DOI 10.31891/2307-5732-2023-323-4-268-277
УДК 004.056

ПОКОТИЛО ОЛЕКСАНДРА
Державний університет «Житомирська політехніка»
ORCID ID: 0000-0002-1587-235X
e-mail: kik_poa@ztu.edu.ua
БАЙЛЮК ЄЛІЗАВЕТА
Державний університет «Житомирська політехніка»
ORCID ID: 0000-0002-4961-7816
e-mail: liza.bailiuk@gmail.com
ЩУР НАТАЛІЯ
Державний університет «Житомирська політехніка»
ORCID ID: 0000-0002-1182-4799
e-mail: thalitana@ztu.edu.ua

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ МОДЕЛЮВАННЯ ЗАГРОЗ

У статті наводяться результати аналізу програмного забезпечення для моделювання загроз, зокрема розглянуто найпопулярніші інструменти Microsoft Threat Modeling Tool, OWASP Threat Dragon, ThreatModeler, IriusRisk та SecuriCAD. Визначено їх основні функції, можливості та обмеження, продемонстровано загальний вигляд побудованих моделей. На основі проведеного аналізу складено таблицю з результатами порівняння розглянутих програмних засобів згідно критеріїв, які найчастіше враховуються при виборі засобів для моделювання загроз. Використовуючи отримані результаті та наведену математичну модель, визначено числові значення наступних показників ефективності для кожної з програм по шкалі від 1 до 5: зручність використання, час моделювання, рівень деталізації, спектр виявлення загроз, рівень підтримки, можливість інтеграції з іншими інструментами.

Ключові слова: метод моделювання, стандарти безпеки, показники ефективності, Microsoft Threat Modeling Tool, OWASP Threat Dragon, ThreatModeler, IriusRisk, SecuriCAD..

POKOTYLO OLEKSANDRA, BAILIUK YELYZAVETA, SHCHUR NATALIIA
Zhytomyr Polytechnic National University

COMPARATIVE ANALYSIS OF THREAT MODELING SOFTWARE

With the increase in the use of information and communication systems, the probability of cyber attacks, which can cause significant damage, increases. In this regard, their security has become one of the main problems of our time. Therefore, there is an important and urgent problem of using software for modeling and analyzing potential threats. The article presents the results of analysis of threat modeling software, including the most popular tools Microsoft Threat Modeling Tool, OWASP Threat Dragon, ThreatModeler, IriusRisk and SecuriCAD. Their main functions, capabilities and limitations are defined, the general appearance of the built models is demonstrated. In addition, the modeling process was investigated with further analysis of the results using each of the considered tools. Their effectiveness in identifying and mitigating potential threats was also evaluated. Based on the analysis, a table was compiled with the results of the comparison of the considered software tools according to the criteria that are most often taken into account when choosing tools for threat modeling, in particular, openness of the source code, support for security standards and various platforms, the possibility of integration with other tools, automatic detection of threats, model visualization, vulnerability analysis, risk assessment and management, planning of security measures, support for joint work with the team, cost. Using the results obtained and the given mathematical model, numerical values of the following performance indicators were determined for each of the programs on a scale from 1 to 5: ease of use, simulation time, level of detail, spectrum of threat detection, level of support, possibility of integration with other tools. The choice of the optimal tool will depend on the level of priority of a specific indicator for the enterprise. The obtained results of the analysis make it possible to simplify the decision-making process of choosing the optimal program, as they clearly demonstrate the advantages and disadvantages of each of them, as well as to increase the effectiveness of the use of software tools for threat modeling thanks to the received evaluations of effectiveness and the identified potential areas of their use.

Keywords: modeling method, security standards, performance indicators, Microsoft Threat Modeling Tool, OWASP Threat Dragon, ThreatModeler, IriusRisk, SecuriCAD..

Постановка проблеми

Моделювання загроз є обов'язковим для кожної організації, яка хоче захистити свої дані, враховуючи все більш зростаючу залежність від технологій. У третьому кварталі 2022 року було зламано приблизно 108,9 мільярдів облікових записів, що на 70% більше, ніж у попередні квартали того ж року[1]. Одна невелика вразливість може дозволити зловмисникам проникнути в мережу або хмару компанії та отримати доступ до даних клієнтів.

Моделювання загроз – це структурований підхід до визначення потенційних ризиків для системи та розробки плану їх пом'якшення. Метою моделювання загроз є виявлення потенційних зловмисників, їх мотивації та методів атаки. Потім ця інформація може бути використана для розробки плану управління ризиками, який можна використовувати для захисту системи.

Сам процес моделювання можна проводити у будь-який момент під час розробки, але найбільш оптимальний варіант – на початку проектування. Це дасть можливість раніше виявити загрози та впоратися з ними до того, як вони можуть завдати збитків.

Для створення моделей загроз використовують спеціалізоване програмне забезпечення, яке

допомагає проаналізувати потенційні загрози і вразливості в системах та розробити ефективні стратегії їх захисту.

На сьогоднішній день існує багато інструментів, які мають свої переваги та недоліки, відрізняються за функціональністю, можливістю інтегруватися з іншими засобами та підтримкою платформ. Їх порівняння між собою дозволяє зрозуміти, які функції та можливості мають бути присутні в програмі та обрати оптимальний інструмент для конкретної потреби організації чи окремого користувача, а також допомогти в ефективному забезпеченні захисту інформаційної системи. Тому питання проведення порівняльного аналізу програмного забезпечення для моделювання загроз є актуальним.

Метою роботи є підвищення ефективності використання сучасних програмних засобів для моделювання загроз, зокрема Microsoft Threat Modeling Tool, OWASP Threat Dragon, ThreatModeler, IriusRisk та SecuriCAD шляхом проведення їх узагальненого порівняння та визначення оцінки ефективності цих інструментів для подальшого визначення потенційної сфери використання кожного з них.

Основними задачами для досягнення поставленої мети є: визначення інструментів для подальшого аналізу; вивчення їх функціональних особливостей та процесу створення моделей загроз; проведення порівняння засобів згідно наступних критеріїв: відкритість вихідного коду, підтримка стандартів безпеки та різних платформ, можливість інтеграції з іншими інструментами, автоматичне виявлення загроз, візуалізація моделі, аналіз вразливостей, оцінка та управління ризиками, планування заходів безпеки, підтримка спільної роботи з командою, вартість; дослідження отриманих результатів.

Аналіз останніх джерел

Дослідженнями програмного забезпечення для побудови моделей загроз займається ряд вітчизняних та закордонних вчених, таких як А.О. Гапон, В.М. Федорченко, А.О. Поляков, І.Ф. Аулов, Дж. Сімен, К.Бернсмед, Д.Крузес, М.Г. Джаатун, М.Айован, А.Шаад, Д.Біндер та інші.

В статті "Підходи до побудови моделі загроз для аналізу безпеки відкритого програмного коду"[2] йдеться мова про аспекти, які потрібно враховувати при побудові моделі загроз, такі як визначення, поняття, класифікація загроз, визначення стратегії перекриття загроз або зниження рівня ризиків, а також тестової стратегії побудованої моделі. Авторами проаналізовано існуючі підходи класифікації загроз, враховуючи весь спектр потенційних ризиків, та сформовано рекомендації для формування моделей загроз, що враховують вразливості в програмному коді.

Публікація "Засоби моделювання та аналізу ризиків в середовищі хмарних обчислень"[3] містить дослідження програмних продуктів з відкритим кодом (OWASP Threat Dragon, CAIRIS, Mozilla Seasponge) та із закритим кодом (Microsoft Threat Modeling Tool, RiskWatch, vsRisk). Наведено ряд переваг та недоліків кожного інструменту, висунуто ряд вимог, за якими порівнювалися програмні продукти. В результаті визначено, що жодна з програм в повній мірі не відповідає висунутим вимогам, описано варіанти їх вдосконалення.

Дослідження "Cyber Threat Prediction and Modelling"[4], "Adopting threat modelling in agile software development projects"[5] та "ML-Supported Identification and Prioritization of Threats in the OVVL Threat Modelling Tool"[6] містять відомості про збір та використання інформації про загрози, яка використовуватиметься в подальшій побудові моделі та про процес моделювання в цілому.

Авторами запропоновано ряд інструментів для автоматизації аналізу загроз для кожного окремого елемента та надано рекомендації, як зробити процес моделювання ефективнішим.

За даними аналізу наявних публікацій зроблено висновок про відсутність робіт, де було б продемонстровано процес створення моделей загроз за допомогою різних програмних засобів і описано функціональні особливості кожного з них, а також проведено оцінку ефективності їх використання залежно від пріоритетів організації, де кожний з інструментів буде застосовуватися.

Виклад основного матеріалу

Процес моделювання загроз складається з визначення активів підприємства, дослідження функцій кожної програми в загальній схемі та створення профілю безпеки для кожної з них. Процес продовжується визначенням потенційних загроз та пріоритетів, а потім – документуванням шкідливих подій та дій, які необхідно вжити для їх усунення[7].

Існують різні методи моделювання загроз, включаючи підходи, орієнтовані на активи, зловмисників і програмне забезпечення. Кожен із цих підходів має свої переваги та недоліки, і організації повинні враховувати свої конкретні потреби та ресурси при виборі методу моделювання загроз.

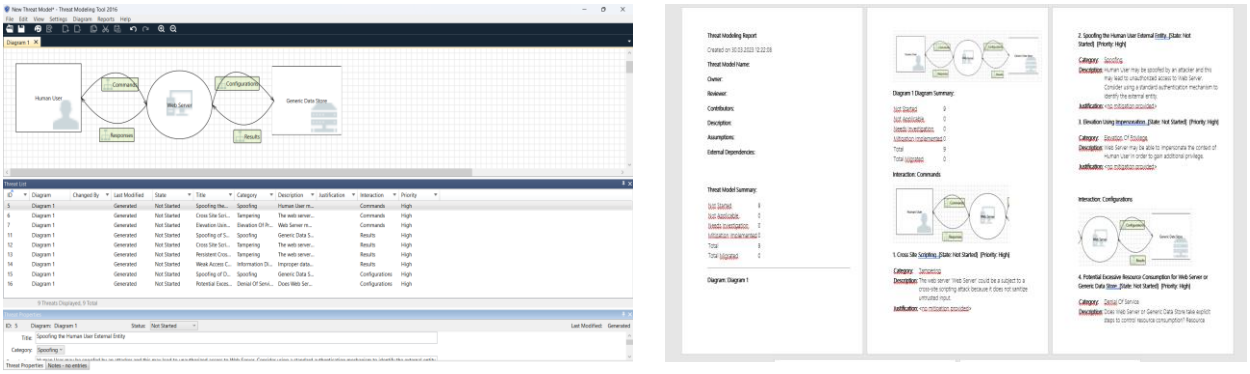
На сьогоднішній день є багато програмних засобів, доступних для моделювання загроз інформаційно-комунікаційної системи. Розглянемо деякі з найпопулярніших інструментів та їх особливості.

Microsoft Threat Modeling Tool – це безкоштовний інструмент, який допомагає організаціям визначати потенційні загрози для їхніх програмних систем. Інструмент використовується для побудови діаграми потоку даних, яка відображає, які дані пересилаються в системі. Після цього визначаються потенційні загрози для кожного елементу побудованої діаграми, та ризики, пов'язані з ними, щоб визначити їх складність та небезпечність. Наступний етап – надання рекомендацій щодо пом'якшення цих загроз. Типова модель загроз, побудована за допомогою даного інструменту, наведена на рис.1(а).

Створені загрози допомагають зрозуміти потенційні недоліки конструкції та надають уявлення про можливі вектори атак, тоді як додатковий опис містить інформацію про те, що саме не так, а також потенційні способи пом'якшення загроз. Після внесення всіх необхідних змін є можливість зберегти або

роздрукувати звіт (рис.1(б)).

Основними перевагами Microsoft Threat Modeling Tool є те, що його можна завантажувати та використовувати безкоштовно, і що ним легко можуть користуватися навіть ті, хто має обмежені технічні знання. Інструмент також інтегрується з життєвим циклом розробки безпеки (SDL) Microsoft, що допомагає переконатися, що безпека вбудована в процес розробки[8]. Microsoft Threat Modeling Tool підтримує різні стандарти безпеки, такі як STRIDE, DREAD та PASTA, та може автоматично генерувати звіти, які допомагають зрозуміти результати аналізу безпеки програмного забезпечення. Інструмент забезпечує високу ефективність виявлення та пом'якшення потенційних загроз, має широкий спектр їх виявлення та високий рівень деталізації.

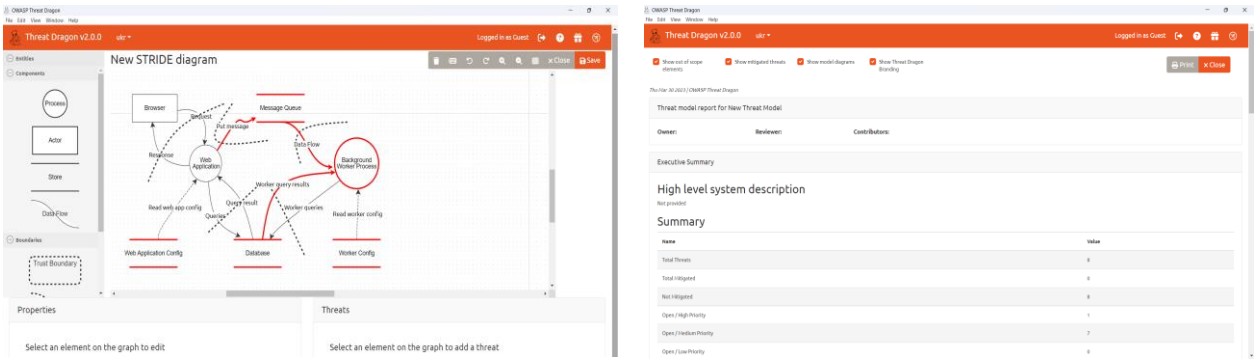


а) **б)**

Рис. 1. Microsoft Threat Modeling Tool : а) – модель загроз; б) – звіт з результатами моделювання

Даний програмний засіб можна використовувати для оцінки безпеки хмарних систем, виявлення потенційних загроз і вразливостей, що характерні для них. Також він може застосовуватися для моделювання та аналізу безпеки пристроїв Інтернету речей (IoT), визначаючи потенційні вектори атак і слабкі місця. Проте Microsoft Threat Modeling Tool має деякі обмеження. Наприклад, він підтримується лише операційними системи Windows, що може обмежити його корисність для організацій, які використовують інші операційні системи. Крім того, він підтримує тільки обмежену кількість архітектур програмного забезпечення[9].

OWASP Threat Dragon – це інструмент моделювання загроз із відкритим кодом, розроблений Open Web Application Security Project (OWASP), з метою допомогти фахівцям із безпеки визначати пріоритети потенційних загроз безпеці у своїх програмах і системах. При запуску програми одразу відкривається сторінка редагування, де можна ввести загальну інформацію про модель. Додавання компонентів системи та потоків даних відбувається шляхом їх перетягування на основне поле. Потім додаються загрози та встановлюються їх властивості, такі як вірогідність виникнення та наслідки. Залишається тільки встановити зв'язки між компонентами та загрозами, після чого можна переходити до аналізу. Приклад моделі загроз, побудованої за допомогою OWASP Threat Dragon, наведено на рис.2(а). У перегляді деталей моделі загроз відображається підсумковий звіт створеної моделі з переліком діаграм, елементів та загроз, який можна зберегти або роздрукувати для подальшого використання(рис.2(б)).



а) **б)**

Рис. 2. OWASP Threat Dragon: а) – модель загроз; б) – звіт з результатами моделювання

Однією з ключових особливостей OWASP Threat Dragon є простота використання. Інструмент розроблено таким чином, щоб бути зручним і доступним як для спеціалістів із безпеки, так і для розробників із невеликим досвідом або зовсім без досвіду моделювання загроз. Це досягається завдяки використанню простого графічного інтерфейсу, який дозволяє користувачам легко створювати та візуалізувати моделі загроз. OWASP Threat Dragon підтримує різноманітні методології моделювання загроз, зокрема STRIDE, DREAD і PASTA. Він також пропонує можливість створювати власні методології моделювання загроз, а також імпортувати й експортувати моделі загроз у різних форматах, включаючи формат Microsoft Threat

Modeling Tool, YAML і JSON[10]. Ще однією важливою особливістю є його інтеграція з іншими інструментами розробки, зокрема такими як Visual Studio Code, Jira та GitLab, що полегшує включення моделювання загроз в існуючі робочі процеси розробки.

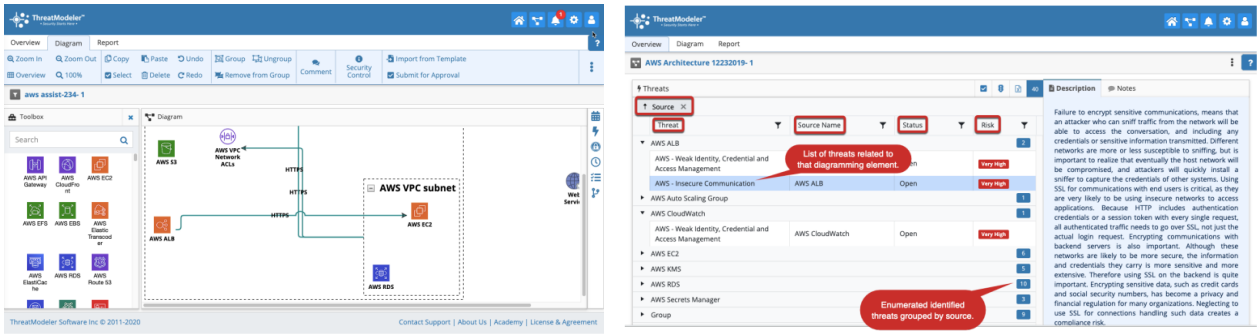
OWASP Threat Dragon є безкоштовним інструментом, та має відкритий код, що дозволяє розробникам та інженерам змінювати його під свої потреби. Він добре підходить для виявлення загроз і вивчення протоколів, але має обмежені можливості для пом'якшення цих загроз. Практичне застосування даного інструменту доцільне для забезпечення безпеки мобільних та веб-додатків. Його можна використовувати для моделювання архітектури і виявлення потенційних загроз, таких як ін'єкційні атаки, міжсайтовий сценарій (XSS) або підробка міжсайтового запиту (CSRF). Threat Dragon також може допомогти проаналізувати безпеку мобільних додатків, виявити такі ризики, як незахищене зберігання даних, незахищений зв'язок або слабкі механізми автентифікації.

Одним із потенційних недоліків OWASP Threat Dragon є обмежена підтримка платформи. Зараз інструмент доступний лише для операційних систем Windows, Linux і macOS. Крім того, він має невеликий спектр виявлення загроз, тому для створення моделей необхідно вручну вводити дані, що може зайняти багато часу та зробити процес складнішим[11].

ThreatModeler – це інструмент моделювання загроз, який використовує автоматичний аналіз даних для визначення потенційних загроз для системи. Інструмент використовує алгоритми машинного навчання для аналізу даних і виявлення шаблонів, які вказують на потенційні загрози.

Створення моделі загроз починається з розміщення попередньо визначених компонентів на полотні діаграми. Потім вони поєднуються відповідними зв'язками та визначаються конкретні властивості компонентів. Це можна робити як для кожного елемента окремо, так і для попередньо створеної групи. Далі додаються загрози та визначаються їх властивості з подальшим встановленням їх зв'язків з компонентами(рис.3(а)).

Подробиці налаштованої моделі відображаються на підсумковому екрані, де можна побачити список сформованих загроз, зокрема їх назву, джерело, статус та рівень ризику, який вони можуть спричинити(рис.3(б))[12].



а) **б)**

Рис. 3. ThreatModeler: а) – головне вікно з побудованою діаграмою; б) – список сформованих загроз

Основна перевага ThreatModeler – це його широкі можливості налаштування. Інструмент дозволяє користувачам визначати власні моделі загроз, які можна адаптувати до конкретних потреб організації, або автоматично їх створювати на основі аналізу коду програмного забезпечення та архітектури системи. Крім того, інструмент надає детальний аналіз потенційних загроз і вразливостей, що може допомогти організаціям розробити більш ефективні плани управління ризиками та забезпечити гнучкість при моделюванні.

ThreatModeler підтримує різні стандарти безпеки, такі як STRIDE, DREAD, CVSS та OWASP Top 10, та може інтегруватися з іншими інструментами безпеки, зокрема з Burp Suite та Splunk. Він забезпечує ефективне виявлення та аналіз потенційних загроз, а також пропонує певні рекомендації щодо їх пом'якшення.

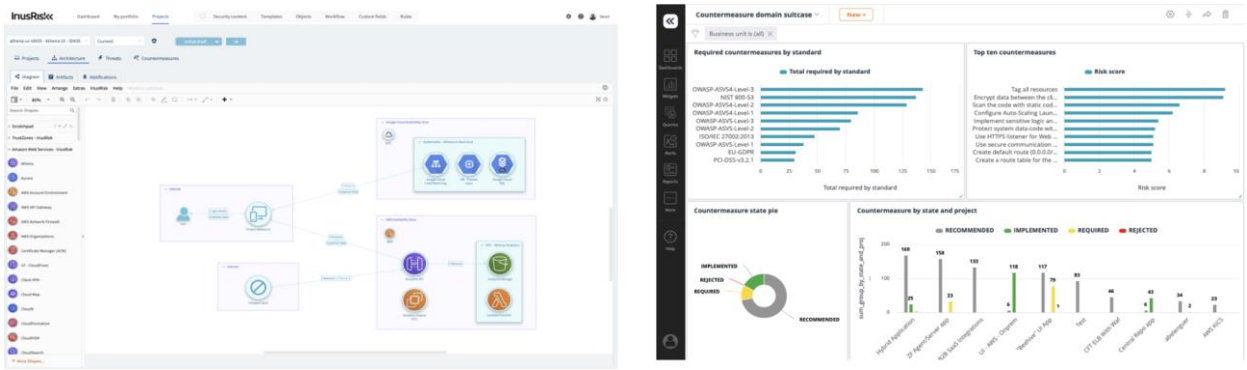
Прикладом практичного використання даного інструменту є інтеграція життєвого циклу розробки програмного забезпечення. ThreatModeler можна використовувати для бездоганної інтеграції моделювання загроз у процес розробки програмного забезпечення, гарантуючи безпеку на кожному етапі.

Однак у ThreatModeler є деякі обмеження. Наприклад, інструмент є відносно дорогим, що може обмежити його корисність для невеликих організацій або окремих користувачів. Крім того, інструмент може бути складним у використанні для користувачів, які не мають багато досвіду в області безпеки, з врахуванням багатьох функцій та можливостей, які пропонуються[13].

IriusRisk – це інструмент моделювання загроз, який використовує підхід, заснований на оцінці ризику, для виявлення потенційних загроз для системи. Інструмент використовує серію попередньо визначених шаблонів для виявлення потенційних загроз і вразливостей, а потім надає рекомендації щодо пом'якшення цих загроз.

Початок створення моделі загроз починається з визначення активів підприємства та встановлення їх взаємозв'язків. Далі формуються сценарії загроз, що можуть на них впливати. Сценарії можна створити

вручну або імпортувати з інших інструментів, таких як Microsoft Threat Modeling Tool, OWASP Threat Dragon або ThreatModeler. Наступний крок – встановити вплив кожної загрози, визначити ризики, які з ними пов'язані, та встановити пріоритети для ризиків. Все це стає основою для розробки плану заходів по зменшенню ризиків і підвищенню безпеки проекта. На рис.4(а) відображено головне вікно програми з побудованою діаграмою. Вбудована система аналітики та звітності дозволяє отримати практичну інформацію про дані моделі загроз в режимі реального часу, яка відображається на інформаційних панелях(рис.4(б)).



а) **б)**

Рис. 4. IriusRisk: а) – модель загроз; б) – результат моделювання

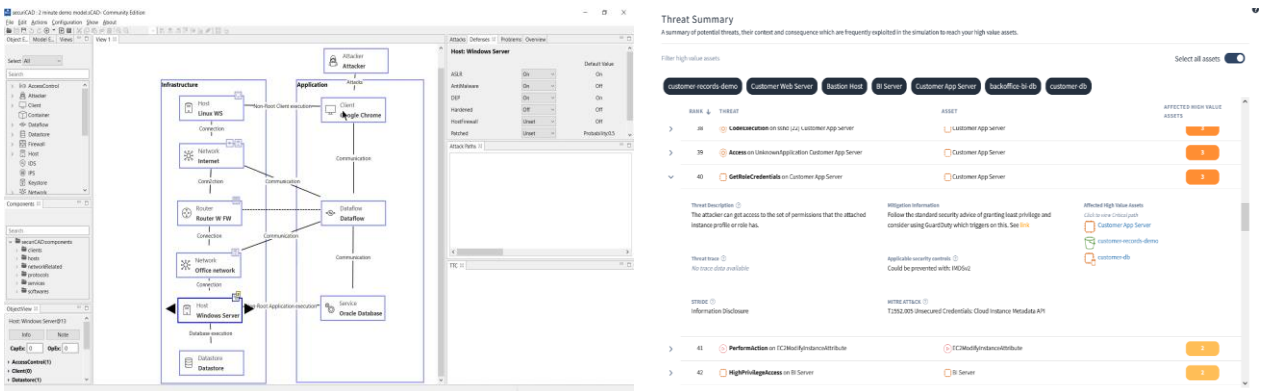
До переваг IriusRisk можна віднести можливість інтегруватися з іншими інструментами безпеки, такими як JIRA, Git та Jenkins та підтримку стандартів безпеки STRIDE, DREAD, CVSS та OWASP Top 10. Інструмент має модульну структуру, що дозволяє користувачам легко налаштовувати та розширювати функціонал. У IriusRisk є також можливість використання готових шаблонів, які допомагають створювати моделі загроз для різних типів проектів, таких як банківські системи, медичні системи тощо. Інструмент має розширені можливості виявлення потенційних загроз та розробки стратегій їх пом'якшення. IriusRisk дозволяє організаціям легко включати моделювання загроз у свої процеси DevSecOps, сприяючи постійному вдосконаленню безпеки протягом життєвого циклу розробки програмного забезпечення.

Серед недоліків варто відмітити складність використання у зв'язку з наявністю великої кількості додаткових функцій, та високу вартість, так як IriusRisk є комерційним інструментом і вимагає платної ліцензії, що може бути непосильним для невеликих організацій та індивідуальних користувачів[14].

SecuriCAD – це інструмент для автоматизованої оцінки ризиків та вразливостей в IT-інфраструктурі компаній та організацій. SecuriCAD має інтуїтивно зрозумілий інтерфейс, який дозволяє легко перетягувати та змінювати розміщення компонентів на полі моделювання. Також інструмент надає можливість використання готових шаблонів, які допомагають створювати моделі загроз для різних типів проектів.

Для побудови моделі загроз в SecuriCAD потрібно додати активи, які необхідно захистити, та компоненти захисту, такі як брандмауери, антивірусні програми, шифрування тощо на поле моделювання. Сценарії атак, які можуть бути спрямовані на визначені ресурси, можна створювати вручну або імпортувати з інших інструментів. Щоб почати симуляцію, потрібно додати зловмисника до моделі. Точки входу зловмисника визначаються шляхом його підключення до існуючих об'єктів у моделі(рис.5(а)).

Після завершення моделювання є можливість згенерувати звіт, який дасть загальне уявлення про рівень ризиків, критичні шляхи атаки, інформацію про всі дії, які виконує зловмисник, щоб отримати доступ до активів високої вартості під час симуляції. Також буде сформовано список засобів безпеки, які можна застосувати, щоб запобігти загрозам(рис.5(б))[15].



а) **б)**

Рис. 5. SecuriCAD: а) – модель загроз; б) – результат моделювання

Сильними сторонами SecuriCAD є виявлення вразливостей на ранніх етапах розробки системи, що

дозволяє вчасно вжити заходів для зменшення ризику їх використання, та різнорівнева оцінка ризиків, що дозволяє зосередитися на найбільш критичних частинах системи та зменшити загальний рівень ризику. SecuriCAD використовує методи машинного навчання та інші автоматизовані методи для аналізу безпеки, що дає можливість ефективно виявляти можливі вразливості та ризики, і може інтегруватися з іншими інструментами безпеки. Він забезпечує ефективне виявлення та аналіз потенційних загроз за допомогою моделювання виробничих процесів та інших систем.

SecuriCAD можна використовувати для моделювання та симуляції атак на системи критичної інфраструктури, такі як електромережі або транспортні мережі, для виявлення потенційних вразливостей і планування стратегій їх пом'якшення. Це дозволяє перевіряти ефективність існуючих заходів безпеки, допомагаючи організаціям посилити захист.

Основні недоліки SecuriCAD на сьогоднішній день – це висока вартість та серйозні вимоги до знань, адже для ефективного використання інструменту користувач повинен мати розуміння процесів розробки програмного забезпечення, безпеки мереж та веб-додатків, що може вимагати додаткових навчань. Крім того, він не має можливості моделювання певних типів IT-інфраструктур, таких як мобільні додатки або хмарні рішення.

Всі розглянуті інструменти надають цінну допомогу у виявленні та зменшенні ризиків безпеки в різних областях, включаючи хмарні архітектури, веб- та мобільні додатки, життєвий цикл розробки програмного забезпечення, критичну інфраструктуру та ін. Вибір інструменту залежить від конкретних потреб організації, складності систем, що моделюються, і бажаного підходу до моделювання загроз.

Ефективність програмних засобів для моделювання можна визначити за допомогою різних показників, але важливо враховувати, що ця оцінка суб'єктивна і буде залежати від конкретних потреб. До загальних показників, які можуть використовуватися для оцінювання ефективності, можна віднести наступні: зручність використання, час моделювання, рівень деталізації, інтеграція з іншими інструментами. спектр виявлення загроз, рівень підтримки.

Для оцінювання використаємо 5-бальну шкалу, в якій значення від 1 до 5 можемо розглядати за такими принципами: 1 – дуже низький рівень (програма має серйозні обмеження в реалізації показника, майже не задовольняє вимогам), 2 – низький рівень (програма частково задовольняє вимогам, є деякі обмеження в реалізації показника), 3 – середній рівень (програма задовольняє основним вимогам щодо показника, без особливих обмежень та винятків), 4 – високий рівень (програма демонструє гарні результати, є деякі обмеження в реалізації показника), 5 – дуже високий рівень (програма демонструє виняткові результати та переваги в реалізації показника). Значення від 1 до 5 дозволяють створити градацію програм за ефективністю виконання показників для їх подальшого порівняння та визначення найкращого варіанту при врахуванні конкретних потреб організації.

На основі загальної методології оцінювання можна навести приблизну математичну модель для визначення значень показників ефективності інструментів для моделювання. Оцінка зручності буде визначатися на основі кількох факторів, таких як інтерфейс користувача, наявність готових шаблонів, інтуїтивно зрозумілих функцій та документації. Для її визначення можна використовувати інформацію з форумів, де користувачі обговорюють простоту використання, або експертні оцінки.

Час моделювання, необхідний для створення діаграми, може бути виміряний в годинах або днях. Чим швидше буде побудовано модель, тим вища оцінка. Для визначення рівня деталізації буде враховуватися кількість та різноманітність елементів, доступних для створення моделі загроз. Більша кількість деталей відповідає вищій оцінці. Оцінка інтеграції базуватиметься на підтримці стандартних форматів обміну даними, API для взаємозв'язку з іншими інструментами, можливості підтримки інших засобів розробки та наявності плагінів. Для оцінювання спектру виявлення загроз враховуватиметься кількість та діапазон різноманітності доступних загроз, які можуть бути змодельовані в програмі. Більшій оцінці відповідає ширший спектр загроз. Оцінка рівня підтримки буде визначена на базі доступності технічної підтримки, активності розробника у виправленні помилок, наявності постійних оновлень, документації та спільноти користувачів.

Результати

В результаті проведеного дослідження пропонується наступна таблиця порівняння інструментів згідно таких критеріїв: відкритий вихідний код (програми з відкритим вихідним кодом забезпечують можливість його перегляду та змінення, що допомагає перевіряти наявність потенційних загроз та вносити власні покращення до програми), підтримка стандартів безпеки (відповідність різним стандартам безпеки гарантує, що програма відповідає встановленим нормам та має належні засоби безпеки), інтеграція з іншими інструментами (дозволяє забезпечити обмін даними та інформацією між різними компонентами системи), автоматичне виявлення загроз (допомагає швидко ідентифікувати потенційні вразливості та загрози безпеки в системі; може включати виявлення аномальної активності або спроб несанкціонованого доступу), візуалізація моделі (графічне відображення допомагає зрозуміти складність побудови системи та виявити потенційні ризики), аналіз вразливостей (здатність виявляти вразливості в системі або програмному коді), оцінка ризиків (можливість ідентифікувати потенційні загрози, виявляти вразливості та визначати ймовірність їх виникнення та потенційні збитки), управління ризиками (відображає здатність ефективно визначати, аналізувати, оцінювати та керувати ризиками з метою зниження ймовірності виникнення небажаних подій та зменшення їх впливу), планування заходів безпеки (здатність до розробки та реалізації

ефективних планів та заходів безпеки), аудит безпеки (можливість проводити процес перевірки та оцінки безпекових заходів для захисту системи від загроз з метою виявлення недоліків в безпеці), перегляд історії змін моделювання (здатність до зберігання та відстеження історії змін), робота з командою (можливість використання програми для спільного доступу до проектів, спілкування та співпраці між учасниками команди, коментування та обговорення моделей), підтримка різних платформ (забезпечує універсальність та доступність програмного забезпечення для користувачів різних операційних систем), вартість (платні та безкоштовні варіанти мають різні функціональні можливості) (табл.1).

Використовуючи результати проведеного аналізу, визначимо числові значення показників ефективності для кожної програми, враховуючи, що вони є умовними і можуть варіюватися в залежності від визначених умов, налаштувань програм та конкретних сценаріїв.

Всі оцінки були визначені шляхом аналізу відгуків та рейтингу користувачів, які можна знайти в публічних джерелах, та загальної інформації, яка є на сайтах розробників. Результати наведено в табл.2.

Таблиця 1

Порівняльна характеристика програмних засобів для моделювання загроз

Критерії	**Microsoft Threat Modeling Tool**	**OWASP Threat Dragon**	**ThreatModeler**	**IriusRisk**	**SecuriCAD**
Відкритий вихідний код	Ні	Так	Ні	Ні	Ні
Підтримка стандартів безпеки	Так (STRIDE, DREAD, CVSS)	Так (OWASP Top 10, CWE)	Так (STRIDE, DREAD, CVSS, CWE)	Так (OWASP Top 10, ISO/IEC 27001)	Так (CVSS)
Інтеграція з іншими інструментами	Так (Visual Studio, Azure DevOps)	Ні	Так (JIRA, ServiceNow, Microsoft Teams, Slack)	Так (JIRA, GitLab)	Так (JIRA, ServiceNow)
Автоматичне виявлення загроз	Ні	Ні	Так	Так	Так
Візуалізація моделі	Так	Так	Так	Так	Так
Аналіз вразливостей	Так	Так	Так	Так	Так
Оцінка ризиків	Так	Так	Так	Так	Так
Планування заходів безпеки	Ні	Ні	Так	Так	Так
Управління ризиками	Ні	Ні	Так	Так	Так
Аудит безпеки	Ні	Ні	Так	Ні	Так
Перегляд історії змін моделювання	Ні	Так	Так	Ні	Так
Спільна робота з командою	Ні	Так	Так	Так	Так
Підтримка різних платформ	Так (Windows, .NET Framework 4.5 і вище)	Так (Windows, macOS, Linux)	Так (Windows, хмарна інфраструктура)	Так (Windows, macOS, Linux, хмарна інфраструктура)	Так (Windows, macOS, Linux)
Вартість	Безкоштовний	Безкоштовний	Платний	Платний	Платний

Таблиця 2

Оцінки ефективності програмних засобів для моделювання загроз

Програмне забезпечення	**Зручність**	**Час моделювання**	**Рівень деталізації**	**Інтеграція**	**Спектр виявлення загроз**	**Рівень підтримки**
Microsoft Threat Modeling Tool	3	4	4	3	5	4
OWASP Threat Dragon	4	3	3	2	3	3
ThreatModeler	3	4	5	3	4	3
IriusRisk	4	3	5	4	5	5
SecuriCAD	3	3	4	5	3	4

На основі визначених числових значень показників ефективності можна зробити висновок, що кращою програмою для моделювання загроз у випадку врахування шести обраних показників і використанні сумарного балу, є IriusRisk. Вона пропонує високий рівень деталізації, розглядає широкий спектр загроз і має високий рівень інтеграції з іншими програмними засобами. Крім того, даний засіб отримує винятковий рівень підтримки, тобто регулярно оновлюється, надає вичерпну документацію та активну технічну підтримку користувачам.

Проте деякі показники можуть мати більш важливе значення для конкретних організацій, залежно від їх пріоритетів. Деякі проекти можуть потребувати детального розгляду загроз та наслідків їх впливу. В такому випадку більший пріоритет матиме рівень деталізації. Якщо достатньо тільки загального огляду

вразливостей, тоді цей показник матиме меншу значущість.

Час моделювання матиме високий пріоритет, якщо термін для створення чи оновлення моделі буде обмеженим. Також в такій ситуації важливою буде зручність, так як програми, що мають більшу оцінку за цим показником, можуть полегшити процес моделювання, підвищити ефективність роботи, та зменшити час, який потрібний для моделювання загроз. Крім того, зручність матиме більший пріоритет у випадку, якщо в організації наявна невелика кількість експертів з безпеки. У випадку, якщо в організації вже використовуються інші інструменти для керування загрозами та безпекою, і є можливість взаємодіяти з ними, показник інтеграції може бути вирішальним.

Щодо організаційного типу, важливо враховувати їх специфічні потреби та обмеження. Наприклад, корпоративні мережі можуть ставити на перше місце показники, пов'язані із швидкістю впровадження та зручністю. Якщо говорити про державні та урядові установи, для них важливими є висока безпека та відповідність стандартам. Підприємства з високою критичністю безпеки, зокрема організації, пов'язані з обробкою персональних даних, або фінансові установи, звертають увагу на рівень деталізації та спектр виявлення загроз. Невеликий бізнес може зосередитися на доступній ціні програмного засобу та зручності його використання. Тому важливо враховувати контекст використання та особливості інформаційно-комунікаційної системи при обранні програмного засобу для моделювання загроз.

Визначимо потенційні сфери використання розглянутих програмних засобів, в яких вони будуть найефективніші, згідно отриманих результатів дослідження. Враховуючи особливості Microsoft Threat Modeling Tool, найкраще застосовувати його для організацій, які вже користуються екосистемою Microsoft та мають інші інструменти безпеки від даного виробника. Крім того, даний засіб може бути особливо корисним у випадку необхідності включення моделювання загроз в ранні стадії життєвого циклу розробки програмного забезпечення завдяки широкому спектру виявлення загроз.

OWASP Threat Dragon ідеально підходить для організацій, які шукають безкоштовний та відкритий варіант програмного забезпечення з акцентом на веб-застосунках, та які дотримуються рекомендацій методології OWASP з безпеки програмного забезпечення, так як даний засіб з усіх розглянутих показників найвищу оцінку має по зручності використання.

Використання ThreatModeler буде найефективнішим для компаній з великою та складною інфраструктурою, які потребують детального моделювання загроз та аналізу ризиків для забезпечення безпеки, завдяки максимальному значенню рівня деталізації.

IriusRisk найкраще підходить для організацій з різними потребами та типами інфраструктури, які потребують зручного та простого у використанні інструмента для моделювання загроз та управління ризиками. Високі оцінки показників рівня деталізації та спектру загроз забезпечують ефективність використання даної програми для проектів, які вимагають глибокого аналізу та комплексного моделювання. Завдяки відмінному рівню підтримки, інструмент також підходить для організацій, які потребують постійної підтримки та оновлення.

Так як SecuriCAD має максимальну оцінку з інтеграції, найефективнішим його використання буде для організацій з комплексною інфраструктурою та потребами у взаємодії з іншими інструментами безпеки, у яких є необхідність моделювати загрози як з фізичної, так і з кібербезпеки.

Не знаючи конкретних потреб організації, складно визначити найкращий засіб для побудови моделі загроз. Наприклад, якщо потрібен інструмент для роботи в середовищі Windows, то найбільш підходящими варіантами будуть Microsoft Threat Modeling Tool та ThreatModeler, а якщо використовуються різні операційні системи, то кращим вибором будуть OWASP Threat Dragon, IriusRisk чи SecuriCAD. Microsoft Threat Modeling Tool, ThreatModeler і IriusRisk підходять для великих корпоративних додатків через свої широкі можливості і високий рівень інтеграції, а OWASP Threat Dragon і SecuriCAD краще використовувати для невеликих проектів, враховуючи їх простоту та спеціалізовані функції.

Вибираючи інструмент моделювання загроз обов'язково мають враховуватися і такі критерії як функціональність, бюджет, технічний досвід та ліцензування. Крім того, організації повинні переконатися, що інструмент добре інтегрується з наявною інфраструктурою безпеки та процесами розробки.

Висновки

Моделювання загроз є важливим процесом для розробки ефективних заходів безпеки для інформаційних і комунікаційних систем. Використання програмних засобів може значно допомогти в цьому процесі, автоматизуючи аналіз даних і надаючи рекомендації щодо пом'якшення потенційних загроз.

Авторами було розглянуто п'ять популярних програмних засобів для моделювання загроз інформаційно-комунікаційних систем. Хоча кожен інструмент має свої переваги та недоліки, усі вони дають цінну інформацію про потенційні загрози та вразливі місця. Всі перераховані програми мають різний рівень ефективності виявлення та пом'якшення потенційних загроз, проте деякі з них мають розширені можливості для розробки стратегій їх пом'якшення, що робить їх більш ефективними у цьому відношенні.

Отримані результати дозволяють обрати найбільш ефективний засіб для моделювання, враховуючи особливості конкретної інформаційної системи.

Наукова новизна цієї роботи полягає в тому, що визначено оцінки ефективності програмних засобів на базі результатів аналізу з використанням шести загальних показників, наведено приблизну математичну модель для визначення ефективності програмних засобів, проаналізовано, в яких випадках кожен з показників матиме більший пріоритет та визначено потенційні сфери використання інструментів з

врахуванням отриманих результатів.

Практична значущість демонструється результатами порівняння, які дозволяють обрати найефективніший засіб для створення моделі загроз, враховуючи особливості конкретної інформаційної системи. Використовуючи ці інструменти, організації можуть краще зрозуміти потенційні загрози своїм системам і розробити більш ефективні плани управління ризиками для їх захисту.

У подальших дослідженнях планується вивчення можливостей використання найсучаснішого програмного забезпечення для моделювання загроз у віртуальному середовищі. Це може допомогти відтворити реальні умови та перевірити ефективність заходів захисту від потенційних загроз.

Література

1. Advantages of Threat Modeling in 2023 & beyond [Електронний ресурс]. Режим доступу: https://www.we45.com/post/ advantages-of-threat-modeling-in-2023-beyond. Дата звернення: 31 берез. 2023

2. А.О Гапон, В.М Федорченко, А.О Поляков "Підходи до побудови моделі загроз для аналізу безпеки відкритого програмного кода", Захист інформації та кібернетична безпека, № 1(160), с. 128–135, 2020. [Онлайн]. Режим доступу: https://journal-hnups.com.ua/index.php/soi/ article/view/184/130. Дата звернення: 5 квіт. 2023.

3. І.Ф Аулов, К.Е Лисицький "Засоби моделювання та аналізу ризиків в середовищі хмарних обчислень", Радиотехника. Методы и алгоритмы защиты и сокрытия информации, № 195, с. 138–143, 2018. [Онлайн]. Режим доступу: https://nure.ua/wp-content/ uploads/2018/Scientific_editions/rvmnts_2018_195_15.pdf Дата звернення: 31 берез. 2023.

4. J. Seaman "Cyber Threat Prediction and Modelling", Artif. Intell. Nat. Secur., с. 113–156, 2022. [Онлайн]. Режим доступу: https://link.springer.com/chapter/10.1007/978-3-031-06709-9_7#citeas Дата звернення: 5 квіт. 2023.

5. K. Bernsmed, D. Cruzes, M. G. Jaatun, M. Iovan "Adopting threat modelling in agile software development projects", J. Syst. Softw. 183(12):111090, 2021. [Онлайн]. Режим доступу: https://www.sciencedirect.com/ science/article/abs/pii/S0164121221001874?via=ihub Дата звернення: 5 квіт. 2023.

6. Schaad, D. Binder "ML-Supported Identification and Prioritization of Threats in the OVVL Threat Modelling Tool", Data Appl. Secur. Privacy XXXIV, с. 274–285, 2020. [Онлайн]. Режим доступу: https://link.springer.com/chapter/10.1007/978-3-030-49669-2_16 Дата звернення: 5 квіт. 2023.

7. What is Threat Modeling: Process and Methodologies [Електронний ресурс] Режим доступу: https://www.simplilearn.com/what-is-threat-modeling-article. Дата звернення: 31 берез. 2023.

8. Microsoft Threat Modeling Tool 2016 [Електронний ресурс] Режим доступу: https://www.microsoft.com/en-us/download/details.aspx?id=49168. Дата звернення: 31 берез. 2023.

9. Microsoft Threat Modeling Tool [Електронний ресурс] Режим доступу: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool. Дата звернення: 31 берез. 2023

10. OWASP Threat Dragon [Електронний ресурс] Режим доступу: https://owasp.org/www-project-threat-dragon/. Дата звернення: 31 берез. 2023.

11. OWASP Cheat Sheet Series. Threat Modeling Cheat Sheet [Електронний ресурс] Режим доступу: https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html. Дата звернення: 31 берез. 2023.

12. ThreatModeler™: Interface Guide [Електронний ресурс] Режим доступу: https://tm-awsmp.s3.amazonaws.com/ThreatModeler%2BInterface%2BGuide.pdf. Дата звернення: 31 берез. 2023.

12.1) ThreatModeler - Automated Threat Modeling Solution [Електронний ресурс] Режим доступу: https://threatmodeler.com/ Дата звернення: 31 берез. 2023.

13. IriusRisk | The Automated Threat Modeling Platform [Електронний ресурс] Режим доступу: https://www.iriusrisk.com/ Дата звернення: 30 берез. 2023.

14. SecuriCAD. NSE Lab [Електронний ресурс] Режим доступу: https://nse.digital/pages/guides/Creating%20threat%20models/securiCAD.html Дата звернення: 30 берез. 2023.

References

1. Advantages of Threat Modeling in 2023 & beyond [Online]. Available: https://www.we45.com/post/ advantages-of-threat-modeling-in-2023-beyond. Accessed on: Mar. 31, 2023.

2. A.O Hapon, V.M Fedorchenko, A.O Polyakov "Threat model building approaches for open code security analysis ", Information protection and cyber security, № 1(160), pp. 128–135, 2020. [Online]. Available: https://journal-hnups.com.ua/index.php/soi/ article/view/184/130. Accessed on: Apr. 5, 2023 [in Ukrainian].

3. I.F Aulov, K. E. Lysytskyi " Risk modeling and analysis tools in the cloud computing environment ", Radio engineering. Methods and algorithms for protecting and hiding information, № 195, pp. 138–143, 2018. [Online]. Available: https://nure.ua/wp-content/uploads/2018/Scientific_editions/rvmnts_2018_195_15.pdf Accessed on: Mar. 31, 2023 [in Ukrainian].

4. J. Seaman "Cyber Threat Prediction and Modelling", Artif. Intell. Nat. Secur., pp. 113–156, 2022. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-06709-9_7#citeas Accessed on: Apr. 5, 2023.

5. K. Bernsmed, D. Cruzes, M. G. Jaatun, M. Iovan "Adopting threat modelling in agile software development projects", J. Syst. Softw. 183(12):111090, 2021. [Online]. Available: https://www.sciencedirect.com/ science/article/abs/pii/S0164121221001874?via=ihub Accessed on: Apr. 5, 2023.

6. A. Schaad, D. Binder "ML-Supported Identification and Prioritization of Threats in the OVVL Threat Modelling Tool", Data Appl.

Secur. Privacy XXXIV, с. 274–285, 2020. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-49669-2_16 Accessed on: Apr. 5, 2023.

7. 7. What is Threat Modeling: Process and Methodologies [Online]. Available: https://www.simplilearn.com/what-is-threat-modeling-article. Accessed on: Mar. 31, 2023.

8. 8. Microsoft Threat Modeling Tool 2016 [Online]. Available: https://www.microsoft.com/en-us/download/details.aspx?id=49168. Accessed on: Mar. 31, 2023.

9. Microsoft Threat Modeling Tool [Online]. Available: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool. Accessed on: Mar. 31, 2023.

10. OWASP Threat Dragon [Online]. Available: https://owasp.org/www-project-threat-dragon/. Accessed on: Mar. 31, 2023.

11. OWASP Cheat Sheet Series. Threat Modeling Cheat Sheet [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html. Accessed on: Mar. 31, 2023.

12. ThreatModeler™: Interface Guide [Online]. Available: https://tm-awsmp.s3.amazonaws.com/ThreatModeler%2BInterface%2BGuide.pdf. Accessed on: Mar. 31, 2023.

13. 13. ThreatModeler - Automated Threat Modeling Solution [Online]. Available: https://threatmodeler.com/ Accessed on: Mar. 31, 2023.

14. 14. IriusRisk | The Automated Threat Modeling Platform [Online]. Available: https://www.iriusrisk.com/ Accessed on: Mar. 30, 2023.

15. SecuriCAD. NSE Lab [Online]. Available: https://nse.digital/pages/guides/Creating%20threat%20models/securiCAD.html Accessed on: Mar. 30, 2023.