 3,5% вразливостей програм-вимагачів упускаються, що наражає організації на серйозні ризики. Дослідження відомих використаних вразливостей CISA (KEV) також показало, що в сканерах відсутні 1,5% вразливостей, пов'язаних із програмним

забезпеченням-вимагачем. Крім того, існує додатковий ризик націлювання на вразливості нульового дня і для їх виявлення потрібен *новий підхід*.

Позитивним є те, що загальна кількість вразливостей програм-вимагачів, упущених сканерами, зменшилася з 22 (4 квартал 2021 року) до 11 (1 квартал 2023 року). Це розвиток у правильному напрямку, і сподіваємося, що всі рішення для сканерів активізуються в боротьбі з програмами-вимагателями, також зменшуючи затримки у випуску плагінів для сканерів [1].

Чітка закономірність помічено з 2021 року – це *зростаюча швидкість використання вразливостей*. Невеликої слабкості в заходах безпеки сторонніх постачальників і організацій, що використовують їхні продукти, достатньо для того, щоб групи програм-вимагачів могли проникнути в уразливі мережі. Вважається, що *управління вразливостями нового покоління має використовувати прогнозний підхід*, який може передбачати високу застосовність вразливостей задовго до того, як вони можуть бути скомпрометовані [1].

Експерти CSW провели дослідження прийомів і тактик, які застосовували зловмисники під час використання недоліків програмного забезпечення. Це дослідження було проведено з використанням понад 500 вразливостей, які були частиною каталогу CISA KEV під час дослідження. Дане дослідження висунуло на перший план різні прогалини, які існують на таких сайтах, як MITRE, NVD та Common Attack Pattern Enumeration and Classification (CAPEC), а також те, як ці невідповідності допомагають зловмисникам. Щоб оцінити прогалини та рекомендувати виправлення кожної вразливості, нашим дослідникам довелося зібрати інформацію з 17 різних джерел, окрім NVD та MITRE. Наші ключові висновки включають [1]:

Щоб подолати такі прогалини в даних і зрозуміти, як можна скористатися цими недоліками, *організації повинні шукати автоматизовані джерела, які можуть відображати вразливості за допомогою відповідних методів MITRE*.

Оскільки дослідники безпеки та IT-команди мають обмежені можливості через інформаційні прогалини, неточно нанесені на карту слабкі місця та відсутня інформація про тактику та техніку, критичні вразливості, пов’язані з програмним

забезпеченням-вимагачем, не є пріоритетними. Крім того, перевантажені команди безпеки не мають ресурсів або часу, щоб переглянути 17+ джерел даних, щоб заповнити прогалини в розвідці та прийняти обґрунтовані рішення для виправлення.

Програми-вимагачі зараз є одним із найбільш переважаючих векторів атак, які впливають на прибуток організацій у всьому світі. У першому кварталі встановлено збільшення кількості вразливостей програм-вимагачів і APT, які використовують програму-вимагач [1].

Однак одна з основних проблем з'явилася відсутність повної видимості загроз для команд безпеки через захаращену інформацію про загрози, доступну в різних джерелах. Якщо командам безпеки потрібно завчасно пом'якшувати атаки програм-вимагачів, вони повинні прив'язати свої виправлення та реагування на вразливості до централізованого робочого процесу управління розвідкою загроз, який забезпечує завершену видимість векторів атаки програм-вимагачів, що змінюють форму, завдяки використанню розвідувальних даних із кількох джерел, кореляції та дії безпеки.

Дослідження вразливостей [1], якими користуються групи програм-вимагачів, виявило 22 нові вразливості в першому кварталі 2023 року, що на 7,6% більше, ніж у грудні 2021 року. Загалом 310 вразливостей тепер пов'язані з програмним забезпеченням-вимагачем. Усі ці вразливості мають доступні виправлення, пом'якшення чи обхідні шляхи, і організаціям рекомендується застосувати виправлення, поки не стало надто пізно.

11 із 22 вразливостей, нещодавно пов'язаних із програмним забезпеченням-вимагачем, належать до 2019 року, що вказує на те, що групи програм-вимагачів шукають вразливості за допомогою вже існуючих засобів експлуатації.

Нещодавно додані вразливості включають три критичного ступеня тяжкості, 18 позначених як високий ступінь тяжкості та одну, що належить до категорії середньої тяжкості [1].

14 з оновлених вразливостей мають відомі загальнодоступні експлойти (шість для віддаленого виконання коду (Remote Code Execution, RCE), 12 для

підвищення привілеїв (Privilege Escalation, PE), чотири для вразливостей веб-додатків і одна для відмови в обслуговуванні (denial-of-service, DoS)). Зокрема, CVE-2021-22005 і CVE-2021-22986 пов'язані з загальнодоступними експлойтами для атак RCE, PE та веб-програм [1].

Сім з 22 вразливостей перераховані в категорії слабкості CWE-59, що призводить до неправильного розв'язання посилань під час доступу до файлів. У народі званий слабкістю «небезпечний тимчасовий файл», програмне забезпечення може використовувати ненавмисний ярлик або ресурс, що може дозволити зловмисникам обійти механізми безпеки. Дві значні виноски: CVE-2021-22986 (F5), який стосується 73 продуктів із F5, і CVE-2021-21985, що стосується 56 продуктів VMware.

Дослідження виявило чотири нових сімейства програм-вимагачів, які з'явилися в першому кварталі 2023 року, збільшивши кількість сімейств програм-вимагачів зі 157 до 161 [1].

New Ransomware Families	No. of CVEs Leveraged by the Family
AvosLocker	5
Karma	3
BlackCat (AlphaV)	2
Night Sky	1

Рис. 1.1. Нові сімейства програм-вимагачів [1]

Сімейства програм-вимагачів AvosLocker і Karma (рис. 1.1) націлені на CVE-2021-31207, CVE-2021-34473 і CVE-2021-34523 на сервері Microsoft Exchange. Ці вразливості також пов'язані з шістьма нещодавно активними сімействами програм-вимагачів, включаючи BlackByte, Conti, Babuk і LockFile.

Фактично всі п'ять вразливостей, пов'язаних з AvosLocker, присутні на

серверах Exchange. Сімейство BlackCat використовує можливості для використання 6-річної вразливості в старих версіях Microsoft Windows. Група також використовує недоліки SQL-ін'єкції 2019 року в пристроях із захищеним віддаленим доступом SonicWall, які вийшли з ладу.

Збільшення кількості сімей програм-вимагачів на 2,5%. Лідер: сімейство програм-вимагачів Conti домінували в першому кварталі 2023 року з його початковою заявою про підтримку Росії у війні проти України. Дослідження [1] пов'язує Conti з 27 вразливостями в першому кварталі 2023 року, що більш ніж удвічі збільшує кількість вразливостей з 2021 року.

Плідні групи програм-вимагачів, такі як Conti, завжди прагнуть додати до свого арсеналу більше вразливостей. Відстежуючи траєкторію цих загроз, ми не можемо підкреслити важливість того, щоб організації використовували розвідку про вразливості, постійне сканування та керування поверхнею атак цифрових екосистем для захисту своїх мереж і даних [1].

Аналіз вразливостей програм-вимагачів виявив дев'ять нових вразливостей які призвели до цих недоліків у першому кварталі 2023 року. З цим збільшенням на 17% тепер ми маємо 189 вразливостей, які забезпечують 310 вразливостей, пов'язаних із групами програм-вимагачів. Оскільки програмне забезпечення-вимагач націлено на конкретні слабкі місця в багатьох продуктах і програмах, організаціям знадобиться додаткове сканування додатків, щоб зрозуміти та визначити пріоритети своїх вразливостей. Виходячи з точки зору тестувальника на проникнення, виділяється шість найнебезпечніших недоліків, які показано на рис. 1.2.

Крім того, наш аналіз методів і тактик, які використовували зловмисники, які експлуатують уразливості, пов'язані з програмним забезпеченням-вимагачем, показав, що 310 вразливостей програм-вимагачів було більш ніж достатньо для того, щоб зловмисники проникли в мережі, проникли глибше, ухилялися від виявлення, блокували файли та вимагали викуп. Це робить список із 310 вразливостей CSW надзвичайно небезпечним і необхідним для захисту.

New Ransomware CWEs in Q1 2022	Weakness Category	OWASP Ranking	MITRE Ranking	Ransomware	Impact
CWE-285	Improper Authorization	A01	-	eCh0raix Qlocker	Could allow unauthorized resource access and can escalate to broken access control issues, XSS, and session replay issues
CWE-294	Authentication Bypass by Capture-Replay	A07	-	ClearEnergy	Can be escalated to perform code execution, session sidejacking, kerberoasting, remote services with stolen credentials, pass the hash, pass the ticket, and adversary-in-the-middle (AiTM) attacks
CWE-345	Insufficient Verification of Data Authenticity	A08	-	UEFI	Could result in failure to verify origin or authenticity of data, and can be used to perform code execution
CWE-36	Absolute Path Traversal	-	-	Phobos JNEC Shkolatacrypt Stop	Could give rise to path traversal and code execution vulnerabilities due to not neutralizing the absolute path
CWE-400	Uncontrolled Resource Consumption	-	27	Conti Khonsari TellYouThePass NightSky Stop	Could lead to lack of throttling for the number of allocated resources, losing all references to a resource before reaching the shutdown stage, not closing or returning a resource after processing, error conditions and other exceptional circumstances, and confusion over which part of the program is responsible for releasing the resource
CWE-693	Protection Mechanism Failure	-	-	UEFI Shkolatacrypt	Could be used to perform forceful browsing, manipulating states, directory indexing, and using unpublished interfaces

Рис. 1.2. Найнебезпечніші недоліків, які експлуатуються зловмисниками [1]

Треба відмітити, що групи програм-вимагачів продовжують використовувати старіші вразливості. У CSW зазначили, що всі вразливості програм-вимагачів, нещодавно виявлені в цьому кварталі, належать до цієї категорії. Зараз маємо 310 старих вразливостей, що на 17,9% більше, ніж у попередньому звіті. Загальна кількість зараз становить 100% вразливостей програм-вимагачів, виявлених під час нашого дослідження, що свідчить про те, що групи використовують зрілі експлойти та загальнодоступні коди, які можна легко налаштувати під свої потреби. CVE-2015-2546, 7-річна вразливість середньої тяжкості, була пов’язана з програмним забезпеченням-вимагачем у першому кварталі 2023 року разом із двома іншими вразливостями 2016 та 2017

років [1].

Age of Vulnerability	Count of Vulnerabilities Used By Ransomware
More than 10 years old (Before 2013)	23
5–10 years old (2013–2017)	133 (includes 4 added in Q1 2022)
Less than 5 years old (2018–2021)	154 (includes 18 added in Q1 2022)

Рис .1.3. Актуальні «старі» вразливості [1]

Постійно спостерігається те, що групи програм-вимагачів не тільки шукають критичні вразливості, але й націлюються на низької та високої серйозності, які часто не мають пріоритету в системі виправлення систем. 20 із 22 вразливостей, виявлених у цьому кварталі, є вразливості з низьким рівнем оцінки CVSS v2 менше восьми. Це означає збільшення на 11,6% у першому кварталі 2023 року, що сприяло 193 з усіх вразливостей програм-вимагачів із низькими результатами. На 82% уразливості високого рівня домінують у списку нещодавно доданих вразливостей у цьому кварталі за класифікацією CVSS V3 [1].

Також, дослідження [1] виявило 919 унікальних продуктів 103 різних постачальників як сприйнятливі до програм-вимагачів. Нові вразливості, виявлені в першому кварталі 2023 року, стосуються 164 різних продуктів (рис. 1.4).

Категорія продуктів, на яку найбільше впливає новий набір вразливостей програм-вимагачів, – це операційні системи, за ними йдуть брандмауери та веб-браузери (рис. 1.5).

Vendor	Overall Count of Vulnerabilities	Product with Most Vulnerabilities
F5	17	Big IP products
Microsoft	143	Windows
VMware	4	Cloud Foundation and vCenter Server

Рис. 1.4. Кількість виявлених вразливостей ПЗ конкретних виробників [1]

Помітні атаки проводилися на сектор охорони здоров'я, такі як атака Conti в Ірландії, зловживання пневматичними трубками, коригування рівня дозування та перебої в мережі лікарень, одна з яких призвела до смерті немовляти [1].

Product Category	Count of Vulnerabilities
Operating System	125
Firewall	17
Web Browser	12
Desktop App	3
Cloud Desktop Application	2
Application Framework	2
Web Application	1
Microsoft Office Suite	1
Email Service	1

Рис. 1.5. Кількість виявлених вразливостей ПЗ [1]

75% під'єднаних до мережі медичних інфузійних насосів були визнані вразливими до недоліків безпеки у 2019–2020 роках, що може призвести до ненормальних і смертельних доз ліків, які вводять пацієнтам.

CVE-2021-43935 в кардіологічних пристроях Hillrom можна використовувати для повного контролю над медичним обладнанням, яке відстежує рівень серцевого стресу, ЕКГ та інші проблеми, пов'язані з серцем.

Вразливості, виявлені в розумних автономних мобільних роботах Aethon TUG і JekyllBot:5, забезпечують легке налаштування для бічного переміщення через лікарняні мережі та ідеальну панель запуску для корисних програм-вимагачів [1].

Медичні працівники повинні бути надзвичайно пильними щодо кібербезпеки. На жаль, коли пандемія заспокоїться, індустрія охорони здоров'я,

ймовірно, стане більш агресивною мішенню атак програм-вимагачів, які калічать мережі та загрожують безпеці пацієнтів. Зловмисники стали більш досконалими, і вони, ймовірно, будуть націлені на пристрої Інтернету речей охорони здоров'я, як-от насоси для внутрішньовенного введення, а не лише на традиційні пристрої, такі як мобільні пристрої та ноутбуки [1].

Ключовим фактором, який виділяється, є швидкість зброї вразливостей програм-вимагачів. Деякі вразливі місця були використані протягом восьми днів після публікації їх постачальником [1].

Усі нові вразливості програм-вимагачів були опубліковані їхніми постачальниками разом із патчем. Виняткові вразливості щодо зброї – CVE-2016-3309, CVE-2017-0101 і CVE-2019-1215 – були використані майже через рік після того, як вразливості були опубліковані та виправлені їхніми постачальниками та додані в NVD. П'ять із вразливостей було використано, перш ніж їх можна було додано до NVD. У середньому нові вразливості програм-вимагачів додавали до NVD через тиждень після того, як їх розкрив постачальник.

Програми-вимагачі є поширеною загрозою. Зловмисники та оператори програм-вимагачів постійно шукають нові вразливості, щоб розширити свій арсенал інструментів, тактик і методів. У звіті ФБР про злочини в Інтернеті за 2021 рік зафіксовано 649 атак програм-вимагачів на критично важливу інфраструктуру, внаслідок чого було втрачено майже 50 мільйонів доларів США. Усі організації піддаються ризику від цієї загрози, і більшість з них не підготовлені для боротьби з нею.

Відсутність кібергігієни, бюджетні обмеження, обмежена робоча сила, відсутність талантів, недостатня інформація про кібербезпеку в потрібний момент, а також відсутність видимості та обізнаності є одними з факторів, які дають змогу операторам програм-вимагачів здійснювати сміливі та жахливі атаки.

Ми бачимо, що за два роки ця загроза експоненціально зросла з 57 до 310 вразливостей. Спостерігається, як постраждалі організації страждають, оскільки

вони втрачають свою репутацію, довіру та цінність бренду, що призводить до втрати бізнесу та клієнтів.

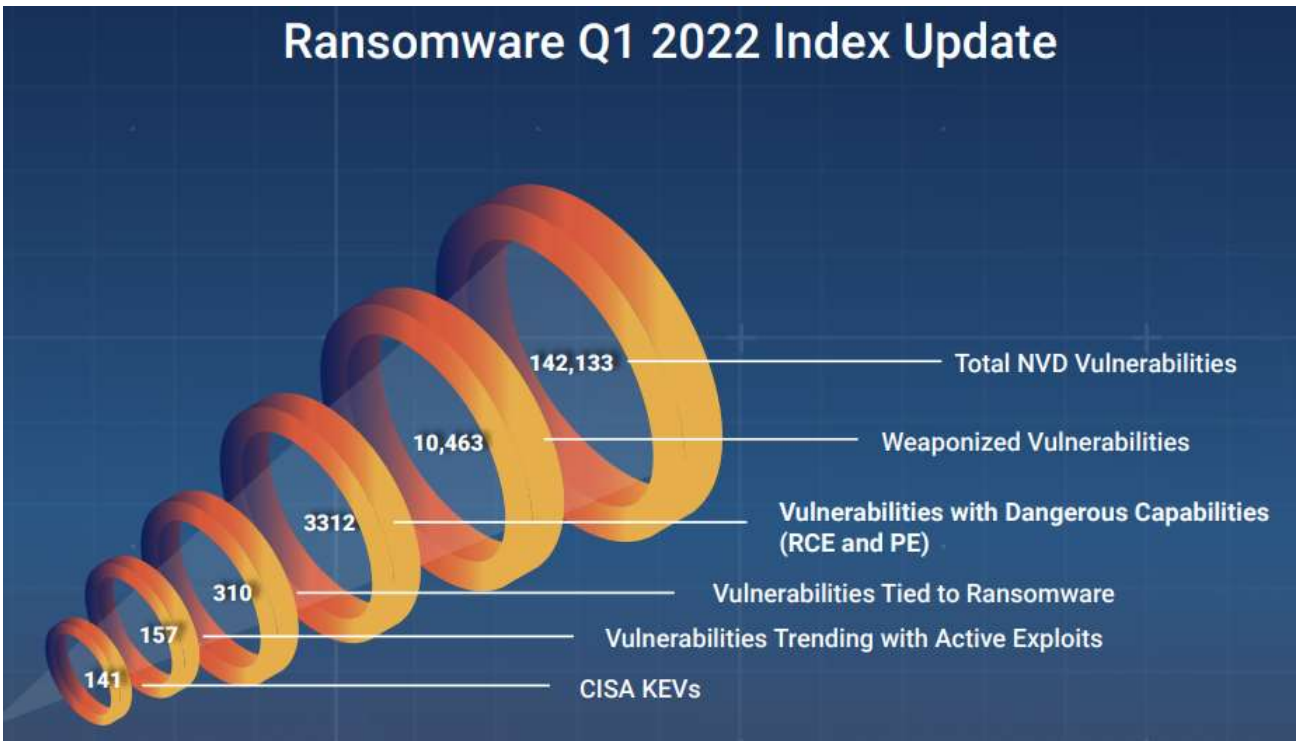

Рис. 1.6. Дінамика зростання вразливостей [1]

Сьогодні лише декілька організацій мають доступ до своєчасних знань і даних про програм-вимагач. Багато хто не знає про рівень загроз, з якими вони стикаються.

1.2. Зміст управління вразливостями корпоративних інформаційних систем

Управління вразливостями – це постійний регулярний процес виявлення, оцінки, звітування про вразливості, керування ними та усунення їх у кінцевих точках, робочих навантаженнях і системах. Як правило, команда безпеки використовує інструмент керування вразливостями, щоб виявляти вразливості та використовувати різні процеси для їх виправлення або виправлення [4].

Потужна програма управління вразливістю використовує дані про загрози

та знання IT та бізнес-операцій, щоб визначати пріоритети ризиків та якнайшвидше усунути вразливості.

Вразливість, за визначенням Міжнародної організації зі стандартизації (SO 27002), це «слабкість активу або групи активів, які можуть бути використані однією або кількома загрозами».

Загроза – це те, що може використовувати вразливість.

Ризик – це те, що відбувається, коли загроза використовує вразливість. Це збиток, який може бути завдано відкритою вразливістю, яку використовує загроза [4].

Стратегія управління вразливістю складається з шести окремих етапів, які показано на рисунку 1.7 [3].

Рис. 1.7. Стратегія управління вразливістю [3]

Інвентаризація активів

Першим етапом у стратегії управління вразливістю має бути проведення інвентаризації. Однак багатьом організаціям бракує ефективного реєстру активів, і тому їм важко захистити свої пристрої. Інвентаризація активів – це інструмент, який адміністратори безпеки можуть використовувати для перегляду пристроїв,

які є в організації, і виділення тих, які мають бути покриті програмним забезпеченням безпеки.

У стратегії управління вразливостями організація повинна почати з надання одному співробітнику відповідальності за управління інвентаризацією активів, щоб гарантувати, що всі пристрої записані та що інвентар залишається актуальним. Інвентаризація активів також є чудовим інструментом, який адміністратори мережі та системи можуть використовувати для швидкого пошуку та виправлення пристроїв і систем. Без інвентаризації деякі пристрої можуть бути залишені, коли нове програмне забезпечення безпеки буде виправлено або встановлено.

Управління інформацією

Другим етапом стратегії управління вразливістю є контроль надходження інформації в організацію. Найважливішим інформаційним потоком є інтернет-трафік, що надходить із мережі організації. Зросла кількість хробаків, вірусів та інших шкідливих програм, від яких організації повинні захищатися. Також спостерігається збільшення потоку трафіку як всередині, так і за межами локальних мереж. Збільшений потік трафіку загрожує принести більше шкідливих програм в організацію. Тому слід звернути увагу на цей інформаційний потік, щоб запобігти проникненню або виходу загроз з мережі.

Окрім загрози зловмисного програмного забезпечення, управління інформацією також стосується даних організації. Організації зберігають різні типи даних, і деякі з них ніколи не повинні потрапляти в руки неправильних людей. Така інформація, як комерційна таємниця та особиста інформація клієнтів, може завдати непоправної шкоди, якщо до неї отримають доступ хакери. Організація може втратити свою репутацію, а також може бути оштрафована на величезні суми за невиконання захисту даних користувачів. Організації конкуренти можуть отримати секретні формули, прототипи та бізнес-секрети, що дозволило їм зашкодити організацію-жертву. Тому управління інформацією є життєво важливим у стратегії управління вразливістю.

Щоб досягти ефективного управління інформацією, організація може

розгорнути групу реагування на інциденти комп'ютерної безпеки (CSIRT) для боротьби з будь-якими загрозами для її зберігання та передачі інформації.

Зазначена команда не просто реагуватиме на інциденти злому, а й інформуватиме керівництво про спроби вторгнення отримати доступ до конфіденційної інформації та рекомендуватиме найкращий спосіб дій. Окрім цієї команди, організація може прийняти політику найменших привілеїв, коли справа стосується доступу до інформації. Ця політика гарантує, що користувачам буде заборонено доступ до всієї інформації, крім тієї, яка необхідна їм для виконання своїх обов'язків. Зменшення кількості людей, які отримують доступ до конфіденційної інформації, є гарним заходом для зменшення можливостей атаки.

Оцінка ризику

Це третій крок у стратегії управління вразливістю. Перш ніж ризики можна буде пом'якшити, команда безпеки повинна провести глибокий аналіз вразливостей, з якими вона стикається. В ідеальному IT-середовищі команда безпеки могла б реагувати на всі вразливості, оскільки мала б достатньо ресурсів і часу. Однак насправді існує багато обмежуючих факторів, коли мова йде про ресурси, доступні для пом'якшення ризиків. Тому оцінка ризику є надзвичайно важливою. На цьому етапі організація має поставити пріоритет одних уразливостей над іншими та виділити ресурси для їх пом'якшення.

ISO 27001, пункт 4.2.1 і ISO 27005, пункт 7.4 встановлюють основні цілі процесу вибору підходу та методології для оцінки ризику, як показано на рисунку 1.8. ISO рекомендує вибрати та визначити підхід до оцінки ризику, який узгоджується з керівництвом організації з методологією, яка відповідає організації.

Оцінка вразливості

Оцінка вразливості тісно слідує за оцінкою ризику в стратегії управління вразливістю. Це тому, що ці два етапи тісно пов'язані. Оцінка вразливості передбачає виявлення вразливих активів. Цей етап проводиться через низку етичних спроб злому та тестів на проникнення. Ці атаки спрямовані на сервери, принтери, робочі станції, брандмауери, маршрутизатори та комутатори в

організаційній мережі. Технічно тестування на проникнення – це перевірка вразливостей, що визначає фактор імовірності за можливістю використання вразливості.

Рис. 1.8. Методологія оцінки ризиків ISO [3]

Оцінка вразливості лише виявляє наявність уразливості.

Мета полягає в тому, щоб змоделювати реальний сценарій злому за допомогою тих самих інструментів і прийомів, які може використовувати потенційний зловмисник. Більшість із цих інструментів обговорювалися в розділах про розвідку та компрометацію системи. Метою цього кроку є не лише виявлення вразливостей, а й швидке та точне виконання цього. Цей крок повинен дати вичерпний звіт про всі вразливості, яким піддається організація. Проблем, з якими стикаються на цьому етапі, багато.

Перше, що слід розглянути, має стосуватися того, що має оцінити організація. Без відповідної інвентаризації активів організація не зможе визначити, на яких пристроях їй слід зосередитися. Також буде легко забути оцінити певні хости, але вони можуть бути ключовими цілями для потенційної атаки.

Інша проблема пов’язана із використовуваними сканерами вразливостей. Деякі сканери надають неправдиві звіти про оцінку і направляють організацію на

неправильний шлях. Звичайно, помилкові результати завжди будуть, але деякі інструменти сканування перевищують допустимий відсоток і продовжують виявляти неіснуючі вразливості.

Це може призвести до втрати ресурсів організації. Збої – це ще один набір проблем, які виникають на цьому етапі. У зв'язку з усіма етичними хакерськими заходами та тестуванням на проникнення страждає мережа, сервери та робочі станції. Мережне обладнання, таке як брандмауери, також працює мляво, особливо коли здійснюються атаки відмови в обслуговуванні.

Відстеження звітності та виправлення

Після оцінки вразливості переходить до етапу звітності та відновлення. Ця фаза має дві однаково важливі завдання: звітність і відновлення. Завдання звітності допомагає адміністраторам системи зрозуміти поточний стан безпеки організації та області, в яких вона все ще не захищена, і вказує на це відповідальній особі. Звітність також дає щось відчутне для керівництва, щоб вони могли пов'язати це з майбутнім напрямком організації. Звіти зазвичай передують виправленню, тому вся інформація, зібрана на етапі управління вразливістю, може безперешкодно передаватись на цей етап.

Виправлення розпочинає фактичний процес завершення циклу керування вразливими місцями. Фаза управління вразливістю, як уже обговорювалося, закінчується передчасно після аналізу загроз і вразливостей, а також визначення прийнятних ризиків. Усунення доповнює це шляхом пошуку рішень для виявлених загроз і вразливостей. Усі вразливі хости, сервери та мережеве обладнання відстежуються та вживаються необхідні кроки для видалення вразливостей, а також для захисту їх від майбутніх експлойтів. Це найважливіше завдання в стратегії управління вразливістю, і якщо воно добре виконане, управління вразливістю вважається успішним.

Планування реагування

Планування реагування можна вважати найпростішим, але, тим не менш, дуже важливим кроком у стратегії управління вразливістю. Це легко, тому що вся важка робота буде виконана на попередніх п'яти кроках. Це важливо, оскільки без

його виконання організація все одно буде наражатися на загрози. На цьому етапі має значення лише швидкість виконання. Великі організації стикаються з серйозними перешкодами, коли справа доходить до його виконання через велику кількість пристроїв, які потребують виправлення та оновлення.

Як приклад, стався інцидент, коли Microsoft оголосила про існування MS03-023 (переповнення буфера в конвертері HTML може дозволити виконання коду, 11) і випустила патч для нього. Менші організації, які мають короткі плани реагування, змогли виправити свої операційні системи оновленням незабаром після оголошення. Однак більші організації, які не мають або мають довгі плани реагування на свої комп’ютери, піддалися сильному нападу хакерів. Хакери випустили хробак MS Blaster для атаки на невиправлені операційні системи лише через 26 днів після того, як Microsoft надала своїм користувачам робочий патч. Цього було достатньо часу навіть великим компаніям, щоб повністю виправити свої системи. Однак відсутність планів реагування або використання тривалих планів реагування спричинили, що деякі з них стали жертвами хробака [3].

Черв'як спричинив млявість мережі або збій на комп'ютерах, які він інфікував. Ще одним відомим інцидентом, який стався, став вимагач WannaCry. Це найбільша в історії атака програмного забезпечення-вимагача, спричинена вразливістю EternalBlue, нібито вкраденою з АНБ [3].

Атака почалася в травні, але Microsoft випустила патч для уразливості EternalBlue у березні. Однак він не випустив виправлення для старих версій Windows, таких як XP. З березня до дня виявлення першої атаки у компаній було достатньо часу, щоб виправити свої системи. Однак більшість компаній не зробили цього до моменту початку атаки через погане планування реагування. Якби атаку не було зупинено, жертвами стали б ще більше комп’ютерів.

Це показує, наскільки важлива швидкість, коли справа доходить до планування реагування. Патчі повинні бути встановлені в той момент, коли вони будуть доступні.

1.3. Аналіз існуючих методів та засобів управління вразливостями корпоративних інформаційних систем

У більшості організацій буквально занадто багато вразливостей, щоб відстежувати їх вручну, і не всі вони становлять однаковий ризик. Тепер уявіть, що ви відстежуєте численні вразливості в тисячах різнорідних активів у розподіленій мережі. Оскільки проміжок між розкриттям вразливостей та їх використанням зловмисниками скорочується, організаціям потрібно швидко їх усунути.

З обмеженим часом і ресурсами, а також без передумов ризику, необхідного для визначення пріоритетів проблем, ваші зусилля з управління вразливістю можуть бути марними. До того ж, багато інструментів керування вразливістю на ринку пропонують виправлення за допомогою сторонньої інтеграції, але поєднання кількох інструментів для оцінки вразливостей та керування виправленнями призводить до фрагментованого та неефективного робочого процесу.

Якщо зловмисник дійсно використовує вразливість як шлюз в мережу, це ігноровані неправильні конфігурації, які вони використовуватимуть, щоб переміщати та використовувати інші машини в мережі. Ось чому кожна лазівка повинна бути усунена разом із вразливістю програмного забезпечення, щоб отримати надійну стратегію безпеки та мінімізувати поверхню атаки.

Хоча випуск виправлень, опублікованих постачальником, для постраждалих машин є ідеальним варіантом відновлення, важливо мати безпечний план, до якого можна відступити в разі невиправлення обставин, таких як програмне забезпечення, яке закінчилося, і вразливості нульового дня.

Програмне забезпечення для управління вразливістю використовує підхід до кібербезпеки, в основі якого лежить активний пошук слабких місць, скануючи та виявляючи вразливі місця в мережі, а також надаючи пропозиції щодо виправлення, щоб пом’якшити ймовірність майбутніх порушень корпоративної безпеки. Це розумний спосіб для компаній бути на крок попереду хакерів [5].

Деякі інструменти керування вразливістю не лише пропонують розуміння того, як усунути потенційні загрози кібербезпеці, вони можуть призначати рівні загроз слабким сторонам, що дозволяє IT-командам визначати пріоритети щодо найважливіших проблем, які слід вирішувати в першу чергу. Деякі можуть навіть автоматично виправляти певні вразливості, застосовуючи виправлення та вносячи інші виправлення [5].

Існує багато підходів, що використовуються в управлінні вразливістю [5]:

сканери вразливостей сканують усі кінцеві точки, щоб знайти відсутні виправлення, діри в безпеці та інші вразливості;

тестування на проникнення – це підхід, який використовує погляд хакера на підприємство, щоб побачити, як і де можна зламати захист;

інструменти моделювання злому та атак (BAS) досліджують слабкі місця та надають спосіб визначення пріоритетів виправлень;

оцінка вразливості аналізує загальну систему безпеки організації та вразливості та може визначити пріоритети рішень;

керування виправленнями потім застосовує виправлення, визначені засобом керування вразливістю.

Інструменти керування вразливостями поєднують кілька з цих підходів і додають пріоритети та виправлення. Деякі продукти автоматизують ці функції, щоб полегшити навантаження на перевантажених співробітників служби безпеки.

Управління вразливістю вимагає надійного набору функцій для інкапсуляції всіх потреб компанії в безпеці підприємства. Основні можливості інструментів управління вразливістю [5]:

постійний моніторинг і пошук потенційних вразливостей;

профіль моніторингу та система правил (IT може визначити, які системи та активи слід відстежувати);

можливість встановлювати правила сповіщень;

візуалізація поверхні атаки;

векторна аналітика та моделювання атаки;

оцінка ризиків;

керування патчами;

автоматичні оновлення та виправлення;

аналіз шляхів доступу до мережі для виявлення проблемних маршрутів доступу та пропозиції щодо перенаправлень трафіку з меншим ризиком;

аналіз доступності для кінцевих точок і захищених активів;

настроювані звіти, наприклад звіти про відповідність правилам;

автоматизоване виправлення.

Розглянемо найкращі рішення для управління вразливістю.

Qualys VMDR дозволяє організаціям автоматично виявляти кожен актив у своєму середовищі, включаючи некеровані активи, які з'являються в мережі; інвентаризація всього апаратного та програмного забезпечення; а також класифікувати та позначати критичні активи – і все це в одному хмарному додатку. Він постійно оцінює ці активи на наявність останніх вразливостей і застосовує останній аналіз загроз, щоб визначити пріоритети та виправити вразливості, які активно експлуатуються.

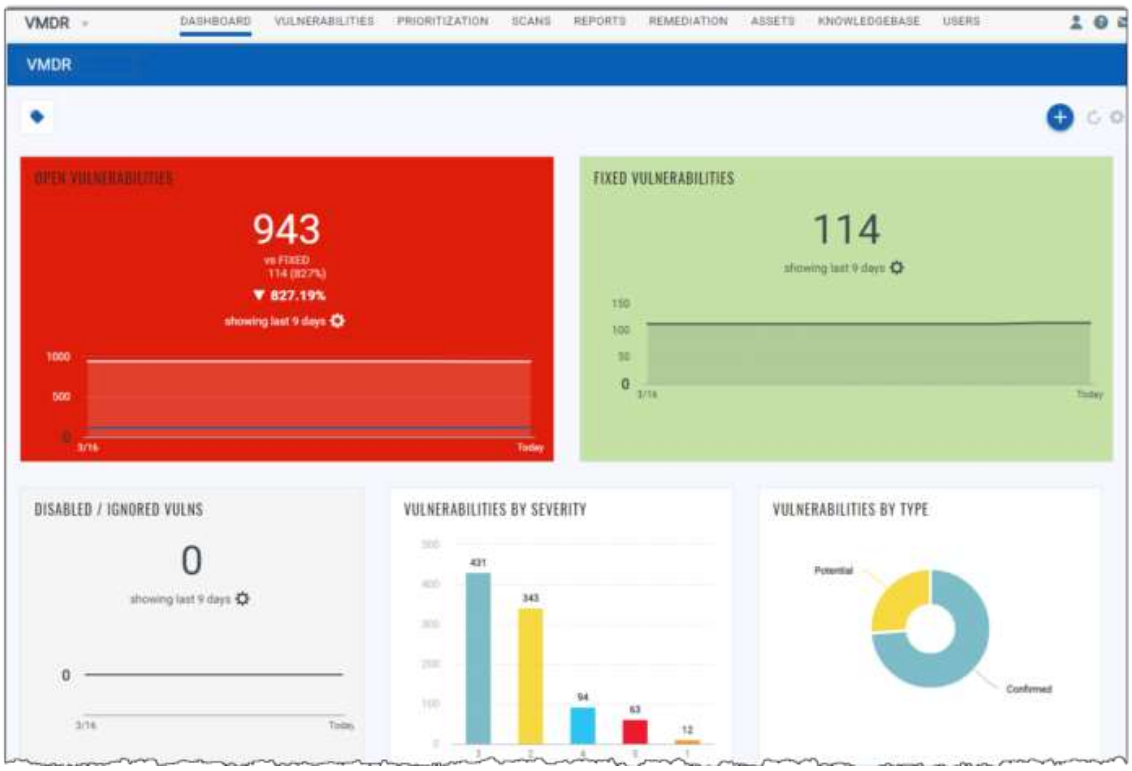

Рис. 1.9. Інтерфейс Qualys VMDR

Ключові диференціатори

Qualys Threat Detection з аналізом загроз у реальному часі та машинним навчанням може контролювати та реагувати на загрози, що розвиваються, і запобігати злом.

Інструмент автоматично виявляє та розгортає останню заміну виправлення для вразливих активів.

Qualys VMDR автоматично виявляє та класифікує відомі та невідомі активи, постійно визначає некеровані активи та створює автоматизовані робочі процеси для керування ними.

Він запитує активи та будь-які атрибути, щоб забезпечити видимість обладнання, конфігурації системи, додатків, служб та інформації про мережу.

Інструмент виявляє та ідентифікує критичні вразливості та неправильні конфігурації, у тому числі на мобільних пристроях, операційних системах і програмах, які розбиваються за активами.

Моделі аналізу загроз у реальному часі, кореляції та машинного навчання автоматично визначають пріоритети найбільш ризикованих уразливостей.

Хмарна платформа Qualys у поєднанні з легкими хмарними агентами, віртуальними сканерами та мережевим аналізом (пасивне сканування) об’єднані в одній програмі за допомогою робочих процесів оркестрації.

Rapid7 пропонує два інструменти. Nexpose Vulnerability Scanner – це локальний сканер уразливостей з охопленням усієї мережі в режимі реального часу. Він адаптується до нових загроз за допомогою свіжих даних. Крім того, його хмарний інструмент InsightVM пропонує все в Nexpose плюс розширені можливості, такі як робочі процеси виправлення та універсальний агент Insight Agent Rapid7.

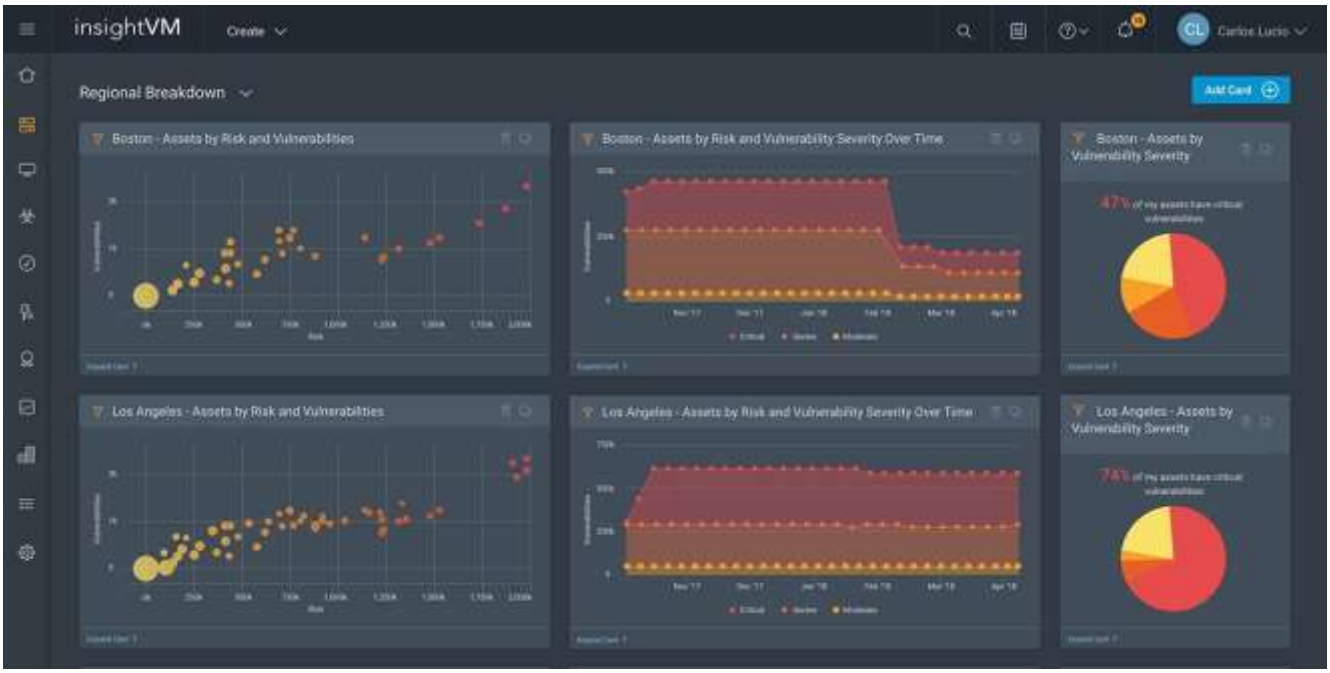

Рис. 1.10. Панель інструментів Rapid7 InsightVM

Ключові диференціатори

Показує, на які вразливості слід зосередитися в першу чергу за допомогою більш значущих показників ризику.

Надає IT інформацію, необхідну для швидкого та ефективного вирішення проблем.

Замість визначення пріоритетів на основі діапазону 1–10, він забезпечує оцінку ризику від 1 до 1000.

Nexpose пропонує нагляд за локальними, хмарними та контейнерними інфраструктурами.

Інструмент має адаптивний захист, який автоматично виявляє та оцінює нові пристрої та вразливості.

Nexpose включає оцінки політики для порівняльних систем.

Доступні спеціальні та вбудовані звіти.

Користувачі можуть скористатися перевагами живих інформаційних панелей, які оновлюються в режимі реального часу.

Інструмент пропонує автоматичне тестування ручкою.

Користувачам доступна велика кількість ресурсів підтримки спільноти.

У Rapid7 є суміжні інструменти, доступні для використання вразливостей, а саме фреймворк Metasploit.

Tenable.io надає своєчасну інформацію про всю поверхню атаки, включаючи уявлення про всі активи та вразливості. Він доступний у вигляді хмарного рішення та допомагає IT підвищити ефективність дій із керування вразливостями.

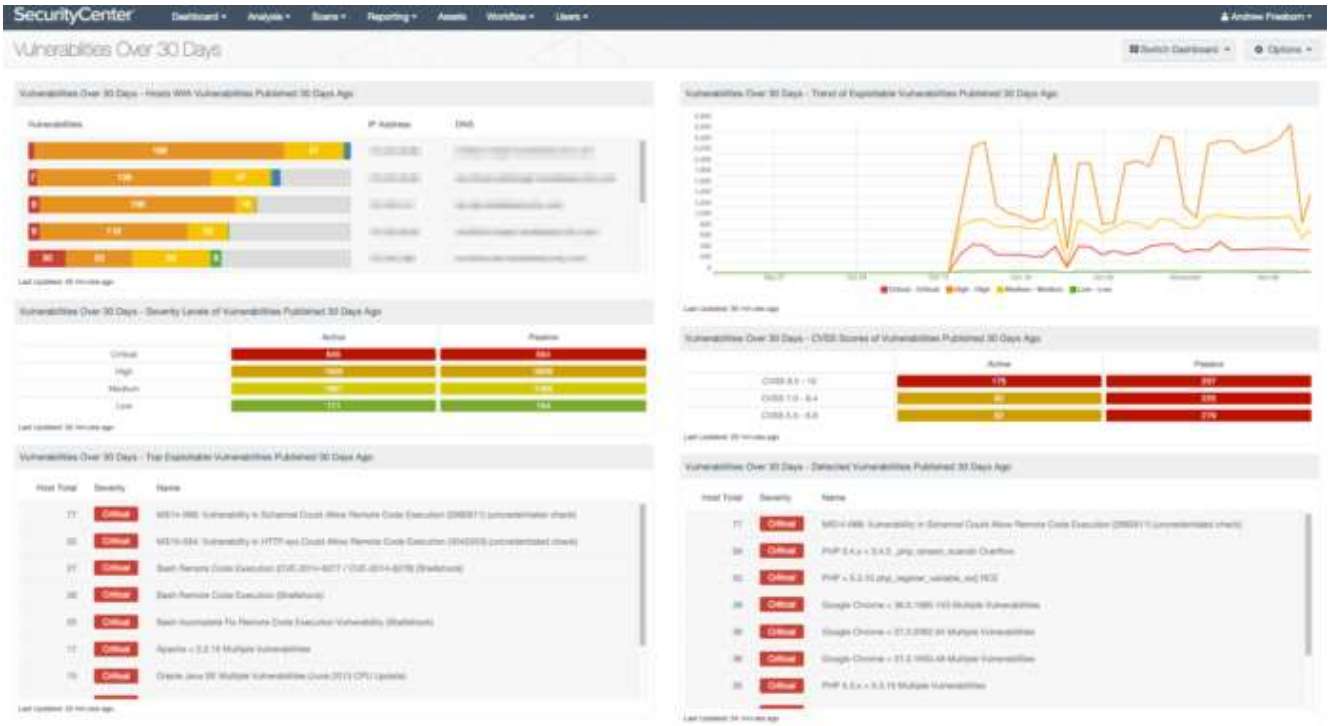

Рис. 1.11. Панель інструментів Tenable.io

Ключові диференціатори

Спільнота Tenable – це місце, де люди зі спільними інтересами в Tenable та управлінні вразливостями збираються разом та обмінюються ідеями.

Датчики Nessus в Tenable.io призначені для активного сканування та сканування агентів і пасивного моніторингу мережі, щоб забезпечити повну видимість від локального до хмари.

Завдяки даним про вразливості, науці про дані та аналізу загроз Tenable.io допомагає визначити, які вразливості мають найбільший вплив.

Інструмент відстежує динамічні IT-активи, такі як віртуальні машини, хмарні екземпляри та мобільні пристрої.

Користувачі можуть безперервно відстежувати мережевий трафік, щоб знаходити та оцінювати пристрої, які важко сканувати, і системи, які не працюють.

Хмарні з’єднувачі забезпечують безперервну видимість і оцінку в загальнодоступних хмарних середовищах через конектори для Microsoft Azure, Google Cloud Platform і Amazon Web Services (AWS).

Попередньо вбудовані інтеграції, API та ресурси SDK автоматизують робочі процеси та обмінюються даними Tenable.io з іншими сторонніми системами.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ НА ПРИКЛАДІ IBM QRADAR VULNERABILITY MANAGER

2.1. Визначення можливостей управління вразливостями в IBM QRadar Vulnerability Manager

У кібербезпеці управління інформацією та подіями безпеки (SIEM) вважається технологією, що відповідає за аналіз, зменшення загроз і реєстрацію подій безпеки у визначеній мережі. SIEM надає загальне уявлення про всю технічну інфраструктуру з конкретними даними про події безпеки та пом’якшення цих інфраструктур [6].

SIEM включає в себе такі функції, як управління інформацією про безпеку (SIM) і управління подіями безпеки (SEM), в єдине рішення. Щоб краще зрозуміти SIEM, подумайте про рішення, яке збирає дані з джерел безпеки для аналізу кореляції та дій щодо можливих загроз.

Керування SIEM пропонує різноманітні функції в таких областях [6]:

збирання подій і журналів;

кореляція правил;

керування джерелами журналів;

адаптивність;

нормалізація даних і реєстр.

Це рішення намагається вирішити сценарії, коли люди не можуть аналізувати передові загрози за допомогою звичайних інструментів моніторингу на загальному рівні, використовуючи технічну інфраструктуру бізнесу та об’єднуючи всі елементи, які зазвичай є агентами в ієрархічній моделі, для збору подій із кінцевих точок, серверів та мережевого обладнання. Він забезпечує взаємодію сторонніх розробників, завдяки чому можна інтегрувати багато рішень, що робить цей продукт масштабованим і більш надійним.

Piggeé описує рішення SIEM як «...групу складних технологій, які разом забезпечують інфраструктуру з висоти пташиного польоту» (Piggeé, 2016) [6].

QRadar є одним з найпопулярніших рішень SIEM на ринку сьогодні. Це платформа для управління мережею, яка забезпечує ситуаційну обізнаність, керування подіями та збереження даних на центральній консолі. Ця консоль нормалізує дані, співвідносить сигнатури, події та потоки та аналізує трафік на предмет будь-якої потенційної загрози в технічному середовищі.

QRadar використовує комбінацію знань мережі на основі потоків, кореляції подій та оцінки вразливості на основі активів.

QRadar надає наступні можливості з конкретними функціями:

активність журналу;

активність мережі;

активи;

порушення;

звіти;

збір даних;

правила QRadar SIEM.

Активність журналу. QRadar може відстежувати та відображати нормовані дані про події в режимі реального часу для виконання розширеного пошуку. Він також може досліджувати дані про події, шукати події, контролювати активність журналу та виявляти помилкові результати.

Активність мережі. Функція мережевої активності надає допомогу для дослідження зв’язку між двома хостами. Якщо рух захоплення вмісту ввімкнено, відображається інформація про те, як передається мережевий трафік і яка інформація була передана. Ця функція надає інформацію в режимі реального часу та контролює мережу за допомогою настроюваних графіків часу.

Активи. QRadar автоматично створює профілі активів, використовуючи дані пасивного потоку та дані про вразливості для виявлення мережевих серверів і хостів. Ці профілі надають інформацію про кожен відомий актив у вашій мережі, включаючи послуги, які вони запустили. Ця функція в основному

використовується для процесів кореляції правил і подій, щоб зменшити ймовірність хибнопозитивного результату.

Порушення. Порушення є продуктом правил, створених для того, щоб ініціювати дію, коли виконується декілька умов. Кожне правило можна налаштувати так, щоб фіксувати та реагувати на конкретну подію, послідовність подій, послідовність потоку або порушення. Порушення спрацьовує після виконання всіх умов, створених правилом і механізмом правил клієнта.

Звіти. Ви можете створювати власні звіти або використовувати звіти за замовчуванням із шаблонами, наданими самим QRadar. Ви можете налаштувати та змінити бренд цих пресетів, щоб вони розповсюджувалися всім користувачам консолі.

Збір даних. QRadar приймає інформацію в різних форматах із широкого спектру пристроїв, включаючи події безпеки, мережевий трафік та результати сканування. Усі зібрані дані розділені на три розділи:

збір даних про події;

збір даних про потік;

інформація про оцінку вразливості.

Колекція подій генерується з джерел журналів, таких як брандмауери, маршрутизатори, сервери, IDS або IPS. Збір даних потоку надає інформацію про мережевий трафік і може бути відправлений на QRadar у таких форматах:

файли Flowlog;

NetFlow;

J-Flow;

SFlow;

Packeteer.

Інформація про оцінку вразливості надходить із різних типів сканерів.

Правила QRadar SIEM. Правила створюються для виконання тестів подій, потоків або порушень. Якщо всі умови дотримані, правило спрацьовує і генерує відповідь або протидію. Ці дії можуть містити широкий спектр дій, включаючи надмірні заборони брандмауера, багаторазові помилки входу або потенційну

активність ботнету. Ви можете використовувати правило виявлення аномалій для виконання тестів. Потім ви можете використовувати результати збереженої інформації про потоки або пошуку подій, щоб виявити незвичайні моделі трафіку, які можуть виникнути в мережі, і подолати можливі загрози до того, як атака або зловмисний процес порушить цілісність технологічної інфраструктури.

Розглянемо архітектуру QRadar.

Коли ви плануєте інтегрувати або впровадити розгортання IBM Security QRadar у вашій мережі та інфраструктурі безпеки, завжди добре знати архітектуру QRadar, щоб побачити, як різні компоненти системи впливають на вашу мережу.

Ясність цих концепцій може полегшити процес планування, щоб ви могли інтегрувати систему IBM Security QRadar і скористатися перевагами, які продукт пропонує вашій організації.

Система IBM Security QRadar збирає, обробляє, об’єднує та зберігає мережеві дані в режимі реального часу. Він використовує ці дані для забезпечення безпеки вашої мережі, надаючи інформацію та кореляцію в реальному часі; система співвідносить усі події та потоки мережевої безпеки та генерує сповіщення та порушення, які може аналізувати ваша команда з безпеки мережі.

Щоб добре зрозуміти, як QRadar обробляє дані, які він отримує від мережевих пристроїв, добре розділити роботу системи IBM Security QRadar на три рівні:

рівень збору даних;

рівень обробки даних;

рівень дослідження даних.

Ця сегментація застосовується до будь-якої структури розгортання QRadar, незалежно від розміру, складності, кількості чи джерел журналів або модулів, які вона встановила чи приєднала до неї.

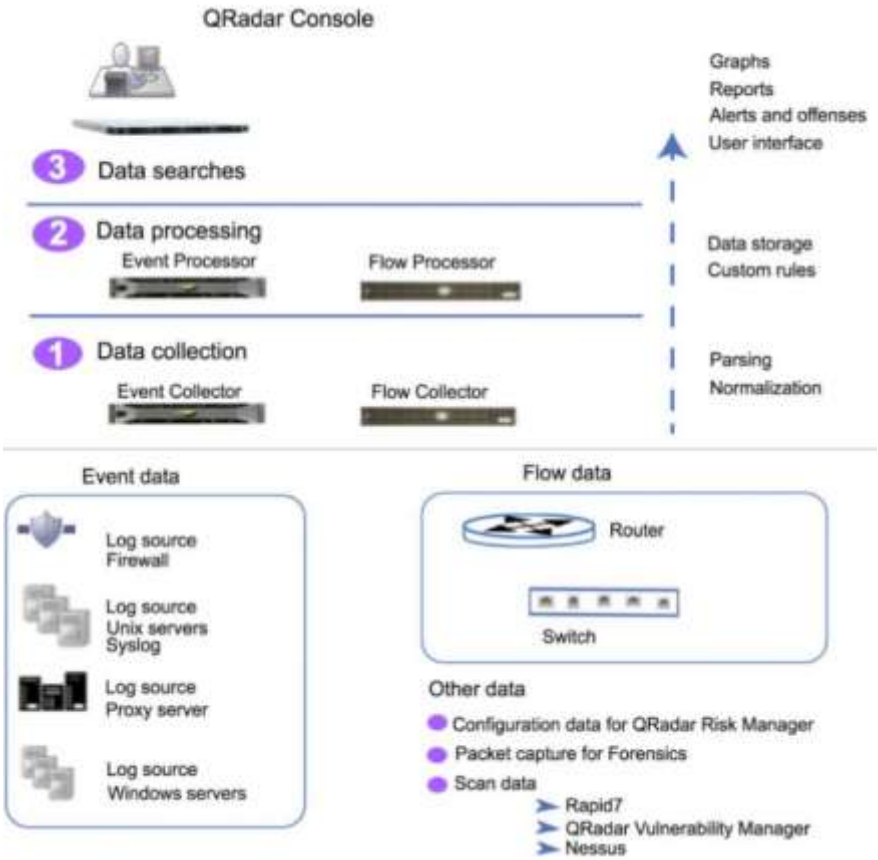

Рис. 2.1. Архітектура QRadar [6, 7]

Рівні, представлені на рис. 2.1, становлять основну функціональність будь-якої системи QRadar. Розуміння цих рівнів може забезпечити більш чітке розуміння того, як кожен з них сприяє обробці даних.

Збір даних. Збір даних є першим рівнем архітектури. На цьому рівні система QRadar отримує дані, такі як події та потоки, які вона отримує від мережевих пристроїв.

Ви можете використовувати пристрій QRadar All-In-One для збору даних безпосередньо з мережі, або адміністратор може використовувати колектори, наприклад QRadar Event Collector або QRadar Flow Collector, для збору даних про події чи потоки. Потім дані обробляються (розбираються та нормалізуються) перед тим, як вони потраплять на рівень обробки.

На додаток до збору інформації про потік за допомогою QRadar Flow Collector, повний захоплення пакетів доступний за допомогою компонента QRadar Incident Forensics.

Дані про події представляють події, які відбуваються в певний момент часу десь у мережі, як-от вхід користувачів, з'єднання VPN, заборони брандмауера, проксі-з'єднання та будь-які інші події, які можуть реєструватися на мережевих пристроях. З іншого боку, дані потоку – це інформація про мережеву активність або інформація про сеанс між двома хостами в мережі, яку система IBM QRadar перетворює в записи потоку. Іншими словами, QRadar перетворює або нормалізує необроблені дані в IP-адреси, порти, кількість байтових пакетів та іншу інформацію в записи потоку, які ефективно представляють сеанс між двома хостами.

Обробка даних. Після збору даних на другому рівні обробки даних система QRadar обробляє ці дані з компонентом Custom Rule Engine (CRE). Після того, як компонент CRE обробить дані, система може генерувати порушення та попередження, щоб потім записати або зберегти дані в сховищі.

Події та потоки можна обробляти за допомогою пристрою All-In-One без необхідності використання процесорів подій QRadar або процесорів потоків; однак, якщо потужність обробки перевищена, вам може знадобитися додати процесори подій або процесори потоку, щоб мати змогу обробляти навантаження. Вам також може знадобитися розгорнути вузли даних QRadar на випадок, якщо вам знадобиться більше місткості.

Інші функції, такі як QRM, QVM або QRadar Incident Forensics, дозволяють обробляти різні типи даних.

Пошук даних. На цьому рівні зберігаються дані, які були зібрані та оброблені системою, і їх можна використовувати для пошуку, звітів, сповіщень та розслідування порушень. Як випливає з назви, у системі All-In-One всі дані збираються, обробляються та зберігаються на одному пристрої.

У розподіленому середовищі консоль QRadar не збирає, обробляє або зберігає події та потоки. У цьому випадку він в першу чергу використовується для того, щоб користувачі мали можливість запускати пошуки, звіти, сповіщення та розслідування порушень.

Висока доступність QRadar. Як і з іншими інформаційними технологіями

та системами безпеки, важливо переконатися, що системи завжди доступні. У випадку такої важливої системи безпеки, як система IBM Security QRadar, завжди добре включати налаштування або рішення високої доступності (HA), щоб переконатися, що система завжди доступна для посилення безпеки мережевої інфраструктури.

Маючи рішення QRadar HA, система може продовжувати збирати, зберігати та обробляти дані про події та потоки, навіть якщо є збій апаратного чи програмного забезпечення.

Щоб система працювала в середовищі високої доступності, QRadar з'єднує основний хост високої готовності з вторинним хостом високої доступності та налаштовує віртуальний IP (VIP), щоб створити кластер високої готовності.

Розглянемо компоненти QRadar. Перш ніж почати розгляд різних компонентів QRadar, які ми можемо побачити в розподіленому середовищі, важливо пам'ятати, що всі пристрої повинні мати однакову версію програмного забезпечення, щоб система працювала правильно. На рисунку 2.2 показано пристрої, які можна знайти в розподіленому середовищі.

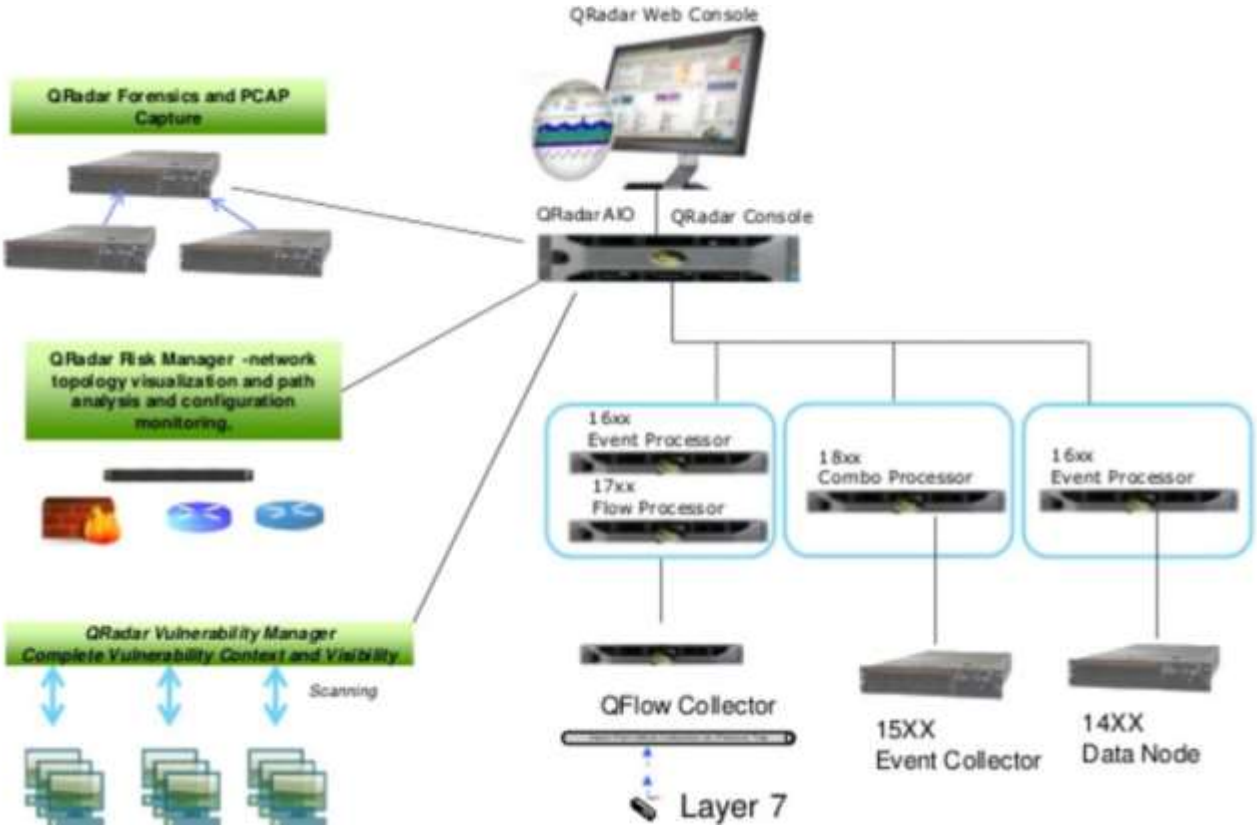

Рис. 2.2. Пристрої QRadar в розподіленому середовищі

Консоль QRadar надає інтерфейс користувача, де користувач може переглядати звіти, порушення, інформацію про активи та адміністративні функції. Його також можна використовувати для налаштування різних системних параметрів, створення та налаштування правил, щоб система могла генерувати порушення, а також для створення звітів відповідно до різних вимог, які може мати ваша компанія.

Колектор подій QRadar. Система збирання подій збирає події з різних джерел журналів, які можуть бути знайдені в мережі. Він також нормалізує отримані вихідні події у формат, який може використовуватися системою IBM Security QRadar для подальшої обробки даних.

Він об'єднує або поєднує ідентичні події, щоб зберегти або заощадити використання системи. Він також надсилає дані (необроблені та нормалізовані) до процесора подій QRadar для подальшої обробки даних.

Процесор подій QRadar. Події, які збираються одним або кількома компонентами збирача подій IBM Security QRadar або безпосередньо отримані з джерел журналів у мережі, обробляються процесором подій QRadar за допомогою механізму користувацьких правил (CRE). Якщо події відповідають користувацьким правилам CRE, які попередньо визначені на консолі, процесор подій виконує дії, визначені для конфігурації відповіді правила.

Зберігання даних відбувається на кожному процесорі подій або це також можна зробити за допомогою даних QRadar.

Вузли (якщо вони розгорнуті та налаштовані). Швидкість обробки визначається ліцензією EPS. Якщо швидкість EPS, визначена в ліцензії, перевищена, події буферизуються і залишаються в чергах джерела збирача подій, доки швидкість не знизиться. Якщо ви продовжуєте перевищувати ставку ліцензії EPS, а черга заповнена, система IBM Security QRadar скидає події та видає сповіщення або попередження, щоб повідомити про це.

Колектор QRadar QFlow. Збірник потоків збирає потоки, підключаючись до порту SPAN або мережевого TAP. Він також підтримує збір зовнішніх джерел даних на основі потоків, таких як Cisco NetFlow або Juniper J-Flow.

Колектори QRadar QFlow не призначені для повного захоплення пакетів. Якщо потрібно мати повну систему захоплення пакетів, ви можете розглянути варіант судової експертизи QRadar Incident Forensics.

Процесор потоку QRadar. Процесор потоку обробляє потоки з однієї або кількох систем QFlow Collector. Він також може збирати зовнішні потоки, такі як NetFlow, J-Flow і sFlow, безпосередньо з мережевих пристроїв.

Колектори подій не зберігають дані локально. Замість цього вони просто збирають і аналізують події, перш ніж відправити ці події на пристрій обробки подій, щоб вони там зберігалися.

Колектор подій успадковує ліцензію EPS Процесора подій, до якого він підключений. Коли процесор подій QRadar додається до системи All-In-One, функція обробки подій переміщується з пристрою All-In-One на новий процесор подій, який був доданий. Коли процесор потоку додається до пристрою «все в одному», обробка потоків переміщується з пристрою «все в одному» на процесор потоку.

Вузол даних QRadar. Вузли даних в основному використовуються для цілей зберігання; вони додають обсяги для зберігання та процесу за потребою. Вузли даних допоможуть збільшити швидкість пошуку під час розгортання, надавши більше апаратних ресурсів для виконання запитів.

Події та потоки QRadar. Основна відмінність між даними події та потоку полягає в тому, що подія відбувається в певний час і реєструється в цей час. Крім того, потік – це запис мережевих комунікацій, який може тривати секунди, хвилини, години або дні, залежно від активності в сеансі або зв’язку. Наприклад, коли ви виконуєте веб-запит, веб-клієнт може завантажити кілька файлів, таких як зображення, текст і відео, і це може тривати від 5 до 10 секунд. Іншим прикладом може бути, коли користувач дивиться фільм або відео. У цьому випадку сеанс мережі може тривати до кількох годин. Таким чином, потік – це запис мережевої активності між двома хостами.

IBM Security QRadar приймає журнали або події з різних джерел журналів, знайдених у мережі. Джерело журналу – це джерело даних, наприклад

брандмауер або пристрій IPS.

Система приймає журнали за допомогою кількох протоколів, таких як Syslog і SNMP. Він також може отримувати журнали, встановлюючи вихідні з'єднання для отримання подій через такі протоколи, як SCP, SFTP, JDBC та Checkpoint OPSEC.

Як згадувалося раніше, перш ніж ви зможете переглядати та використовувати дані про події на консолі QRadar, події збираються з джерел журналу, а потім обробляються системою процесора подій. Пам'ятайте, що у випадку багатофункціонального пристрою система працює як колектор подій, процесор подій і консоль одночасно.

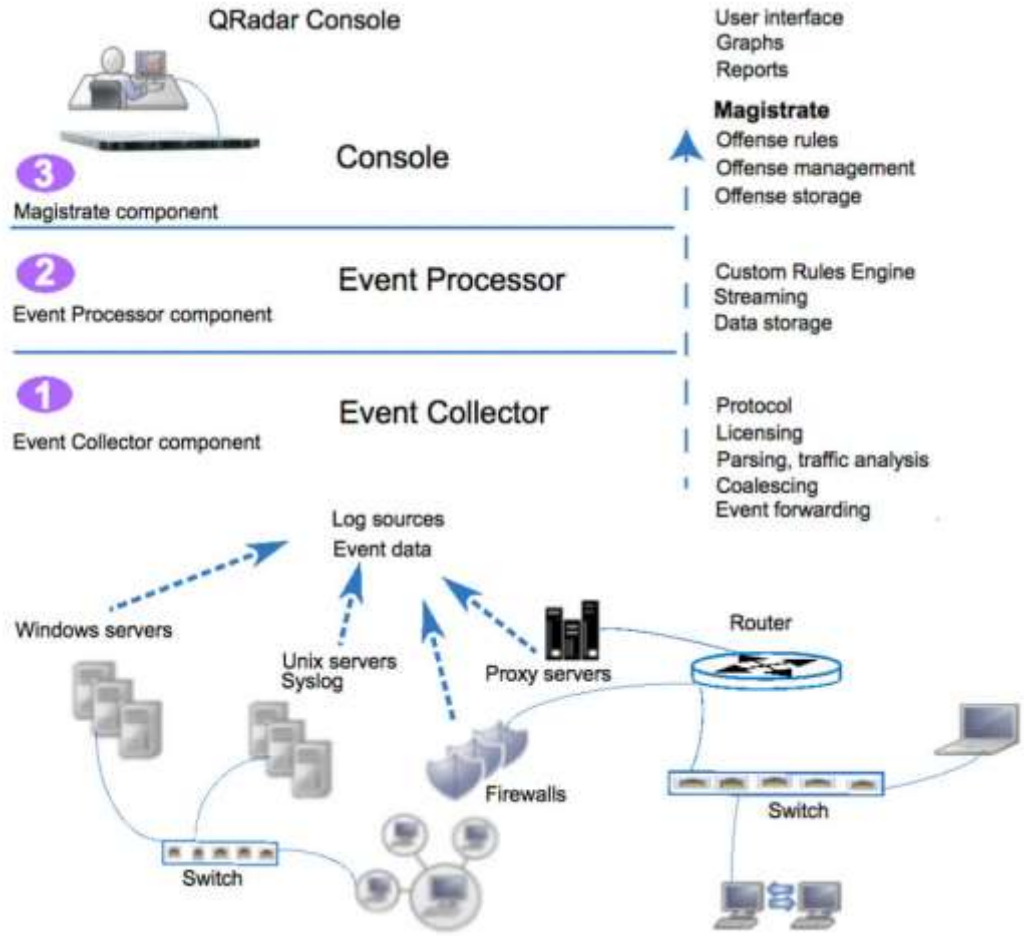

Рис. 2.3. Конвеєр подій QRadar [7]

Збирання подій. IBM Security QRadar Event Collector збирає дані з джерел журналів, використовуючи різні протоколи, які він підтримує. Він також

відповідає за моніторинг кількості вхідних подій для керування чергами введення та ліцензування EPS, яке обробляється процесом регулювання ліцензії. Він приймає вихідні події, отримані з джерел журналу, і аналізує поля у форматі QRadar.

IBM Security QRadar Event Collector також відповідає за аналіз трафіку джерела журналів і процеси автоматичного виявлення; він обробляє проаналізовані та нормалізовані дані про події з усіма DSM, які підтримують автоматичне виявлення.

Події аналізуються, а потім об’єднуються або об’єднуються на основі загальних атрибутів подій, це робиться за допомогою процесу об’єднання.

Колектор подій нарешті відповідає за пересилання подій. Він застосовує правила маршрутизації для системи для пересилання даних до зовнішніх цілей, зовнішніх серверів системного журналу та інших SIEM (якщо налаштовано для цього).

Коли колектор подій отримує події з різних джерел журналу, події передаються у черги введення для подальшої обробки. Розмір черги змінюється залежно від використовуваного протоколу або методу, і з цих черг події аналізуються та нормалізуються. Процес нормалізації – це в основному перетворення вихідних даних у формат, який має такі поля, як IP-адреси, які QRadar може використовувати.

Система IBM Security QRadar розпізнає відомі джерела журналів за IP-адресою джерела або іменем хоста, що міститься в заголовку. Це відомо як ідентифікатор джерела журналу.

QRadar обробляє (розбирає та об’єднує) події з джерел журналу в записи. Події з нових або невідомих джерел даних, які не були виявлені або автоматично налаштовані в минулому, передаються до механізму аналізу трафіку або механізму автоматичного виявлення.

Обробка подій. Компонент Процесор подій (Event Processor) відповідає за обробку подій, отриманих QRadar, і порівняння їх із визначеними правилами за допомогою Механізму спеціальних правил (Custom Rule Engine, CRE);

відстеження систем, залучених до інцидентів з часом, створення сповіщень для користувачів.

Коли події відповідають правилу, з Процесора подій до компонента Magistrate на консолі QRadar надсилається сповіщення, яке вказує, що конкретна подія ініціювала або вражала правило. Компонент магістрату відповідає за створення порушень і управління ними. Коли запускаються правила, генеруються відповіді або дії, такі як повідомлення, нові події системного журналу, пастки SNMP, повідомлення електронної пошти та порушення.

Процесор подій IBM Security QRadar також надсилає дані про події в режимі реального часу на консоль QRadar, коли користувач переглядає події на вкладці «Активність журналу» з режимом реального часу (потокова передача).

Потокові події не надаються з бази даних.

Колектор подій надсилає нормалізовані дані про події до процесора подій, де події обробляються засобом Custom Rules Engine (CRE). Якщо події відповідають користувацьким правилам CRE, які попередньо визначені на консолі QRadar, процесор подій виконує дію, визначену для відповіді правила.

Компонент магістрату відповідає за моніторинг та дії щодо порушень; він генерує дії, такі як надсилання сповіщень електронною поштою, створення правопорушень або будь-які дії, зазначені в правилі, якому відповідала подія. Він також відповідає за оновлення активних правопорушень, зміну статусів порушень та надання користувачам доступу до інформації про правопорушення з вкладки Порушень. Нарешті, він записує дані про порушення в базу даних Postgres, де вони зберігаються.

Ядро магістрату (Magistrate Processing Core, MPC) також відповідає за співвіднесення порушень із повідомленнями про події від кількох компонентів процесора подій. Майте на увазі, що компонент магістрату можна знайти лише на консолі QRadar.

Потоки. Потоки QRadar представляють мережеву активність шляхом нормалізації IP-адрес, портів, кількості байтів і пакетів та інших даних у записи потоків, які фактично є записами мережевих сеансів між двома хостами.

Компонент у QRadar, який збирає та створює інформацію про потік, відомий як QFlow.

Потік починається, коли Flow Collector виявляє перший пакет, який має унікальну IP-адресу джерела, IP-адресу призначення, порт джерела, порт призначення та інші специфічні параметри протоколу. Кожен новий пакет оцінюється тут. Кількість байтів і пакетів додається до статистичних лічильників у записі потоку. В кінці інтервалу запис статусу потоку надсилається на процесор потоку, а статистичні лічильники потоку скидаються.

Потік закінчується, якщо протягом налаштованого часу для потоку немає жодної активності.

QFlow може обробляти потоки з внутрішніх або зовнішніх джерел. Зовнішніми джерелами є такі джерела потоку, як NetFlow, sFlow і JFlow. Їх можна надіслати до спеціального колектора потоку або до процесора потоку, такого як пристрій QRadar Flow Processor 1705.

Зовнішні джерела не вимагають стільки обробки ЦП, оскільки кожен пакет не обробляється для побудови потоків. У цій конфігурації у вас може бути виділений колектор потоку та процесор потоку, які отримують і створюють дані потоку. У невеликих середовищах зі швидкістю менше 50 Мбіт/с пристрій «все в одному» може обробляти всю обробку даних.

Flow Collector також може збирати внутрішні потоки, використовуючи або підключаючись до порту SPAN або мережевого TAP. На рисунку 2.4 показано варіанти збору потоків у мережі.

Flow Collector генерує дані потоку з необроблених пакетів, які збираються з портів моніторингу, таких як SPAN, TAP і сеанси моніторингу, або із зовнішніх джерел потоку, таких як NetFlow, sFlow і JFlow. Ці дані перетворюються або упаковуються у формат потоку QRadar і передаються по конвеєру для обробки.

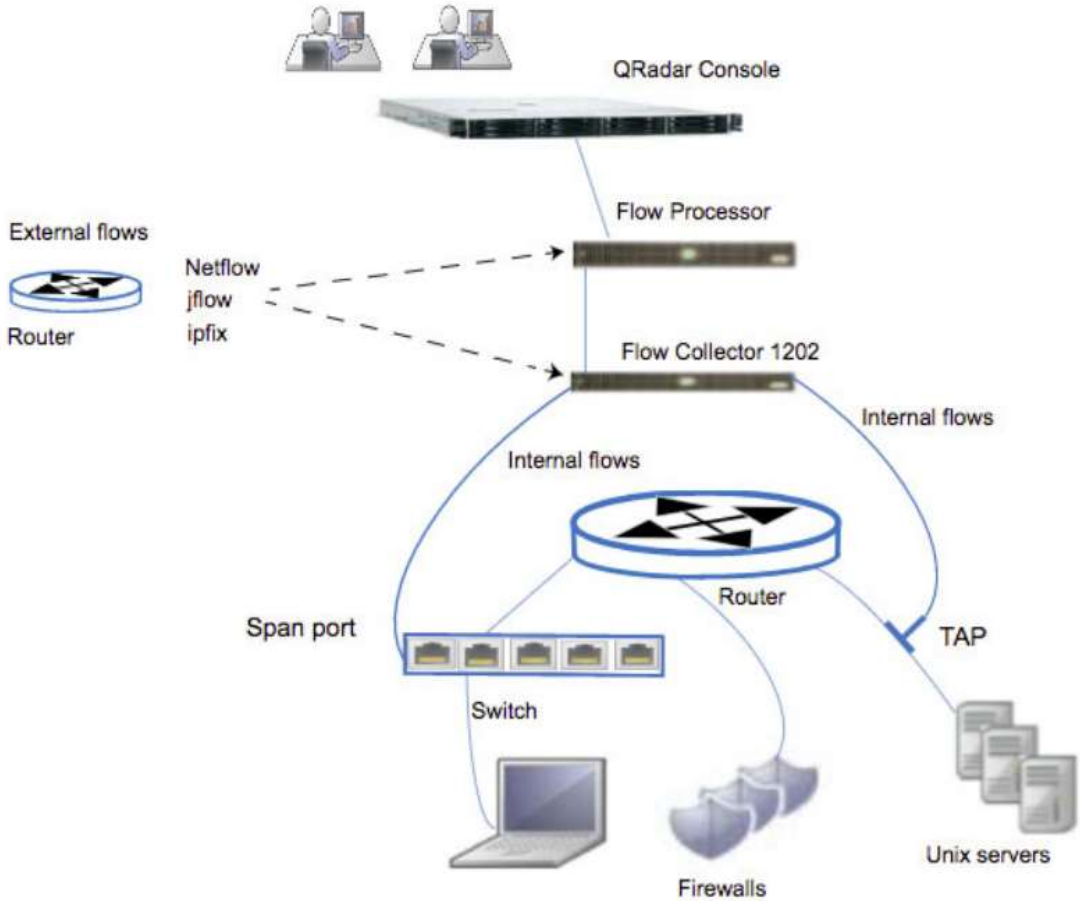

Рис. 2.4. Варіант збору потоків у мережі [7]

Процесор потоку відповідає за процес дедуплікації потоків, який видаляє повторювані потоки, коли кілька колекторів потоків надають дані пристроїв процесорів потоків. Він також поєднує дві сторони кожного потоку, коли дані надаються асиметрично. Цей процес виконується для того, щоб система могла розпізнавати потоки з кожного боку, а потім об'єднувати їх в один запис. Він відстежує кількість вхідних потоків у систему для керування чергами введення та ліцензуванням. Нарешті, він застосовує правила маршрутизації для системи, такі як надсилання даних потоку до зовнішніх цілей, зовнішніх систем Syslog, систем JSON та інших SIEM.

Дані потоку обробляються через Механізм користувацьких правил (CRE), вони співвідносяться та аналізуються з правилами, налаштованими в системі, щоб на основі цієї кореляції та обробки можна було створити правопорушення. Як згадувалося раніше, порушення можна переглянути на вкладці Порушення.

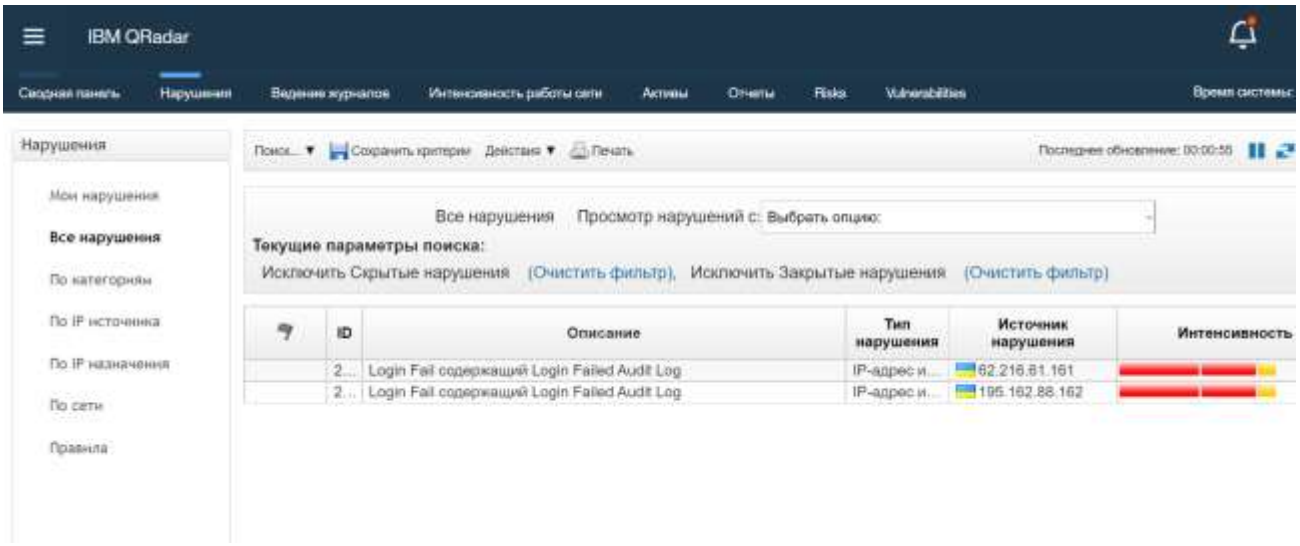

Рис. 2.5. Панель Порушення

2.2. Методи сканування вразливостей, які реалізовані в IBM QRadar Vulnerability Manager

IBM QRadar може інтегруватися з окремими пристроями, які можуть виконувати певні дії для розширення можливостей цих пристроїв.

IBM Security QRadar Vulnerability Manager (QVM) – це платформа мережевого сканування, яка виявляє вразливості в додатках, системах і пристроях у мережі. QRM використовує аналіз безпеки, щоб допомогти вам керувати вразливостями мережі та розставляти пріоритети [8].

Видимість вразливостей в режимі реального часу, які виявляються вбудованим сканером вразливостей QRadar та іншими сторонніми сканерами (Сканери сторонніх розробників інтегровані з QRadar і включають HCL BigFix, IBM Guardium, HCL AppScan, Nessus, nCircle, і Rapid 7) можна досягти.

QVM використовується для виконання таких завдань [8]:

постійного відстежування вразливостей;

покращення конфігурації ресурсу;

визначення виправлення програмного забезпечення.

встановлення пріоритетності недоліків у безпеці, співвідносячи дані про вразливості з мережевими потоками, даними журналів, брандмауером та даними

системи запобігання вторгненням (IPS);

планування сканування в зручний для ваших мережевих ресурсів час;

вказівки об’єктів, які потрібно виключити зі сканування, глобально або для кожного сканування;

налаштування автентифікованого сканування патчів для операційних систем Linux, UNIX або Windows;

налаштуваня різних протоколів сканування або визначення діапазонів портів, які потрібно сканувати.

У QVM скануванням вразливостей керують шляхом створення профілів сканування, які визначають активи, які необхідно перевіряти, і розклад сканування. Процесор уразливості також автоматично розгортається на консолі QRadar, коли купується ліцензія на QVM; процесор містить компонент сканування QVM.

QVM перевіряє декілька типів вразливостей у мережі, ці вразливості поділяються на такі широкі категорії:

ризиковані налаштування за замовчуванням: залишивши деякі налаштування за замовчуванням, ви можете зробити свою мережу вразливою для атак;

функції програмного забезпечення: деякі параметри програмного забезпечення для систем або програм призначені для покращення зручності використання, але ці параметри можуть створювати ризик для мережі;

неправильна конфігурація: Визначте неправильну конфігурацію в налаштуваннях за замовчуванням;

недоліки постачальника: це широка категорія, яка включає такі події, як переповнення буфера, проблеми з форматом рядка та міжсайтові сценарії.

QVM використовує комбінацію активних перевірок, які передбачають надсилання пакетів і віддалених зон, і пасивних перевірок кореляції. База даних QVM охоплює близько 70 000 вразливостей мережі, операційної системи та прикладного рівня. Ви можете здійснити пошук у повній бібліотеці сканування у вікні дослідження на вкладці Уразливості.

Тести QRadar Vulnerability Manager. Нижче наведено приклади деяких категорій, які перевіряє QRadar Vulnerability Manager:

перевірка маршрутизатора;

перевірки брандмауера;

перевірки бази даних;

перевірка веб-сервера;

перевірки сервера веб-додатків;

поширені перевірки веб-скриптів;

спеціальні перевірки веб-додатків;

перевірка DNS-сервера;

перевірки поштового сервера;

перевірки сервера програм;

перевірка безпроводової точки доступу4

загальні службові перевірки;

застаріле програмне забезпечення та системи.

IBM QRadar Vulnerability Manager визначає вразливості безпеки, додає контекст і допомагає визначити пріоритети заходів з усунення. Він використовує передову аналітику, щоб збагатити результати сканування уразливостей, щоб знизити ризик і досягти відповідності.

QRadar Vulnerability Manager співвідносить дані про вразливості з топологією мережі та даними підключення, щоб розумно керувати ризиками. Механізм політики автоматизує перевірку відповідності. Використання QRadar Vulnerability Manager може допомогти розробити оптимізований план дій для подолання ризиків безпеки, щоб працювати більш ефективно та зменшувати витрати. На рисунку 2.6 показано інформаційну панель QRadar Vulnerability Manager.

Рис. 2.6. Інформаційна панель QRadar Vulnerability Manager.

2.3. Варіанти розгортання системи управління вразливостями корпоративної інформаційної системи на базі IBM QRadar Vulnerability Manager

Ми можемо знаходити і керувати вразливостями корпоративної мережі, розгорнувши IBM QRadar Vulnerability Manager. Ми можемо підвищити безпеку мережі, інтегруючи додаткові функції, такі як HCL BigFix та IBM Security SiteProtector [9].

IBM QRadar Vulnerability Manager виявляє вразливості на корпоративних мережевих пристроях, додатках та програмному забезпеченні, додає контекст до вразливостей, визначає пріоритетність ризику активів у корпоративній мережі та підтримує усунення виявлених вразливостей.

Ми можемо інтегрувати QRadar Risk Manager для додаткового захисту, який забезпечує топологію мережі, активні шляхи атак і коригування показника ризику активів високого ризику для активів на основі відповідності політиці. QRadar Vulnerability Manager і QRadar Risk Manager об’єднані в одну пропозицію, і обидва доступні через єдину базову ліцензію.

Залежно від продукту, який встановлюється, і від того, чи оновлюєте IBM QRadar чи встановлюєте нову систему, вкладка «Вразливості» може не

відображатися. Доступ до IBM QRadar Vulnerability Manager за допомогою вкладки Вразливості. Якщо ви інсталюєте IBM QRadar SIEM, вкладка «Вразливості» за замовчуванням увімкнена з тимчасовим ліцензійним ключем. Якщо ви інсталюєте QRadar Log Manager, вкладка Вразливості не буде ввімкнено.

Ви можете скористатися опцією «Спробувати», щоб випробувати QRadar Vulnerability Manager протягом 30 днів. Ви можете придбати ліцензію на QRadar Vulnerability Manager окремо та увімкнути її за допомогою ліцензійного ключа.

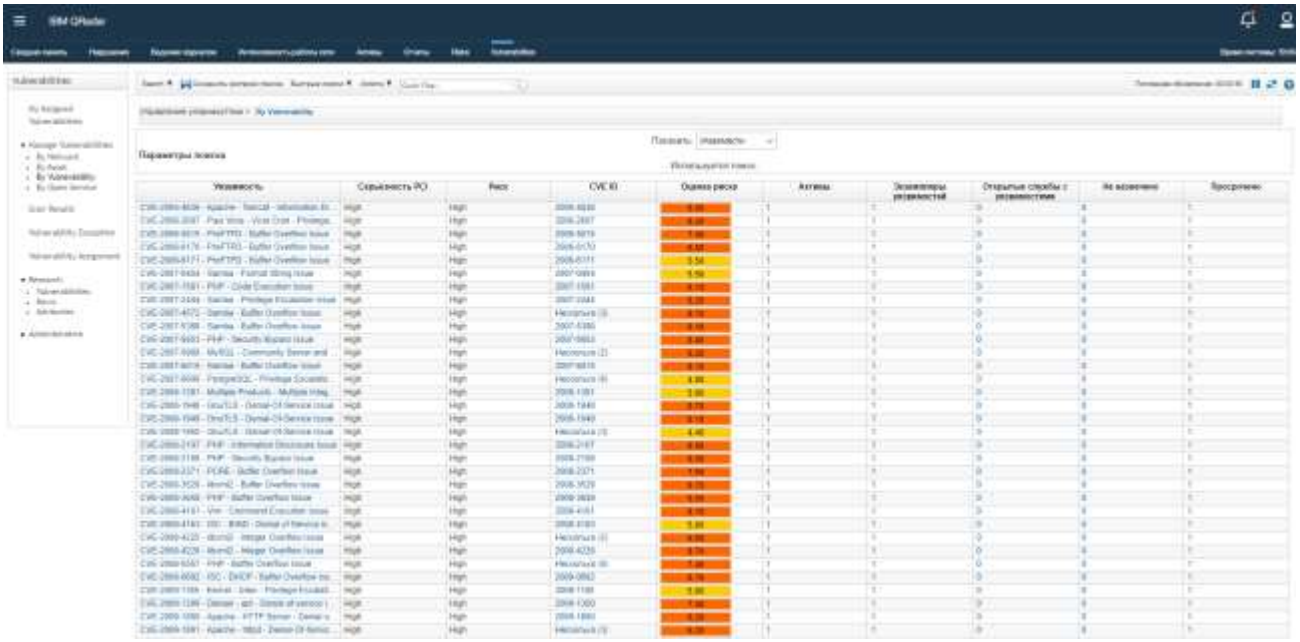

Рис. 2.7. Інструментальна панель QRadar Vulnerability Manager

Компоненти QRadar Vulnerability Manager

Процесор сканування відповідає за планування та керування скануваннями, а також за делегування роботи сканерам, які можуть бути поширені у корпоративній мережі [9].

У розгортанні QRadar можна мати лише один процесор сканування.

Коли ви встановлюєте та ліцензуєте QRadar Vulnerability Manager в системі All-in-One, процесор вразливостей автоматично розгортається на вашій консолі QRadar і включає компонент сканування.

За замовчуванням процесор вразливості забезпечує компонент сканування. Якщо потрібно, ви можете перемістити процесор вразливості на інший керований хост у вашому розгортанні.

Якщо ви додаєте керований хост-пристрій 600, і QRadar Vulnerability Manager використовується вперше, то процесор сканування призначається керованому хост-пристрою 600.

Процесор сканування керується ліцензією на обробку, яка визначає максимальну кількість активів, які можуть бути оброблені QRadar Vulnerability Manager.

Процесор сканування може працювати на консолі QRadar або на керованому хості.

Сканер QRadar Vulnerability Manager. Ви можете розгорнути сканер на віртуальній машині або лише як програмне забезпечення.

Ви можете розгорнути спеціальний сканер QRadar Vulnerability Manager, який є 610. Ви можете розгорнути сканер на консолі QRadar або на таких керованих хостах: Flow Collector, Flow Processor Event Collector, Event Processor або Data Node.

Кількість активів, які можна сканувати за допомогою сканера, визначається потужністю сканера і на нього не впливає ліцензування.

Розгортання «все в одному». Ви можете запустити QRadar Vulnerability Manager із системи «все в одному», де функції сканування та обробки знаходяться на консолі. Наведена нижче інформація описує, що можна зробити за допомогою базового налаштування [9]:

сканувати до 255 ресурсів;

необмежена кількість сканувань для виявлення;

використовувати розміщений сканер для сканування DMZ;

керувати даними сканування зі сторонніх сканерів, інтегрованих з QRadar;

розгорнути сканер на будь-якому керованому хості;

розгорнути необмежену кількість автономних програм або віртуальних сканерів.

Розширення розгортання. У міру розгортання вам може знадобитися перемістити функцію обробки з консолі QRadar, щоб звільнити ресурси, і ви можете розгорнути сканери ближче до своїх активів.

У наведеному нижче списку описано, чому потрібно додати сканери до свого розгортання [9]:

щоб сканувати активи в іншому географічному регіоні, ніж процесор QRadar Vulnerability Manager;

якщо ви хочете сканувати багато активів одночасно за короткий проміжок часу;

ви можете додати сканер, щоб уникнути сканування через брандмауер, який є джерелом журналу. Ви також можете розглянути можливість додавання сканера безпосередньо до мережі, додавши інтерфейс на хост сканера, який обходить брандмауер. На рисунку 2.8 показано розгортання сканування із зовнішнім скануванням і сканерами, розгорнутими на керованих хостах.

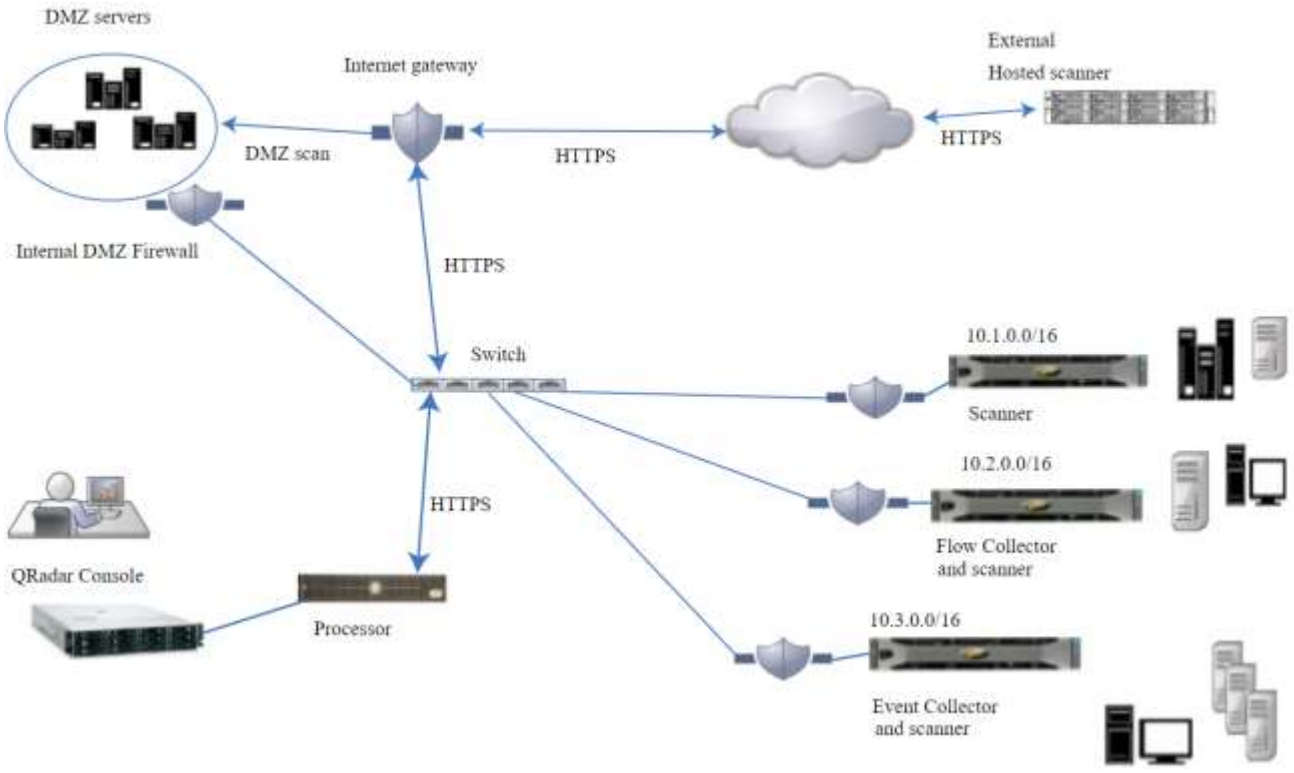

Рис. 2.8. Розгортання сканування із зовнішнім скануванням і сканерами, розгорнутими на керованих хостах [9]

Сканер, розміщений у DMZ. Розміщений сканер сканує вашу DMZ з Інтернету, використовуючи вашу загальнодоступну IP-адресу. Якщо ви хочете перевірити активи в DMZ на наявність вразливостей, вам не потрібно розгортати сканер у вашій DMZ. Ви повинні налаштувати QRadar Vulnerability Manager з розміщеним сканером IBM, який знаходиться поза межами вашої мережі.

Інтеграція QRadar Vulnerability Manager. IBM QRadar Vulnerability Manager інтегрується з HCL BigFix, щоб допомогти вам відфільтрувати та визначити пріоритетність вразливостей, які можна виправити. BigFix забезпечує спільну видимість і контроль між IT-операціями та безпекою. BigFix застосовує Fixlets до високопріоритетних вразливостей, які ідентифіковані та надіслані QRadar Vulnerability Manager до BigFix. Фікслети – це пакети, які ви розгортаєте на своїх ресурсах або кінцевих точках для усунення певних вразливостей.

QRadar Vulnerability Manager інтегрується з IBM Security SiteProtector, щоб допомогти спрямувати політику системи запобігання вторгненням (IPS). Коли ви налаштовуєте IBM Security SiteProtector, вразливості, виявлені скануванням, автоматично пересилаються до IBM Security SiteProtector. IBM Security SiteProtector отримує дані про вразливості від сканувань QRadar Vulnerability Manager, які запускаються лише після налаштування інтеграції.

QRadar Vulnerability Manager забезпечує ефективну платформу керування вразливостями, незалежно від джерела даних сканування. QRadar Vulnerability Manager легко інтегрується зі сторонніми сканерами, такими як Nessus, nCircle і Rapid 7.

Вам потрібно сканувати QRadar Vulnerability Manager, щоб отримати наступні параметри [9]:

сканування на основі подій і на вимогу;

сканування бази даних активів і списку спостереження;

сканування з наявних пристроїв QRadar і керованих хостів;

виявлення нещодавно опублікованих вразливостей, яких немає в результатах сканування.

Вам потрібен QRadar Risk Manager, щоб отримати наступні параметри:

управління вразливістю на основі активів, вразливостей і трафіку;

відкориговані показники вразливості та оцінка ризику з урахуванням контексту.

IBM QRadar Vulnerability Manager надає кілька типів політики сканування за замовчуванням. Ви також можете визначити власні сканування з шаблонів сканування.

Для виконання наведених нижче операцій сканування необхідно мати належні ліцензійні можливості. Наступні шаблони сканування є найбільш часто використовуваними шаблонами [8]:

Політика сканування виявлення. Виявляє мережеві активи, а потім сканує порти, щоб визначити ключові характеристики активів, такі як операційна система, тип пристрою та служби. Уразливі місця не перевіряються.

Легке сканування без облікових даних, яке шукає в адресному просторі активні IP-адреси, а потім сканує їхні порти. Він виконує пошук DNS і NetBIOS, щоб виявити операційну систему, відкриті служби та мережеві імена.

Якщо можливо, запускайте це сканування без облікових даних щотижня, щоб забезпечити хорошу видимість мережі. Це сканування є найкориснішим для виявлення нових об’єктів та змін до раніше відсканованих об’єктів.

Політика повного сканування. Виявляє мережеві ресурси, використовуючи діапазон портів швидкого сканування. Запускає настроюване користувачем сканування портів і неавтентифіковане сканування знайдених служб, таких як FTP, Інтернет, SSH і база даних. Автентифіковане сканування запускається, коли надаються облікові дані.

Запускає повний набір тестів QRadar Vulnerability Manager.

Повне сканування має такі етапи:

сканування виявлення;

сканування без облікових даних. Перевіряє служби, які не вимагають облікових даних, наприклад, читання банерів і відповідей на інформацію про версії, закінчення терміну дії сертифіката SSL, тестування облікових записів за замовчуванням і тестування відповідей на наявність вразливостей;

сканування облікових даних. QRadar Vulnerability Manager входить до активу та збирає інформацію про інвентарний список встановлених програм і необхідну конфігурацію, а також підвищує або пригнічує вразливості. Сканування облікових даних переважніше, ніж сканування без облікових даних. Сканування без акредитації дають корисний огляд уразливості мережі. Однак для комплексної та ефективної програми управління вразливістю необхідне сканування облікових даних.

Ви не можете редагувати вбудовані політики, але можете скопіювати їх, щоб створити свою власну політику сканування.

Політика сканування виправлень. Розвідує мережу, щоб виявити активи, а потім виконує швидке сканування портів та облікових даних активів.

Ви використовуєте сканування виправлень, щоб визначити, які виправлення та продукти встановлені чи відсутні в мережі.

Сканування патчів складається з двох основних етапів:

сканування виявлення;

сканування облікових даних.

Запустіть це акредитоване сканування кожні 1–4 тижні, щоб визначити, які виправлення та продукти встановлені або відсутні у вашій мережі. Сканування патчів створює лише мінімальне навантаження на вашу мережу, а активне тестування тримається на низькому рівні.

Політика сканування PCI. Сканує всі порти TCP та UDP 0-65535. Вам не потрібно сканувати всі порти UDP на відповідність PCI. Зазвичай ви скануєте найпоширеніші порти UDP на відповідність PCI, але список портів з часом може дещо змінюватися відповідно до стандартів безпеки PCI.

Якщо ви проскануєте всі порти UDP, перевірка може зайняти тривалий час і не завершитися протягом періоду очікування на великих сегментах мережі, що призведе до деяких екземплярів вразливості «Виявлено перешкоди сканування – сканування потенційно неповне ».

Ви можете створити власну політику сканування PCI, скопіювавши цю політику, перейменувавши політику та змінивши порти сканування UDP

відповідно до ваших вимог.

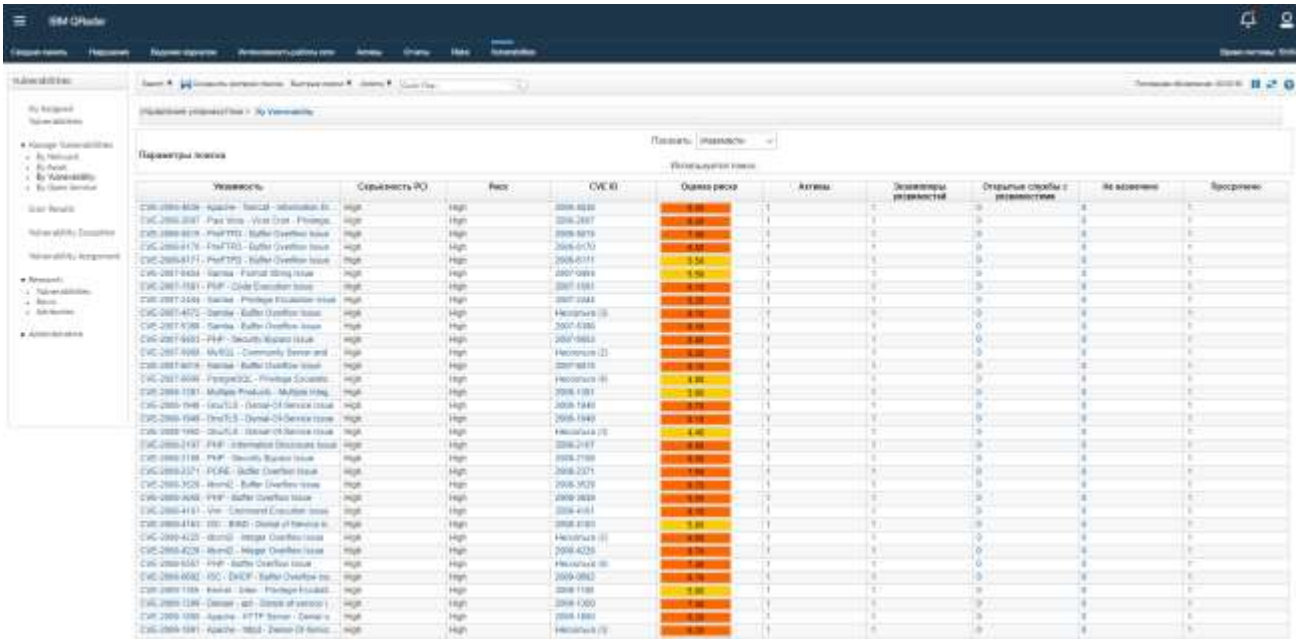

Рис. 2.9. Загальний звіт по наявним вразливостям активів

Політика сканування бази даних. Сканує порти бази даних 523, 1433, 1521 і 3306 на пошук популярних служб баз даних. Використовуйте сканування бази даних без облікових даних для сканування портів DB2 (523), Microsoft SQL (1433), MySQL (3306), Oracle (1521) і Informix (1526) для популярних служб баз даних. Регулярно виконуйте це сканування, якщо у вас висока активність бази даних.

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1. Алгоритм сканування з використанням QRadar Vulnerability Manager

IBM QRadar Vulnerability Manager виявляє вразливості на ваших мережевих пристроях, програмах та програмному забезпеченні, додає контекст до вразливостей, визначає пріоритетність ризику активів у вашій мережі та підтримує усунення виявлених вразливостей [9].

Завдання сканування виконуються процесором і компонентом сканера. На наступній схемі (рисунок 3.1) показано компоненти сканування та запущені процеси. Розглянемо їх більш детальніше.

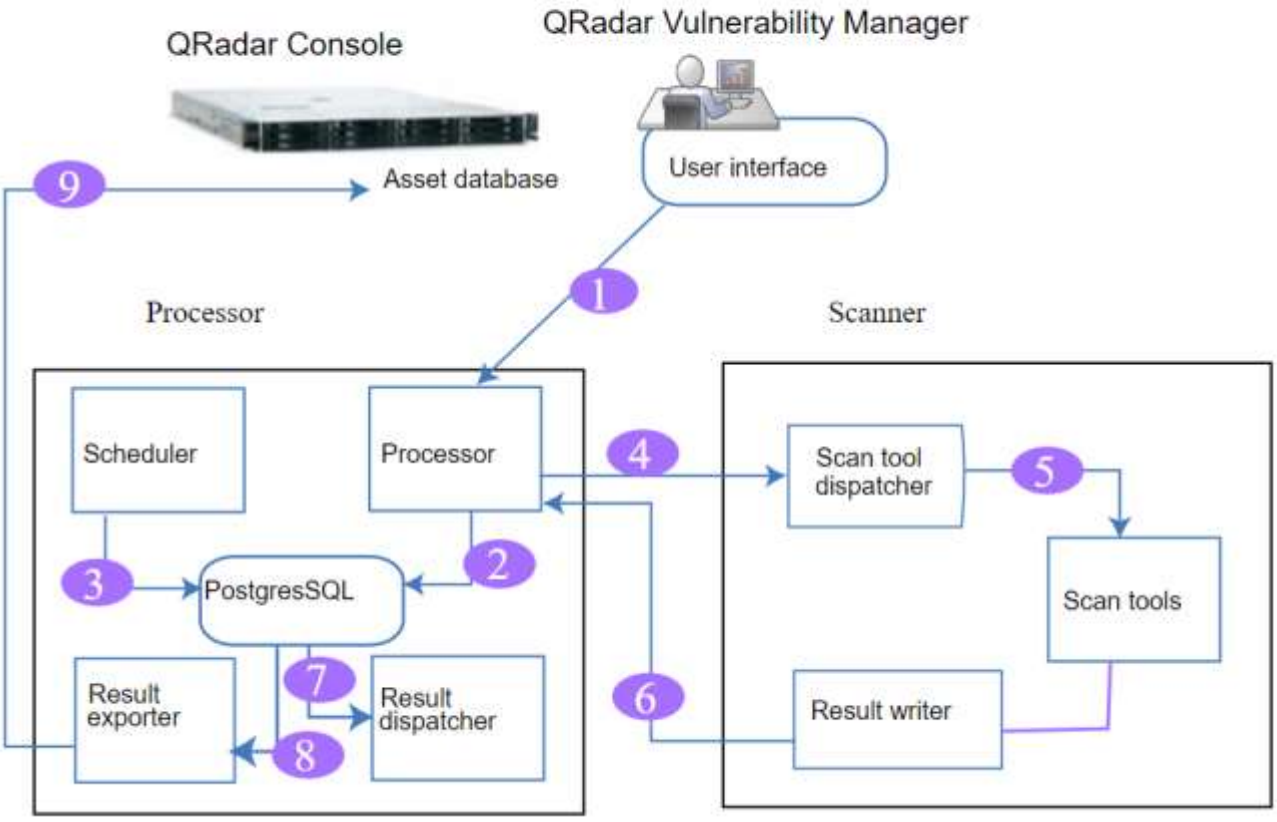

Рис. 3.1. Компоненти та процес сканування

Алгоритм процесу сканування вразливостей з використанням QRadar Vulnerability Manager складається з наступних кроків [9]:

1. Ви створюєте завдання сканування, вказуючи такі параметри, як IP-адреси активів, тип сканування та необхідні облікові дані для автентифікованого сканування.

2. Завдання сканування приймається процесором, реєструється та додається до бази даних разом з інформацією про планування, щоб визначити, коли завдання виконується.

3. Компонент планувальника керує плануванням сканування. Коли планувальник ініціює сканування, він визначає список необхідних інструментів і ставить їх у чергу для виклику, а потім інструменти призначаються відповідному сканеру.

4. Сканери постійно опитують процесор сканування щодо інструментів сканування, які він повинен запустити, надсилаючи унікальний ідентифікатор сканера. Коли планувальник має в черзі інструменти, які мають відношення до конкретного сканера, інструменти надсилаються до сканера для виклику.

QRadar Vulnerability Manager використовує методологію дерева атак для керування скануваннями та визначення інструментів, які запускаються. Етапи: виявлення активів, виявлення порту/служби, сканування служби та сканування виправлення.

5. Диспетчер запускає та керує кожним інструментом сканування у списку. Для кожного запущеного інструменту диспетчер надсилає процесору повідомлення, яке вказує, коли інструмент сканування запускається та закінчується.

6. Результати інструменту сканування зчитуються записувачем результатів, який потім передає ці результати назад до процесора.

7. Диспетчер результатів обробляє вихідні результати з інструментів сканування та записує їх у базу даних Postgres.

8. Експортер результатів знаходить завершені сканування в базі даних процесора та експортує результати на консоль QRadar.

9. Експортовані результати додаються до бази даних QRadar, де користувачі можуть переглядати та керувати результатами сканування.

Адміністратори можуть налаштувати сканування такими способами:

запланувати сканування в зручний для ваших мережевих ресурсів час;

вказати час, протягом якого сканування заборонено виконувати;

вказати об’єкти, які потрібно виключити зі сканування, глобально або для кожного сканування;

налаштувати автентифіковане сканування патчів для операційних систем Linux, UNIX або Windows;

налаштувати різні протоколи сканування або вкажіть діапазони портів, які потрібно сканувати.

IBM QRadar Vulnerability Manager перевіряє декілька типів уразливостей у вашій мережі. Уразливості поділяються на такі широкі категорії:

небезпечні налаштування за замовчуванням;

особливості програмного забезпечення;

неправильна конфігурація;

недоліки постачальника.

Залишивши деякі *налаштування за замовчуванням*, ви можете зробити свою мережу вразливою для атак. Нижче наведено приклади, які можуть зробити вашу мережу вразливою:

залишити зразки сторінок або сценаріїв під час встановлення IIS;

не змінювати пароль за замовчуванням на 3Com Hub/Switch;

залишити «загальнодоступне» або «приватне» як назву спільноти SNMP на пристрої з підтримкою SNMP;

не встановлюється пароль для входу SA на сервер MS-SQL.

Особливості програмного забезпечення. Деякі параметри програмного забезпечення для систем або програм призначені для зручності використання, але ці параметри можуть створювати ризик для вашої мережі. Наприклад, протокол Microsoft NetBIOS корисний у внутрішніх мережах, але якщо він відкритий для Інтернету або ненадійного сегмента мережі, він створює ризик для вашої мережі.

Нижче наведено приклади програмних функцій або команд, які можуть піддати вашу мережу ризику:

запити на мітку часу або маску мережі ICMP;

розгорніть або перевірте команди Sendmail;

служби протоколу ідентифікації, які ідентифікують власника запущеного процесу.

Неправильна конфігурація. На додаток до виявлення неправильних конфігурацій у налаштуваннях за замовчуванням, QRadar Vulnerability Manager може виявити більш широкий діапазон неправильних конфігурацій, наприклад у таких випадках:

ретрансляції SMTP;

необмежений доступ до файлів NetBIOS;

перенесення зон DNS;

світові доступні для запису каталоги FTP;

облікові записи адміністрування за замовчуванням, які не мають паролів;

експортовані каталоги NFS World.

Недоліки постачальника – це широка категорія, яка включає такі події, як переповнення буфера, проблеми з форматом рядка, переміщення каталогів і міжсайтові сценарії. Уразливості, які вимагають виправлення або виправлення оновлення, включені до цієї категорії.

QRadar Vulnerability Manager використовує комбінацію активних перевірок, які передбачають надсилання пакетів і віддалених перевірок, і пасивних перевірок кореляції. База даних QRadar Vulnerability Manager охоплює приблизно 70 000 вразливостей мереж, ОС та прикладного рівня.

Ви можете здійснити пошук у повній бібліотеці сканування за CVE, діапазоном дат, назвою постачальника, назвою продукту, версією продукту та назвою ризику у вікні «Дослідження » на вкладці «Вразливості».

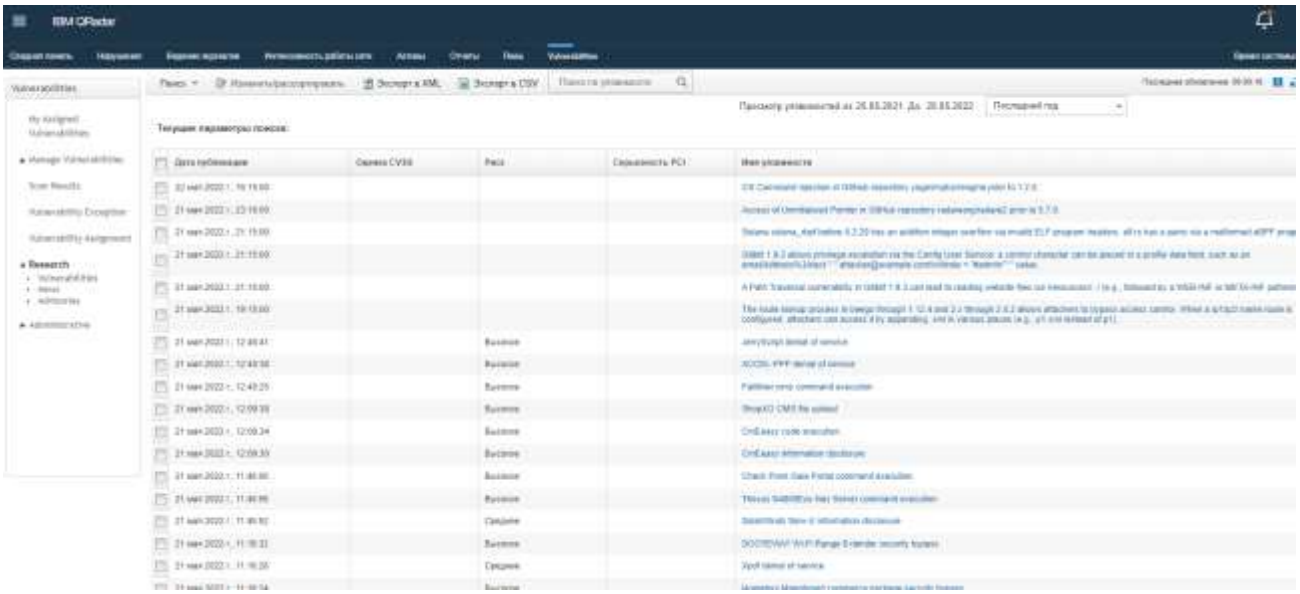

Рис. 3.2. Панель «Дослідження » на вкладці «Вразливості».

Приклади деяких категорій, які перевіряє QRadar Vulnerability Manager:

перевірки бази даних;

перевірка веб-сервера;

перевірки сервера веб-додатків;

поширені перевірки веб-скриптів;

спеціальні перевірки веб-додатків;

перевірка DNS-сервера;

перевірки поштового сервера;

перевірки сервера програм;

перевірка бездротової точки доступу;

загальні службові перевірки;

застаріле програмне забезпечення та системи.

Ви можете відобразити інформацію про вразливості на інформаційній панелі QRadar (рис. 3.3).

IBM QRadar Vulnerability Manager поширюється з панеллю керування вразливостями за замовчуванням, щоб ви могли швидко переглянути ризики для вашої організації.

Ви можете створювати нову інформаційну панель, керувати наявними інформаційними панелями та змінювати параметри відображення кожного

елемента інформаційної панелі про вразливості.

Рис. 3.3. Інструментальна панель «Управління вразливостями»

3.2. Рекомендації щодо управління вразливостями корпоративних інформаційних систем

Фахівці з кібербезпеки давно знають про важливість усунення вразливостей у своїх IT-середовищах. У звітах постійно вказується, що невиправлені відомі вразливості залишаються одним з головних векторів атак [10].

Досвідчені лідери в галузі безпеки погоджуються з тим, що *управління вразливістю не повинно здійснюватися на разовій основі або за допомогою неформальних методів.* Швидше, це має відбуватися програмно, щоб забезпечити дії, підзвітність та постійне вдосконалення [10].

Використовуючі поради експертів з безпеки в [10] сформулюємо рекомендації для створення програми управління вразливістями корпоративних інформаційних систем.

По-перше, необхідно створити команду фахівців, які будуть займатися управлінням вразливістю та встановленням виправлень, До цієї команди треба залучити інших ключових зацікавлених осіб, таких як співробітники бізнес-

підрозділів, які можуть розповісти про вплив, з яким стикається організація, коли системи відключаються для перезавантаження, щоб команда могла розуміти, як їхня робота впливає на інших.

По-друге, треба постійно вести наявний перелік активів. Ще одним основним елементом будь-якої ефективної програми управління вразливістю є актуальна інвентаризація активів із процесом, що гарантує, що вона залишається максимально актуальною та повною. Це складне питання в сучасних швидко мінливих середовищах з їхніми фізичними елементами, віддаленими підключеннями співробітників та компонентами IoT, а також хмарними технологіями, SaaS та елементами з відкритим вихідним кодом.

По-третє, необхідно забезпечити «видимість» корпоративної мережі для розуміння взаємозв'язків вашого середовища, де знаходяться потоки даних та інтеграції.

По-четверте, необхідно проводити періодичне сканування корпоративної мережі. Сканування вразливостей – ще один основний елемент надійної програми кібербезпеки, проте експерти кажуть, що багато організацій, які регулярно проводять сканування, як і раніше, не можуть виявити проблеми, тому що вони недостатньо ретельні.

Отже, у високопродуктивних програмах управління вразливістю використовуються агресивніші методи сканування, що включають кілька варіантів. Команди повинні включати сканування з обліковими даними для більш ретельного пошуку слабких конфігурацій і відсутніх виправлень на додаток до сканування, що часто використовується, на основі агентів і сканування мережі.

По-п’яте, необхідно продумати та задокументувати робочі процеси, визначити як їх проводити та хто відповідальний. Команди повинні розробити загальну операційну картину, при якій одні й ті самі дані та відомості про загрози мають бути доступні всім членам команди, які працюють над управлінням уразливістю.

По-шосте, необхідно встановити та відстежувати ключові показники ефективності KPI (Key Performance Indicators). Це потрібно для підтвердження

ефективності ваших засобів контролю та довести керівництву, що вони ефективні, корисно мати показники, які повідомляють про продуктивність вашої програми управління вразливістю.

Організації можуть застосовувати будь-який з ключових показників ефективності, що широко використовуються, наприклад, відсоток критичних уразливостей, усунених під час, та відсоток критичних уразливостей, не усунених вчасно, для вимірювання поточного стану та відстеження поліпшень з часом.

Інші KPI, які можна використовувати, можуть включати відсоток інвентаризованих активів, час виявлення, середній час відновлення, кількість інцидентів через вразливість, швидкість повторного відкриття вразливостей та кількість наданих винятків.

По-сьоме, необхідно визначити орієнтири. Відстеження ключових показників ефективності може показати, чи покращується ваша власна програма управління вразливістю з часом, але вам потрібно буде порівняти зусилля інших компаній, щоб визначити, чи перевершує ваша програма інші, чи відстає від них.

Бенчмаркінг (орієнтир) допомагає вам зрозуміти, наскільки ви ефективні в порівнянні з колегами та конкурентами, а також дає керівництву впевненість у тому, що ваша програма управління вразливістю ефективна.

По-восьме, треба визначити та призначити відповідального. Багато експертів кажуть, що для того, щоб мати справжню програму управління вразливістю, організації повинні покласти на когось відповідальність за свою роботу і, зрештою, за свої успіхи та невдачі.

По-дев’яте, необхідно запровадити систему стимулів за покращення програми та успіхі.

По-десяте, створіть програму винагороди за виявлення помилок. Як приклад, у 2021 році Salesforce винагородила етичних хакерів більш ніж на 2,8 мільйона доларів за виявлення проблем безпеки у своїх продуктах, розглядаючи цю нагороду за виявлення помилок як важливу частину управління вразливістю.

По-одинадцяте, переконайтеся у своїх очікуваннях, але з часом коригуйте їх. Кількість публічно розкритих недоліків безпеки у списку загальних

уразливостей та загроз (CVE) продовжує зростати, а кількість нових, що додаються щороку, збільшувалася майже щороку протягом останнього десятиліття. У 2011 р. було 4813 CVE; згідно з аналізом Kenna Security, у 2020 році їх було 11463 [10].

Враховуючи обсяг, експерти погоджуються, що організації мають розставити пріоритети, які вразливості становлять найбільший ризик, щоб вони могли усунути їх насамперед.

По-дванадцяте, запровадити систему звітів про результативність програми перед заінтересованими сторонами. Експерти кажуть, що окрім інформування зацікавлених сторін усередині організації про будь-які роботи з встановлення виправлень, які можуть вплинути на їх доступ до систем, команда безпеки повинна звітувати про загальну продуктивність програми управління вразливістю з точки зору бізнесу, пов'язаної з ризиками та їх зниженням.

ВИСНОВКИ

В роботі досліджено проблему управління вразливостями корпоративних інформаційних систем. Управління вразливостями – це ефективне рішення безпеки, яке допомагає виявляти вразливості в мережах, додатках, процесах і програмному забезпеченні та усувати їх. Управління вразливостями – це процес виявлення вразливостей у середовищі, оцінки ризиків, пов’язаних з ними, та вжиття відповідних заходів для їх зменшення.

Досліджено зміст управління вразливостями корпоративної інформаційної системи. Управління вразливістю базується на виявленні та реагуванні, що становить основу кібербезпеки, якої потребують сучасні гібридні, динамічні та розподілені корпоративні середовища. Це безперервний, безперебійно організований робочий процес з автоматизованого виявлення активів, керування вразливостями, визначення пріоритетів загроз та їх усунення. Впроваджуючи життєвий цикл управління вразливостями, організації зменшують ризики компрометації, ефективно запобігаючи порушенням та швидко реагуючи на загрози.

Проаналізувано існуючі методи та засоби управління вразливостями на прикладі IBM QRadar Vulnerability Manager. IBM QRadar Vulnerability Manager – це платформа для мережевого сканування, яка виявляє вразливості в додатках, системах і пристроях у корпоративній мережі або в DMZ. QRadar Vulnerability Manager використовує аналіз безпеки, щоб допомогти фахівцям керувати вразливостями корпоративної мережі та визначити їх пріоритетність.

Розглянуто варіанти системи управління вразливостями корпоративної інформаційної системи з використанням IBM QRadar Vulnerability Manager. Розглянуто розгортання IBM QRadar Vulnerability Manager для сканування із зовнішнім скануванням і сканерами, розгорнутими на керованих хостах.

Розглянуто алгоритм сканування з використанням QRadar Vulnerability Manager.

Розроблено рекомендації керівникам підприємств та фахівцям з кібербезпеки щодо організації та здійсненню управління вразливостями корпоративної інформаційної системи.

Таким чином, запропоновані в роботі рекомендації мають сприяти ефективному управлінню вразливостями корпоративної інформаційної системи.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ransomware Index Update Q1 2021. Whitepapers. Cyber Security Works. [Електронний ресурс] – Режим доступу: https://cybersecurityworks.com/resources/whitepapers/ransomware-index-update-q1-2021.html.

2. Biggest Cybersecurity Challenges in 2023. Check Point. [Електронний ресурс] – Режим доступу: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/biggest-cybersecurity-challenges-in-2023/.

3. Erdal Ozkaya. The vulnerability management strategy. G-Forum. November 11, 2020. [Електронний ресурс] – Режим доступу: https://globalcioforum.com/the-vulnerability-management-strategy/.

4. Vulnerability Management? May 6, 2021. [Електронний ресурс] – Режим доступу: https://www.crowdstrike.com/cybersecurity-101/vulnerability-management/.

5. Drew Robb. Top Vulnerability Management Tools for 2023. March 17, 2023. [Електронний ресурс] – Режим доступу: https://www.esecurityplanet.com/products/vulnerability-management-software/.

6. Elias Carabaguiaz. Fabian Alfaro. Francisco Villalobos. Jeffry Arias. Kenneth Gonzalez. Warren Pere. IBM QRadar Version 7.3. Planning and Installation Guide. IBM, January 2018. – 112 p.

7. IBM QRadar Security Intelligence Platform 7.4. QRadar architecture overview. Last Updated: 2023-02-08. [Електронний ресурс] – Режим доступу: https://www.ibm.com/docs/en/qsip/7.4?topic=deployment-qradar-architecture-overview.

8. Overview of QRadar Vulnerability Manager. Last Updated: 2021-11-08. [Електронний ресурс] – Режим доступу: https://www.ibm.com/docs/en/qradar-on-cloud?topic=manager-overview-qradar-vulnerability.

9. IBM QRadar Security Intelligence Platform 7.4. QRadar Vulnerability Manager Deployments. Last Updated: 2023-02-17. [Електронний ресурс] – Режим

доступу: https://www.ibm.com/docs/en/qsip/7.4?topic=overview-qradar-vulnerability-manager-deployments.

10. Mary K. Pratt. 12 steps to building a top-notch vulnerability management program. CSO, May 16, 2023 [Електронний ресурс] – Режим доступу: https://www.csoonline.com/article/3659838/12-steps-to-building-a-top-notch-vulnerability-management-program.html.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)