الجمهورية اليمنية

وزارة التربية والتعليم والبحث العلمي

جامعة آزال للتنمية البشرية

كلية الهندسة وتقنية المعلومات

: CyberSim Defender
محاكي لالتقاط الهجمات ومعرفة نوعها

الاء علي علي الجيواني	2022140476
اية محمد قاسم حجر	2022010863
شيماء عبدالله حميد دغيش	2022010842
غدير عبدالحكيم عامر دغيش	2022010850
ماريا قايد حسن العباسي	2022011003

تحت اشراف:

د/عبدالسلام خاقو

البحث مقدم الى كلية الهندسة وتقنية المعلومات قسم الامن السيبراني؛ جامعة أزال للتنمية البشرية

لاستكمال نيل درجة البكالوريوس في الامن السيبراني

2026-2025

الآية القرآنية

اعوذ بالله من الشيطان الرجيم

قال تعالى:

(قالوا سبحانك لا علم لنا الا ما علمتنا * انك انت العليم الحكيم)

سورة البقرة الآية 32

صدق الله العظيم

المستخلص :

مشروع (CyberSim Defender) يقوم ببناء تطبيق يعمل على نظام ويندوز لمحاكاة الهجمات السيبرانية وتحليلها واقتراح حلول مناسبة، الفكرة الأساسية هي توفير بيئة تفاعلية تسمح للمستخدم بمراقبة النظام واكتشاف الهجمات وفهم طبيعتها ثم اتخاذ إجراءات وقائية بناءً على توصيات الذكاء الاصطناعي.

يعتمد التطبيق على عدة مكونات رئيسية أولها المحرك الذكي في الخلفية وهو المسؤول عن تحليل حركة الشبكة والملفات الحساسة باستخدام أدوات مثل SharpPcap لالتقاط الحزم، ويعتمد على نماذج تعلم آلي عبر ONNX Runtime لتصنيف الهجمات، بالإضافة إلى قواعد كشف مدمجة (rule-based) تدعمها نماذج الذكاء الاصطناعي لاكتشاف الهجمات مثل DDoS و SQL Injection و Port Scan وغيرها، كما يقوم بمراقبة الملفات الحيوية في النظام عبر حساب قيم التجزئة (MD5 Hash) لاكتشاف التغييرات غير المصرح بها.

ثانياً واجهة المستخدم الرسومية التي تبنى باستخدام WPF وتحتوي على ثلاث نوافذ رئيسية تعرض للمستخدم محاكاة الهجمات التعليمية خطوة بخطوة مع رسوم متحركة توضيحية، ومراقبة الملفات مع عرض التهديدات المكتشفة، ومراقبة الشبكة مع إحصائيات فورية وتنبيهات أمنية ونصائح فورية يستخرجها مستشار الأمان المدعوم بالذكاء الاصطناعي.

يرتبط المحرك الذكي بالواجهة عبر أحداث (Events) وربط البيانات (Data Binding) مما يضمن التواصل السلس بين الطبقات، كما يحتوي التطبيق على قاعدة معرفة مدمجة تخزن فيها أنواع الهجمات العشرة المختلفة مع مراحلها والحلول المقترحة التي يوصي بها الذكاء الاصطناعي.

المشروع يقدم قيمة تعليمية وتدريبية كبيرة فهو يدمج الذكاء الاصطناعي، تحليل الشبكات، مراقبة الملفات، ومحاكاة الهجمات في تطبيق قابل للتوسع والاستخدام في بيئات تعليمية أو تدريبية.

Abstract :

CyberSim Defender is a Windows-based application designed to simulate cyberattacks, analyze their behavior, and propose appropriate mitigation strategies. The core idea is to provide an interactive environment that allows users to monitor system activity, detect attacks, understand their nature, and take preventive actions based on AI-powered recommendations.

The application is built on several key components. At its core lies the **intelligent backend engine**, responsible for analyzing network traffic and sensitive files using tools such as **SharpPcap** for packet capture. It leverages **machine learning models via ONNX Runtime** to classify attacks, complemented by **rule-based detection mechanisms** enhanced by AI models to identify threats such as DDoS, SQL Injection, Port Scanning, and others. Additionally, the engine monitors critical system files by computing **MD5 hash values** to detect unauthorized modifications.

The **graphical user interface (GUI)** is developed using **WPF** and features three main windows:

An **interactive attack simulation** window with step-by-step educational scenarios and animated visuals.

A **file monitoring** window displaying detected threats.

A **network monitoring** window with real-time statistics, security alerts, and instant recommendations from an **AI-powered security advisor**.

The backend engine communicates with the GUI seamlessly through **events** and **data binding**, ensuring smooth interaction between layers. The application also includes an **integrated knowledge base** that stores ten different attack types, along with their phases and AI-generated mitigation recommendations.

CyberSim Defender offers significant educational and training value by integrating **artificial intelligence**, **network analysis**, **file integrity monitoring**, and **attack simulation** into a single, scalable application suitable for educational or training environments.

الاهداء (Dedication)

بسم الله الرحمن الرحيم

نهدي هذا الجهد المتواضع ثمرة سنوات من البحث والدراسة الى اللذين كانوا خير عون وسند ،لهم كل الشكر والعرفان على كل قربات قدموها وكل دعاء رددته السنتهم وكل تضحية بذلوها من اجلنا فانتم سر النجاح وروح الإنجاز الى من كان لهم الفضل الأكبر ابائنا الأعزاء وامهاتنا الغاليات، الى اسرنا الكريمة شكرا لكم على كل لحظة دعم وكل كلمة تشجيع وكل صبر وسعة صدر خلال رحلتنا الدراسية، مشرفنا الفاضل الدكتور عبدالسلام خاقو الذي لم يبخل علينا بوقته او علمه فكان نبراساً ينير لنا الطريق بتوجيهاته القيمة جزاه الله خير الجزاء، الى دكاترتنا الافاضل على ما غرسوه فينا من علم فكانوا لنا خير معين، أصدقائنا الأعزاء الذين كانوا معنا في السراء والضراء، الى كل من مد لنا يد العون ولو بكلمة طيبة او نظرة تشجيع ساهمت في اكمال هذا المشوار، هذا العمل هو محاولة متواضعة نقدمها لكم شكراً لكم جميعاً ونسأل الله ان نكون عند حسن ظنكم.

شكر وتقدير (Acknowledgment)

نود ان نعبر عن خالص امتنانا وتقديرنا العميق لدكاترتنا واساتذتنا الافاضل على كل ما بذلوه من جهود لاثراء عقولنا بالعلم والمعرفة وشكر خاص لمشرف المشروع الدكتور عبد السلام خاقو على نصائحه القيمة وصبرة على متابعة هذا العمل؛ كما لا يفوتنا ان نتوجه بالشكر الجزيل لاعضاء لجنة المناقشة على شرف قبولهم مناقشة هذا العمل وتقييمه وعلى ملاحظاتهم البناءة التي اكسبت البحث دقة أكبر؛ ولعائلتنا الكريمة التي كانت خير عون لها منا كل التقدير والحب؛ ونسأل الله ان نكون قد وفقنا في تقديم عمل يليق بكل هذا الدعم.

إقرار المشرف (Supervisor Certification)

اشهد ان هذا المشروع اعد بواسطة:

الاء علي علي الجيواني وايه محمد قاسم حجر وشيماء عبدالله حميد دغيش وغدير عبدالحكيم عامر دغيش وماريا قايد حسن العباسي

تحت اشرافي في جامعة أزال كلية الهندسة وتقنية المعلومات قسم الامن السيبراني للحصول على درجة البكالوريوس في الامن السيبراني.

اسم المشرف:

التوقيع:

التاريخ:

لجنة الحكم والمناقشة (Examination Committee)

عنوان المشروع: CyberSim Defender

المشرف

NO	الاسم	الوظيفة	التوقيع
1			

لجنة الحكم والمناقشة

NO	الاسم	الوظيفة	التوقيع
1			
2			
3			
4			

جدول المحتويات

جدول الرسوم التوضيحية

جدول الجداول

الفصل 1
المقدمة(Introduction)

1.1 نظرة عامة عن المشروع (Overview):

يقوم هذا المشروع بتطوير تطبيق تفاعلي لمحاكاة الهجمات السيبرانية ومراقبة النظام على بيئة نظام تشغيل Windows، وذلك لأغراض التدريب والتحليل الأمني. يتيح التطبيق للمستخدمين ثلاث واجهات متكاملة: الأولى لمحاكاة الهجمات خطوة بخطوة مع رسوم متحركة توضيحية، والثانية لمراقبة الملفات الحساسة واكتشاف التغييرات غير المصرح بها، والثالثة لتحليل حركة الشبكة في الوقت الفعلي. يمكن للمستخدم اكتشاف الأنماط المشبوهة، وتصنيف نوع الهجوم، ثم اقتراح حلول دفاعية مناسبة عبر مستشار الأمان المدمج.

يعتمد المشروع على دمج تقنيات متعددة تشمل الذكاء الاصطناعي عبر نماذج ONNX Runtime، وتحليل الشبكات باستخدام مكتبة SharpPcap، ومراقبة الملفات عبر حساب قيم التجزئة MD5، ضمن واجهة رسومية جميلة وسهلة الاستخدام تم بناؤها بتقنية WPF. كما يوفر بيئة تعليمية آمنة لفهم كيفية حدوث 10 أنواع مختلفة من الهجمات (SQL Injection ، DoS، DDoS، BruteForce، Ransomware، Phishing، Man-in-the-Middle، XSS، DNS Spoofing، Zero-Day Exploit) وآليات التصدي لها، دون تعريض الأنظمة الحقيقية للخطر.

يوفر المشروع واجهة إدارة موحدة تمكن المستخدمين من متابعة الحالة الأمنية للجهاز، وعرض قائمة التهديدات المكتشفة في مراقب الملفات، وعرض التنبيهات الأمنية في مراقب الشبكة، مع إمكانية عرض تقارير تفصيلية عن كل تهديد (نوع الهجوم، المصدر، الوجهة، نسبة الثقة، والإجراءات المقترحة)، واقتراح الإجراءات المناسبة للتعامل معها مثل حظر عناوين IP المشبوهة أو عزل الملفات الخطرة. يتميز بقدرته على التعامل مع أنواع متعددة من الهجمات بما فيها هجمات DDoS، هجمات الحقن (SQL Injection)، هجمات Ransomware، هجمات التصيد (Phishing)، هجمات الرجل في المنتصف (MITM)، مع تقديم حلول مخصصة لكل نوع من هذه التهديدات عبر مستشار الأمان (Advisor Service) المدعوم بقواعد معرفية.

يعمل المشروع بشكل مستقل مع إمكانية التكامل مع البنى التحتية الأمنية الموجودة من خلال واجهات الأحداث (Events) وربط البيانات (Data Binding)، مما يجعله حلاً مناسباً لكل من المستخدمين الأفراد والمؤسسات. يتم تحديث قاعدة معرفة التهديدات يدوياً أو عبر إضافة أنواع جديدة من الهجمات وقواعد الكشف، مع الحفاظ على خصوصية البيانات وأمانها خلال عملية التحليل والمراقبة التي تتم محلياً على جهاز المستخدم.

تم تطوير المشروع بلغة C# وإطار WPF المتوافقة مع بيئة Windows، مع التركيز على الكفاءة والأداء والموثوقية من خلال استخدام أنماط التصميم الحديثة مثل MVVM و Service Locator، مما يضمن تشغيلاً مستقراً على مختلف إصدارات نظام التشغيل Windows.

2.1 مشكلة المشروع (Problem Statement):

مشكلة المشروع عنصر جوهري تنطلق منه فكرة المشروع، فهي تمثل الأساس الذي يبنى عليه هدف المشروع، تحديد المشكلة وفهم نطاقها وتأثيرها يساعد في إيجاد حلول فعالة ومناسبة لها.

في السنوات الأخيرة شهدت اليمن تصاعداً ملحوظاً في الهجمات السيبرانية بنسبة 42% في الهجمات الخبيثة على أجهزة Windows خلال عامي 2023 و 2024 حسب تقارير Kaspersky [1].

أيضاً منصة Digital Watch أفادت في تقاريرها أن 60% من المؤسسات اليمنية لا تمتلك أنظمة كشف مبكر للهجمات السيبرانية [2].

1. غياب أدوات تفاعلية محلية لمحاكاة الهجمات السيبرانية واكتشافها.
2. ضعف الأنظمة التقليدية في تتبع مسار الهجوم بشكل تحليلي.
3. عدم وجود استجابة ذكية مخصصة لكل نوع من أنواع الهجمات.
4. عدم تكامل مراقبة الملفات مع مراقبة الشبكة في نظام واحد.
5. اعتماد الحلول الأمنية الحالية على نماذج أجنبية غير ملائمة للبيئة اليمنية.

3.1 أهداف المشروع (Project Objective):

أهداف المشروع هي عنصر أساسي الغرض منها حل مشاكل المشروع. بعد النظر والاطلاع على مشاكل المشروع التي تم ذكرها سابقاً:

1- تطوير نظام محاكاة متكامل لمحاكاة 10 أنواع من الهجمات السيبرانية بدقة على أنظمة Windows، مع مراقبة مستمرة للشبكة مع عرض تفاعلي لتتبع مسار الهجوم.

2- تطوير واجهة مستخدم رسومية بـ WPF تحتوي على ثلاث نوافذ رئيسية (محاكاة الهجمات، مراقبة الملفات، مراقبة الشبكة) لرصد وتحليل التهديدات، وتدعم اللغة العربية مع تجربة مستخدم سلسة.

3- تصميم محرك كشف هجين يجمع بين القواعد المدمجة والذكاء الاصطناعي عبر ONNX Runtime، قادر على اكتشاف وتصنيف الهجمات على الملفات الحساسة وحركة الشبكة بدقة، مع اقتراح حلول مخصصة خلال زمن استجابة لا يتجاوز 3 ثوان.

4- تحقيق تكامل كامل بين نظام مراقبة الملفات ونظام مراقبة الشبكة في واجهة موحدة، مع ضمان استقرار التشغيل على أنظمة Windows 10/11.

5- توفير حل أمني متكامل باللغة العربية بالكامل يناسب البيئة اليمنية والمؤسسات المحلية، مع إمكانية التوسع وإضافة أنواع جديدة من الهجمات مستقبلاً.

4.1 مساهمة المشروع (Project Contribution):

يمثل المشروع مساهمة نوعية في مختلف جوانب الحياة الأكاديمية والمهنية والتقنية، حيث يجمع بين الجانب النظري والتطبيقي في مجال الأمن السيبراني .

كما يسهم المشروع في رفع مستوى الوعي الأمني لدى المستخدمين، من خلال واجهة رسومية تفاعلية تعرض الحالة الأمنية للنظام بشكل حي، وتقدم حلولًا واقعية قابلة للتنفيذ داخل بيئة ويندوز.

أولًا: المساهمة في الحياة الأكاديمية:

- تعزيز الفهم العملي للأمن السيبراني **:** يوفر المشروع بيئة تطبيقية لفهم أنواع الهجمات وأساليب التصدي لها، مما يربط بين الجانب النظري والعملي في المناهج الدراسية.

- دعم مشاريع التخرج والبحث العلمي : يُعد المشروع نموذجًا تطبيقيًا يمكن البناء عليه في أبحاث الذكاء الاصطناعي، تحليل الشبكات، أو تطوير الأنظمة الدفاعية.
- تطوير المهارات التقنية للطلاب : من خلال استخدام تقنيات برمجة متعددة وتقنيات متقدمة، يساهم المشروع في صقل مهارات البرمجة، تحليل البيانات، والتفكير المنطقي.
- إثراء المحتوى التعليمي : يمكن استخدام المشروع كمادة تدريبية في المختبرات الأكاديمية أو كورسات الأمن السيبراني، مما يرفع من جودة التعليم.

ثانيًا: المساهمة في الحياة المهنية:

- تأهيل الكوادر لسوق العمل : يساعد المشروع في إعداد الطلاب والمهتمين بمجال الأمن السيبراني للعمل في المؤسسات التقنية، من خلال تجربة واقعية للهجمات والحلول.
- تحسين أدوات الحماية في المؤسسات : يمكن تطوير المشروع ليصبح أداة داخلية في الشركات لاختبار جاهزية الأنظمة ضد الهجمات.
- دعم فرق الاستجابة للحوادث الأمنية : من خلال تحليل سلوك الهجمات وتقديم حلول ذكية، يمكن أن يكون المشروع نظام كشف مبكر للهجمات على مستوى الشبكة والملفات مما يساعد في الأستجابة السريعة قبل تفاقم الهجوم.

ثالثًا: المساهمة في المجتمع والتوعية العامة:

- رفع الوعي الأمني لدى المستخدمين : من خلال الواجهة التفاعلية والتنبيهات، يتعلم المستخدم كيف يكتشف السلوكيات المشبوهة ويحمي نفسه.
- المساهمة في الأمن الوطني السيبراني : يمكن أن يكون المشروع نواة لتطوير أنظمة دفاعية محلية تساهم في حماية البنية التحتية الرقمية.
- تشجيع الابتكار المحلي : يمثل المشروع نموذجًا ملهمًا للطلاب والمطورين في المنطقة لتطوير حلول تقنية محلية تخدم المجتمع.

5.1 نطاق المشروع (Project Scope):

نطاق المشروع هو تحديد ما سيتضمنه المشروع من مهام وأهداف ووظائف، ويشمل جميع الأنشطة والعمليات التي سيتم إنجازها لتحقيق أهداف المشروع.

يشمل نطاق المشروع:

- أنواع الهجمات التي سيتم محاكاتها: SQL Injection، DoS Attack، DDoS Attack، Brute Force، Ransomware، Phishing Attack، Man-in-the-Middle (MITM)، XSS Attack، DNS Spoofing، Zero-Day Exploit.

- الهجمات التي يتم مراقبتها في الشبكة : (DDoS , WebAttacks , SYN-Flood , RST-Flood , ICMP-Flood , UDP-Flood , SSH-patator , FTP-Patator)

- الأنظمة المدعومة: Windows 10 / 11.

- بناء واجهة رسومية متكاملة: باستخدام WPF، تحتوي على ثلاث نوافذ رئيسية (محاكاة الهجمات، مراقبة الملفات، مراقبة الشبكة) مع دعم كامل للغة العربية.

- التقاط الحزم وتحليل حركة الشبكة: باستخدام SharpPcap و PacketDotNet لالتقاط الحزم من واجهة الشبكة وتحليل التدفقات (flows) في الوقت الفعلي.

- مراقبة الملفات الحساسة: باستخدام حساب قيم التجزئة MD5 لإنشاء بصمة (baseline) للمسارات الحرجة مثل System32، SysWOW64، Startup، Temp، والكشف عن التغييرات غير المصرح بها.

- تصنيف الهجمات واكتشاف التهديدات: باستخدام قواعد كشف مدمجة (rule-based detection) ونماذج الذكاء الاصطناعي عبر ONNX Runtime.

- اقتراح الحلول والنصائح الأمنية: من خلال مستشار الأمان (Advisor Service) الذي يقدم إجراءات فورية ونصائح وقائية حسب نوع الهجوم.

- تخزين السجلات والأحداث والتهديدات: باستخدام ObservableCollection في الذاكرة مع إمكانية التوسع لاستخدام SQLite مستقبلاً.

6.1 قيود المشروع (Project limitations):

قيود المشروع هي العوامل التي قد تؤثر على تنفيذ المشروع او تحد من تحقيق أهدافه ، مثل قيود الوقت و الميزانية والمتطلبات التقنية.

1- القيود التقنية:

- نظام التشغيل المستهدف :التطبيق مصمم خصيصًا لنظام Windows باستخدام WPF وC# ، مما يعني أنه غير قابل للتشغيل على أنظمة مثل Linux أو macOS دون إعادة كتابة شاملة.
- أدوات محددة :الاعتماد على مكتبات مثل SharpPcap لالتقاط الحزم، و Windows API لمراقبة الملفات، يفرض قيودًا على التوافق مع الإصدارات المختلفة من Windows.
- مراقبة الشبكة :التقاط الحزم يتطلب صلاحياتAdministrator ، وقد لا يعمل بشكل صحيح على بعض واجهات الشبكة الافتراضية.
- نموذج الذكاء الاصطناعي :استخدام ONNX Runtime مع قواعد كشف مدمجة (rule-based) قد يحد من دقة التصنيف مقارنة بنماذج التعلم العميق الأكثر تعقيدًا التي تحتاج إلى موارد أكبر

2- القيود الزمنية:

- مدة التنفيذ :المشروع مقيد بجدول زمني مدته 20 أسابيع، مما يحد من إمكانية التوسع أو إضافة ميزات متقدمة.
- اختبارات محدودة :بسبب ضيق الوقت، قد لا يتم اختبار جميع أنواع الهجمات أو السيناريوهات الواقعية بشكل شامل.

3- القيود الأمنية:

- صلاحيات التشغيل :يتطلب التطبيق صلاحيات Administrator لمراقبة الملفات الحساسة والتقاط حزم الشبكة، مما قد يشكل خطرًا إذا تم تشغيله بصلاحيات غير مناسبة.

4- القيود الوظيفية:

- واجهة المستخدم :رغم أنها تفاعلية، إلا أن التصميم الأولي قد لا يشمل جميع حالات الاستخدام أو التخصيصات المتقدمة مثل تغيير الثيمات أو إعادة ترتيب العناصر.
- تخزين البيانات :يعتمد التطبيق حاليًا على ObservableCollection للتخزين المؤقت في الذاكرة، مما يعني فقدان البيانات عند إغلاق التطبيق، مع عدم وجود تخزين دائم على القرص.
- قاعدة المعرفة :تعتمد على بيانات مدمجة في الكود المصدر (AttackStep) و(ThreatInfo) ، مما يتطلب إعادة compilation لإضافة أنواع جديدة من الهجمات أو قواعد الكشف.

5- القيود البيئية:

- توافر الموارد :يتطلب بيئة تطوير متكاملة تشمل Visual Studio ، NET 6.0.، ومكتبات SharpPcap وPacketDotNet .
- إمكانية التشغيل على الأجهزة الشخصية :قد تواجه بعض الأجهزة مشاكل في تشغيل التقاط الحزم بسبب عدم توافق بطاقات الشبكة أو جدار الحماية.

6- قيود الموارد والأداء:

- أداء النظام يعتمد على توفر ذاكرة RAM لا تقل عن GB 8 ومعالج متعدد الأنوية، مما يحد من التشغيل على الأجهزة ذات المواصفات المنخفضة.
- تنفيذ عمليات تحليل الشبكة والتصنيف في الوقت الحقيقي قد يؤدي إلى استهلاك مرتفع للموارد، ويؤثر على استجابة النظام.

7- قيود السلامة والأمان:

- غياب آلية استعادة تلقائية في حال فشل النظام قد يؤدي إلى فقدان البيانات أو توقف الخدمة.

8- قيود التوافق مع الأجهزة:

- النظام غير متوافق مع الأجهزة المحمولة أو اللوحية.
- يتطلب دعم بطاقة الشبكة لوضع Promiscuous Mode ، والذي قد لا يكون مدعومًا في بعض بطاقات الشبكة اللاسلكية.

7.1 منهجية المشروع(Project Methodology) :

يعتمد هذا المشروع على منهجية منظمة تتضمن عدة مراحل رئيسية، يتم تنفيذها بشكل متسلسل لضمان تحقيق الأهداف بكفاءة، مع تحديد الأدوات المستخدمة في كل مرحلة، وآليات التقييم، ومعايير النجاح.

1- مرحلة التهيئة وجمع المتطلبات:

في هذه المرحلة يتم تحديد نطاق المشروع بدقة ، وجمع المعلومات الضرورية حول أنواع الهجمات السيبرانية المستهدفة ، واحتياجات المستخدمين (طلاب ، متدربين ، باحثين) .

يتم إجراء مقابلات شخصية مع المختصين في الأمن السيبراني ، بالإضافة الى إعداد استبيانات لفهم توقعات المستخدمين من النظام.

الهدف من هذه المرحلة هو بناء تصور واضح للوظائف المطلوبة ، وتحديد الأولويات التقنية والتعليمية .

معيار النجاح : توثيق 10 أنواع هجمات قابلة للمحاكاة ، وتحديد 5 احتياجات رئيسية للمستخدمين .

2- مرحلة تحليل المتطلبات:

تتضمن تحليل المتطلبات التي تم جمعها من المقابلات والاستبيانات ، وتحديد المتطلبات الوظيفية (مثل المحاكاة ، التصنيف ، الاستجابة) وغير الوظيفية (مثل الأداء ، الأمان ، التوافق) .

يتم استخدام الرسوم البيانية مثل UML لتوثيق السيناريوهات ، حالات الاستخدام ، وتدفق البيانات بين الوحدات .

معيار النجاح : إنتاج وثيقة تحليل متكاملة تشمل جميع المكونات ، واعتمادها من قبل المشرف الأكاديمي .

3- مرحلة التصميم:

يتم في هذه المرحلة وضع تصميم شامل للنظام ، يشمل واجهة المستخدم وتجربة الاستخدام (UX) ، بالإضافة إلى تصميم طبقات النظام مثل المحاكاة ، التصنيف ، قاعدة المعرفة ، الاستجابة .

يتم إعداد نماذج أولية (Prototypes) باستخدام أدوات مثل Figma ، Adobe XD ، لتسهيل فهم التصميم النهائي قبل التنفيذ .

معيار النجاح : إنشاء نموذج أولي تفاعلي يغطي جميع الوظائف الأساسية ، والحصول على موافقة المستخدمين التجريبيين بنسبة رضا 85% .

4- مرحلة البرمجة:

يتم تطوير النظام الفعلي بناءً على التصميم المعتمد.

تشمل هذه المرحلة بناء ثلاث وحدات رئيسية: وحدة محاكاة الهجمات باستخدام C# و WPF لعرض 10 أنواع من الهجمات خطوة بخطوة مع رسوم متحركة توضيحية،

وحدة مراقبة الملفات باستخدام C# و MD5 Hash لمراقبة المسارات الحرجة واكتشاف التغييرات غير المصرح بها،

وحدة مراقبة الشبكة باستخدام SharpPcap لالتقاط الحزم وتحليل التدفقات في الوقت الفعلي.

يتم بناء واجهة المستخدم الرسومية باستخدام WPF وتتكون من ثلاث نوافذ رئيسية (محاكاة الهجمات، مراقبة الملفات، مراقبة الشبكة) مع دعم كامل للغة العربية.

يتم ربط الوحدات مع الواجهة من خلال أحداث (Events) وربط البيانات (Data Binding) ، مع استخدام ONNX Runtime لدمج نماذج الذكاء الاصطناعي في كشف الهجمات وتصنيفها، و ObservableCollection للتخزين المؤقت للتهديدات والسجلات في الذاكرة.

معيار النجاح : تنفيذ جميع الوظائف الأساسية بنسبة نجاح 95%، وتشغيل النظام داخل بيئة Windows 10/11 حقيقية بكفاءة مع محاكاة 10 أنواع من الهجمات ومراقبة الملفات الحساسة وتحليل حركة الشبكة في الوقت الفعلي.

5- مرحلة الاختبار والتقييم:

في هذه المرحلة يتم اختبار النظام لضمان أنه يعمل كما هو متوقع، باستخدام عدة أجهزة. تشمل الاختبارات:

- اختبار الوظائف: التأكد من قدرة النظام على محاكاة الهجمات، اكتشافها، وتصنيفها بدقة.
- اختبار الأداء: قياس زمن الاستجابة، استهلاك الموارد، واستقرار النظام.
- اختبار تجربة المستخدم: تقييم سهولة الاستخدام، وضوح الواجهة، ودعم اللغة العربية.
- اختبار التوافق: تجربة النظام على إصدارات مختلفة من Windows وعلى أجهزة بمواصفات متفاوتة.

معيار النجاح :اجتياز جميع الاختبارات بنسبة دقة 90%، واستقرار 99%، ومعدل رضا المستخدمين 85%.

6- **التحسين النهائي والتوثيق:**

بعد تحليل نتائج الاختبارات، يتم تحسين النظام بناءً على الملاحظات، وتوثيق جميع المكونات والوظائف بشكل أكاديمي، استعدادًا لتسليم المشروع النهائي.

8.1 أدوات المشروع (Project Tools):

يرتكز تنفيذ هذا المشروع على مجموعة من الأدوات البرمجية والتقنيات الحديثة، التي تم اختيارها بعناية لتلبية متطلبات النظام من حيث الأداء، التوافق مع بيئة التشغيل، والقدرة على محاكاة الهجمات السيبرانية واكتشافها والاستجابة لها بفعالية.

تم تقسيم الأدوات وفقًا للطبقات الوظيفية للنظام كما يلي:

جدول 1-1 أدوات المشروع

الأدوات المستخدمة	الهدف	الطبقة
• C# / .NET 6.0 : لمعالجة البيانات، الشبكات، والذكاء الاصطناعي • SharpPcap / PacketDotNet :لالتقاط وتحليل الحزم الشبكية من واجهة الشبكة • ONNX Runtime : لدمج نماذج الذكاء الاصطناعي في تصنيف الهجمات • MD5 Hashing : لمراقبة الملفات الحساسة واكتشاف التغييرات غير المصرح بها	• تنفيذ المنطق البرمجي وتحليل البيانات والهجمات • تحليل حركة المرور واكتشاف الهجمات في الوقت الفعلي • تصنيف الهجمات واقتراح استجابات ذكية حسب نوع التهديد • إنشاء بصمة للملفات الحرجة وكشف التعديلات المشبوهة	طبقة البرمجة والتحليل
• WPF (Windows PresentatioFoundation) : لبناء واجهة رسومية متقدمة على ويندوز مع ثلاث نوافذ رئيسية • XAML / MVVM :لتصميم واجهات المستخدم وربط البيانات	• توفير تجربة تفاعلية للمستخدم لمراقبة النظام وتنفيذ الحلول • فصل منطق العرض عن منطق الأعمال لتطوير قابل للصيانة	طبقة واجهة المستخدم
• Events / Data Binding : لربط المحرك الذكي بالواجهة الأمامية عبر أحداث وربط البيانات • Service Locator Pattern :لإدارة خدمات التطبيق بشكل مركزي	• ربط الواجهة الأمامية بالمحرك الخلفي دون الحاجة إلىAPI • تنظيم الخدمات (NetworkMonitor ، ThreatDetection ،AdvisorService)	طبقة الربط بين المكونات
• ObservableCollection :لتخزين الأحداث والسجلات والتهديدات في الذاكرة مؤقتاً • AttackStep / ThreatInfo Classes :لتخزين أنواع الهجمات ومراحلها والحلول المقترحة بشكل مدمج في الكود	• تخزين معلومات الهجمات والتهديدات المكتشفة وعرضها في الواجهة • تخزين 10 أنواع من الهجمات مع شرح وتفاصيل تقنية وإجراءات وقائية	طبقة قاعدة المعرفة

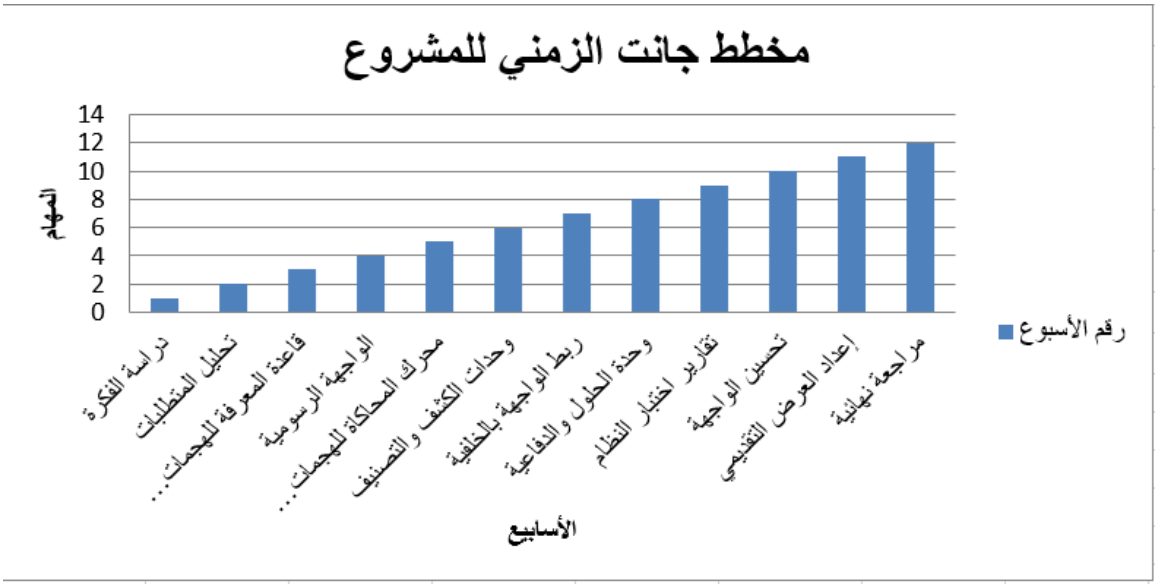
• محاكاة الهجمات التعليمية (Attack Simulator) : لعرض 10 أنواع من الهجمات خطوة بخطوة مع رسوم متحركة	• محاكاة هجمات تعليمية دون التأثير الفعلي على النظام	طبقة المحاكاة
• Windows API / File System :لمراقبة الملفات والمسارات الحرجة (System32 ، Startup، Temp) • مستشار الأمان (Advisor Service) : لاقتراح إجراءات فورية ونصائح وقائية حسب نوع الهجوم	• تنفيذ إجراءات دفاعية على النظام الحقيقي (مراقبة وكشف) • تقديم حلول مخصصة وتوصيات أمنية للمستخدم	طبقة الحماية والاستجابة

9.1 الجدول الزمني لتنفيذ المشروع (Project implementation Timeline)

جدول 2-1 زمن تنفيذ المشروع

الفترة	المهام	شرح المهام
2025/8/6 - 2025/8/15	دراسة الفكرة	تحديد نطاق المشروع + مراجعة متطلبات النظام + وضع خطة العمل
2025/8/16 - 2025/9/16	تحليل المتطلبات	تصميم أولي للواجهات الثلاث (محاكاة الهجمات، مراقبة الملفات، مراقبة الشبكة) + تحليل النظام وتحديد المكونات
2025/10/1 - 2025/10/25	الواجهة الرسومية	تطوير الواجهة الرسومية الأساسية باستخدام WPF مع ثلاث نوافذ رئيسية ودعم اللغة العربية
2025/10/29 - 2025/11/17	محرك المحاكاة للهجمات السيبرانية	بناء محرك المحاكاة باستخدام #C لعرض 10 أنواع من الهجمات (SQL Injection ، DoS، DDoS، Brute Force، Ransomware، Phishing، MITM، XSS، DNS Spoofing، Zero-Day) مع رسوم متحركة وتفاصيل تقنية
2025/11/20 - 2025/11/23	ربط الواجهة بالخلفية	ربط الواجهة بالمحركات الخلفية عبر أحداث (Events) وربط البيانات(Data Binding)
2025/11/25 - 2025/12/30	وحدات الكشف والتصنيف	تطوير وحدة كشف التهديدات باستخدام ONNX Runtime وقواعد كشف مدمجة لتحليل حركة الشبكة (SharpPcap) والملفات الحساسة(MD5 Hash)
2026/1/1- 2026/1/20	وحدة الحلول والدفاعية	تطوير مستشار الأمان (Advisor Service) لاقتراح إجراءات فورية ونصائح وقائية حسب نوع الهجوم.
2026/1/21 - 2026/1/28	تقارير اختبار النظام	اختبار النظام على سيناريوهات متعددة تشمل جميع أنواع الهجمات العشرة واختبار الكشف.
2026/2/2 - 2026/2/10	تحسين الواجهة	تحسين تجربة المستخدم مع واجهة تفاعلية ديناميكية تشمل عرض التنبيهات والتهديدات والنصائح بشكل لحظي.
2026/3/1 - 2026/3/30	إعداد العرض التقديمي	توثيق عرض PowerPoint + وثائق المشروع النهائية.
2026/4/1 - 2026/4/25	مراجعة نهائية	اختبار شامل للتطبيق على أنظمة Windows 10/11 + التعديلات والملاحظات النهائية + تجهيز تقرير المشروع النهائي

المخطط الزمني لتنفيذ المشروع يتطلب تنظيما دقيقا للوقت والمهام كما هو موضح في الجدول التالي:



رسم توضيحي 1-1 لمخطط جانت

10.1 هيكل البحث(Research Infrastructure):

مقدمة التوثيق:

يحتوي هذا الجزء على ايه قرانيه وخلاصة واهداء وشكر وتقدير وجدول المحتويات.

الفصل الأول (المقدمة):

يحتوي هذا الفصل على مقدمة المشروع ومشكلة المشروع واهداف المشروع ومساهمة المشروع ونطاق المشروع وأدوات المشروع والجدول الزمني للمشروع وقيود حدود المشروع وملخص الفصول.

الفصل الثاني (الخلفية النظرية والدراسات السابقة):

يحتوي هذا الفصل على الخلفية النظرية والنظريات الداعمة ومفاهيم متعلقة بمحاكات الهجمات السيبرانية والدراسات السابقة وما سيقدمه المشروع.

الفصل الثالث (تحليل المتطلبات والنمذجة):

يحتوي هذا الفصل على نظرة عامة عن المشروع و دراسة الجدوى و جمع المتطلبات ومنهجية المشروع وتحديد المتطلبات و متطلبات النمذجة و واجهات المشروع.

الفصل الرابع (تنفيذ المشروع):

يحتوي هذا الفصل على المقدمة و بناء الواجهات والواجهات الرئيسية والمحاكاة ومراقبة الشبكة

الفصل الخامس (اختبار المشروع):

هذا الفصل يحتوي على المقدمة واختبار الواجهات للمستخدم

الفصل السادس (الاستنتاجات والتوصيات المستقبلية):

هذا الفصل يحتوي على المقدمة والاستنتاجات والتوصيات المستقبلية

الفصل 2

الخلفية النظرية والدراسات السابقة

Background and)
(Literature Review

1.2 المقدمة

- **الخلفية النظرية (Background):**

في ظل التحول الرقمي المتسارع، أصبحت الأنظمة التقنية عرضة لهجمات سيبرانية متزايدة ومعقدة، تستهدف البنية التحتية الحيوية والبيانات الحساسة. ومن هنا برزت الحاجة إلى تطوير تقنيات حديثة لمحاكاة الهجمات السيبرانية كأداة فعالة لفهم سلوك المهاجمين واختبار جاهزية الأنظمة الدفاعية.

يقدم مشروع **CyberSim Defender** نموذجاً متكاملاً يجمع بين محاكاة الهجمات التعليمية وأنظمة المراقبة الأمنية الحقيقية. يتيح التطبيق للمستخدم ثلاث واجهات رئيسية: الأولى لمحاكاة 10 أنواع من الهجمات بشكل تفاعلي خطوة بخطوة مع رسوم متحركة، والثانية لمراقبة الملفات الحساسة عبر MD5 Hash، والثالثة لمراقبة حركة الشبكة عبر SharpPcap ونماذج ذكاء اصطناعي مدربة على CIC-IDS2017.

يهدف المشروع إلى تمكين المستخدمين من فهم آليات الهجمات وتقييم أداء الأنظمة الدفاعية، من خلال مستشار الأمان الذي يقدم إجراءات فورية ونصائح وقائية. تُعد هذه المنهجية امتداداً لنظرية "الدفاع العميق"، حيث يجمع المشروع بين طبقات متعددة من الحماية في بيئة آمنة .

ولضمان فعالية هذه الأنظمة، يتم تقييمها وفق مجموعة من المعايير، أبرزها:

- **دقة المحاكاة :**مدى واقعية السيناريوهات الهجومية مقارنة بالهجمات الفعلية.
- **قابلية التخصيص :**قدرة النظام على تعديل السيناريوهات حسب نوع الهجوم .
- **زمن الاستجابة :**الوقت المستغرق لاكتشاف الهجوم وعرض الإجراءات الدفاعية.
- **قابلية التكرار :**إمكانية إعادة تنفيذ نفس السيناريو لأغراض التدريب أو التقييم.
- **التكامل مع أدوات الأمن :**مدى توافق النظام مع أدوات مثلWindows Defender ، PowerShell، وأنظمةSIEM

وقد أظهرت الدراسات الحديثة أن المحاكاة المنتظمة للهجمات السيبرانية تساهم في تقليص زمن الاستجابة، وتحسين قدرة فرق الأمن السيبراني على اكتشاف التهديدات والتعامل معها بكفاءة.

- **منهجية جمع وتحليل الدراسات:**

تم جمع الدراسات السابقة من قواعد بيانات علمية موثوقة مثل IEEE Xplore، Springer، MDPI، و Google Scholar، باستخدام كلمات مفتاحية محددة مثلRandom Forest Intrusion Detection :، CIC-IDS2017 Dataset، File Integrity Monitoring using Hash، Cyber Range، Attack Simulation، AI-based Intrusion Detection، Defensive Response Systems تم التركيز على الدراسات المنشورة خلال السنوات الخمس الأخيرة (2020-2025) لضمان حداثة المحتوى وارتباطه بالتحولات الرقمية الحالية والتطورات السريعة في مجال الهجمات السيبرانية.

وقد تم تحليل هذه الدراسات من خلال تصنيفها حسب المجالات التالية:

- مجال كشف التسلل باستخدام التعلم الآلي :مثل دراسة Random Forest التي حققت دقة 99.9% على CIC-IDS2017
- مجال مجموعات البيانات المعيارية :مثل دراسة CIC-IDS2017 التي توفر 79 ميزة و 7 أنواع من الهجمات.
- مجال مراقبة سلامة الملفات :مثل دراسة استخدام Hash و Baseline في File Integrity Monitoring.
- مجال محاكاة الهجمات السيبرانية :مثل منصات cyber Range

تمت مقارنة المنهجيات المستخدمة في هذه الدراسات، واستخلاص نقاط القوة مثل (الدقة العالية، تنوع الهجمات، سرعة الكشف) ونقاط القصور مثل (صعوبة النشر، قلة التكامل، تكلفة عالية). كما تم التركيز على الدراسات التي تقدم نماذج قابلة للتنفيذ مثل Random Forest مع ONNX Runtime أو تقييمات عملية (مثل تقييم CIC-IDS2017على خوارزميات التعلم الآلي)، بهدف دعم الجانب التطبيقي للمشروع في مرحلتي مراقبة الشبكة ومراقبة الملفات.

- **نطاق التغطية :**

اقتصر نطاق التغطية في هذه الدراسة على الأبحاث التي تناولت محاكاة الهجمات السيبرانية واستخدام الذكاء الاصطناعي في الكشف عن الهجمات ومراقبة سلامة الملفات، مع التركيز على التطبيقات العملية التي تتوافق مع بيئةWindows .

تم استبعاد الدراسات النظرية البحتة أو تلك التي لا تقدم نماذج قابلة للتنفيذ، وذلك لضمان توافق النتائج مع أهداف المشروع التطبيقي.

كما تم تجاهل الدراسات التي تعتمد على بيئات تشغيل غير مدعومة مثل Linux-only أو أنظمة الشبكات الصناعية، لضمان تركيز المشروع على بيئة المؤسسات التعليمية والتقنية العامة.

2.2 مفاهيم متعلقة بمشروع cybersim (Concepts):

1.2.2الاختراق الأخلاقي (Ethical Hacking):

- هو تنفيذ هجمات سيبرانية خاضعة للرقابة بهدف اختبار أمان الأنظمة، ويُنفذ من قبل مختصين يُعرفون بـ "الهكر الأخلاقيين".

2.2.2 اختبار الاختراق (Penetration Testing):

- عملية منهجية لمحاولة اختراق نظام أو جهاز بهدف اكتشاف الثغرات الأمنية. تُستخدم أدوات مثل Metasploit وNmap وBurp Suite.

3.2.2 الفرق الحمراء والزرقاء (Red Team vs Blue Team):

- Red Team: تحاكي المهاجمين الحقيقيين وتنفذ الهجمات.
- Blue Team: مسؤولة عن الدفاع واكتشاف الهجمات والاستجابة لها.

4.2.2 الهجمات الفيزيائية (Physical Attacks):

- تشمل الوصول الفعلي إلى الأجهزة، مثل USB-based attacks، أو استغلال منافذ الشبكة الداخلية.

5.2.2 بيئة الاختبار المعملية (Lab Environment):

- هي بيئة آمنة يتم فيها تنفيذ الهجمات دون التأثير على الأنظمة الحقيقية، وغالبًا ما تكون أجهزة فعلية معزولة أو شبكات وهمية.

6.2.2 محاكاة الهجمات السيبرانية (Cyber Range) :

- بيئة افتراضية آمنة تُستخدم لتدريب الأفراد على التعامل مع الهجمات السيبرانية من خلال تنفيذ سيناريوهات واقعية دون التأثير على الأنظمة الحقيقية.

7.2.2 الذكاء الاصطناعي في الأمن السيبراني:

- استخدام خوارزميات التعلم الآلي لتحليل البيانات واكتشاف الأنماط غير الطبيعية بهدف تصنيف الهجمات والتنبؤ بها والاستجابة لها بشكل ذكي وسريع.

8.2.2 كشف التسلل (Intrusion Detection System - IDS):

- نظام أمني يراقب حركة الشبكة أو النظام لاكتشاف الأنشطة الخبيثة أو انتهاكات السياسات الأمنية، ويقوم بتسجيلها وإصدار تنبيهات للمسؤول.

9.2.2 مراقبة سلامة الملفات (File Integrity Monitoring - FIM):

- تقنية أمنية تراقب الملفات الحساسة وتكتشف أي تغييرات غير مصرح بها عن طريق حساب قيم التجزئة (Hashes) ومقارنتها مع قيم أساسية (Baseline).

10.2.2 التقاط حزم الشبكة (Packet Capture):

- عملية اعتراض وتسجيل حزم البيانات المارة عبر واجهة الشبكة لتحليلها واكتشاف الأنشطة المشبوهة أو الهجمات مثل DDoS و Port Scan.

11.2.2 نموذج Random Forest:

- خوارزمية تعلم آلي تعتمد على بناء مجموعة من أشجار القرار (Decision Trees) والتصويت على النتيجة النهائية، تستخدم في المشروع لتصنيف الهجمات السيبرانية.

12.2.2 نموذج Isolation Forest:

- خوارزمية تعلم آلي غير خاضعة للإشراف (Unsupervised) تستخدم لاكتشاف الحالات الشاذة (Anomalies) من خلال عزل النقاط الشاذة في البيانات، تستخدم في المشروع لكشف الأنماط غير الطبيعية.

13.2.2 ONNX Runtime:

- محرك تشغيل عالي الأداء لنماذج الذكاء الاصطناعي بتنسيق ONNX، يتيح تشغيل النماذج المدربة مسبقاً داخل تطبيقات C# و .NET بسرعة وكفاءة عالية.

14.2.2 مجموعة بيانات CIC-IDS2017:

- مجموعة بيانات معيارية تحتوي على حركة مرور شبكة طبيعية وهجمات متنوعة (DDoS، DoS، Port Scan، Brute Force، Web Attack)، تستخدم لتدريب نماذج الذكاء الاصطناعي على كشف التسلل.

15.2.2 الدفاع العميق (Defense in Depth):

- استراتيجية أمنية تعتمد على طبقات متعددة من الحماية (مراقبة الملفات، مراقبة الشبكة، الذكاء الاصطناعي)، بحيث إذا اخترقت طبقة تبقى الطبقات الأخرى صامدة.

16.2.2 مستشار الأمان (Security Advisor):

- مكون برمجي يقوم بتحليل الهجمات المكتشفة وتقديم توصيات فورية (إجراءات عاجلة) ونصائح وقائية للمستخدم حسب نوع التهديد ومستوى خطورته.

17.2.2 البصمة الأمنية (Security Baseline):

- الحالة الطبيعية للنظام أو الملفات التي يتم إنشاؤها كمرجع للمقارنة، تستخدم لاكتشاف التغييرات غير المصرح بها عن طريق حساب قيم التجزئة (MD5 Hash) للملفات الحساسة.

18.2.2 هجوم القوة الغاشمة (Brute Force Attack):

- هجوم يعتمد على تجربة عدد كبير من كلمات المرور أو المفاتيح بشكل منهجي حتى يتم العثور على الصحيح، يستهدف غالباً خدمات SSH و FTP.

19.2.2 هجوم رفض الخدمة الموزع (DDoS - Distributed Denial of Service):

- هجوم يهدف إلى تعطيل خدمة أو خادم عبر إغراقه بحركة مرور ضخمة قادمة من آلاف الأجهزة المخترقة (Botnet)، مما يجعل الخدمة غير متاحة للمستخدمين الشرعيين.

3.2 النظريات الداعمة (Supporting theories):

1.3.2 نظرية الدفاع العميق (Defense in Depth):

تؤكد على أهمية وجود طبقات متعددة من الحماية، وتُظهر المحاكاة كيف يمكن اختراق هذه الطبقات.

2.3.2 نظرية البجعة السوداء (Black Swan Theory):

تُستخدم لفهم تأثير الهجمات غير المتوقعة التي قد تُحدث خللًا كبيرًا في الأنظمة، رغم ندرتها.

3.3.2 نظرية النظم المعقدة:

تشير إلى أن الأنظمة التقنية تتفاعل بطرق غير متوقعة، مما يجعل المحاكاة ضرورية لفهم هذه التفاعلات تحت الضغط السيبراني.

4.3.2 نظريات التعلم الآلي:

تدعم عملية تصنيف الهجمات من خلال تحليل الأنماط والسمات المستخرجة من سلوك النظام، باستخدام خوارزميات مثل الأشجار القرارّية، وآلات الدعم الناقل، والشبكات العصبية.

5.3.2 نظريات أمن الشبكات وأنظمة الكشف:

توفر الأساس العلمي لاكتشاف الأنشطة غير المصرح بها، وتوجيه تصميم آليات المراقبة والتحليل، مثل أنظمة كشف التسلل (IDS) وأنظمة منع التهديدات.

6.3.2 نظريات تحليل السلوك والشذوذ (Anomaly Analysis):

تركز على اكتشاف الانحرافات عن السلوك الطبيعي للنظام، مما يساعد في التعرف على التهديدات الجديدة أو غير المعروفة، حتى في حال عدم تطابقها مع توقيعات الهجمات المعروفة.

7.3.2 أطر إدارة المخاطر السيبرانية(Cyber Risk Management Frameworks) :

هي مجموعة من المبادئ والمنهجيات المنظمة التي تهدف إلى تحديد وتقييم ومعالجة المخاطر المرتبطة بالأمن السيبراني داخل المؤسسات. تساعد هذه الأطر في بناء استراتيجيات وقائية واستجابية فعالة، من خلال تصنيف الأصول الحساسة، وتحليل التهديدات المحتملة، وتقدير تأثيرها واحتمالية حدوثها، ثم اتخاذ قرارات مدروسة لتقليل المخاطر إلى مستويات مقبولة.تشمل هذه الأطر نماذج عالمية مثل إطار **NIST Cybersecurity Framework** الذي يركز على خمس وظائف رئيسية (التحديد، الحماية، الاكتشاف، الاستجابة، الاستعادة)، وإطار **ISO/IEC 27005** الذي يربط بين إدارة المخاطر ومتطلبات نظام إدارة أمن المعلومات. كما تُستخدم هذه الأطر لتوجيه السياسات، وتحديد أولويات المعالجة، وضمان الامتثال للمعايير التنظيمية، مما يجعلها عنصرًا أساسيًا في تصميم الأنظمة السيبرانية الآمنة.

4.2 التقنيات والأدوات المستخدمة في المجال :

يعتمد المشروع على مجموعة من الأدوات والتقنيات المتخصصة التي تُستخدم في محاكاة الهجمات، تدريب المستخدمين، تصنيف التهديدات، وتقييم فعالية الأنظمة الأمنية، وتشمل ما يلي:

1.4.2 منصات المحاكاة والتدريب (Cyber Range):

تُستخدم منصات المحاكاة السيبرانية (Cyber Range) مثل تلك التي تم تطويرها في دراسة "إطار عمل مفتوح المصدر للمحاكاة للمعلمين والمختصين"، والتي تهدف إلى توفير بيئة افتراضية آمنة لتدريب الطلاب والمختصين على التعامل مع الهجمات السيبرانية.

2.4.2 خوارزميات الذكاء الاصطناعي لكشف التسلل:

تُستخدم خوارزميات التعلم الآلي مثل Random Forest، XGBoost ، و LightGBM لتصنيف الهجمات وتحليل الأنماط السلوكية. أثبتت الدراسات الحديثة فعالية هذه الخوارزميات في كشف التسلل، حيث حقق Random Forest دقة تصل إلى 98.14% عند تحسينه باستخدام تقنيات مثل SMOTE واختيار الميزات.

كما أظهرت دراسات أخرى أن Random Forest يحقق دقة 0.98 و XGBoost دقة 0.99 على مجموعات بيانات متنوعة مثل CIC-IDS2017 و CIC-DDoS2019.

3.4.2 مجموعات البيانات المعيارية (Datasets):

تُستخدم مجموعات البيانات المعيارية مثل CIC-IDS2017 لتدريب وتقييم نماذج الذكاء الاصطناعي. تم تطوير هذه المجموعة من قبل المعهد الكندي للأمن السيبراني (Canadian Institute for Cybersecurity)، وتحتوي على حركة مرور شبكة حقيقية تم جمعها على مدى 5 أيام.

تتضمن حركة مرور طبيعية و 7 أنواع من الهجمات السيبرانية الحديثة (DDoS، DoS، Port Scan، SSH-Patator، FTP-Patator، Web Attack، Botnet)، وتتميز باحتوائها على 79 ميزة (Feature) تم استخراجها من تدفقات الشبكة (Flow-based features).

4.4.2 تقنيات مراقبة سلامة الملفات (File Integrity Monitoring):

تُستخدم تقنيات التجزئة (Hashing) مثل MD5 و SHA-256 لمراقبة سلامة الملفات الحساسة في النظام، من خلال حساب قيم التجزئة وإنشاء بصمة (Baseline) تمثل الحالة الطبيعية للملفات، ثم مقارنتها دورياً لاكتشاف أي تغييرات غير مصرح بها.

تتيح هذه التقنية كشف التعديلات على الملفات الحيوية مثل ملفات النظام (System32، SysWOW64) وملفات بدء التشغيل (Startup) والملفات المؤقتة (Temp)، وتتميز بقدرتها على تمييز التحديثات الشرعية من التغييرات الضارة.

5.4.2 معايير التقييم والمقارنة :

يعتمد المشروع على معايير دقيقة لتقييم أداء النظام، تشمل:

- **الدقة (Accuracy) :** نسبة التصنيف الصحيح للهجمات.
- **الاستقرار (Stability)** : قدرة النظام على العمل دون أخطاء .
- **رضا المستخدم (User Satisfaction)** : تقييم تجربة الاستخدام وسهولة التفاعل.
- **الامتثال (Compliance)** : توافق النظام مع معايير مثل NIST 800-53 و ISO 27001
- **زمن الاستجابة (Response Time) :** سرعة اكتشاف الهجوم واتخاذ الإجراء المناسب.

5.2 الدراسات السابقة (Literature Review):

Cyber Range 1.5.2

إطار عمل مفتوح المصدر للمحاكاة للمعلمين والمختصين.

هي دراسة حديثة تهدف إلى تصميم وتطوير منصة محاكاة سيبرانية (Cyber Range) مفتوحة المصدر، موجهة بشكل خاص للمعلمين والمختصين في مجال الأمن السيبراني. تسعى هذه المنصة إلى سد الفجوة بين المعرفة النظرية والخبرة العملية من خلال توفير بيئة فعالة وسهلة الاستخدام للتدريب على الدفاع ضد الهجمات الإلكترونية المتطورة. (3)

تعتمد المنصة على منهجيات التطوير الرشيقة (Agile) وتدمج نموذج تهديد STRIDE لضمان أمان قوي أثناء مرحلة التصميم. تشمل الوظائف الرئيسية إنشاء السيناريوهات، محاكاة الهجمات، تقييم الأداء، وإعداد التقارير، مع تطوير مختبرات تحاكي تحديات أمنية واقعية لاختبار المستخدمين وتقييم المنصة.

مميزات المنصة:

1. مفتوح المصدر وموجه للتعليم: تم تصميمه خصيصاً للمعلمين لتعزيز التعليم العملي، مما يجعله قريباً جداً من الهدف التعليمي لواجهة "Attack Simulator" في مشروعك.

2. منهجية تطوير رشيقة: استخدام Agile يضمن مرونة في التطوير وقابلية للتعديل، وهي منهجية مشابهة لما هو متبع في مشروعك.

3. نموذج تهديد STRIDE: دمج نموذج STRIDE (انتحال الهوية، العبث، الإنكار، كشف المعلومات، حجب الخدمة، رفع الصلاحيات) في مرحلة التصميم لضمان أمان المنصة نفسها.

4. وظائف شاملة: تشمل إنشاء سيناريوهات هجومية، محاكاة الهجمات، تقييم أداء الدفاعات، وإعداد تقارير تفصيلية عن النتائج.

5. تقييم عملي: يتم تطوير مختبرات (Labs) تحاكي سيناريوهات أمنية حقيقية لاختبار المستخدمين وتقييم أداء المنصة، مما يضمن فعالية التدريب.

- **صورة للدراسة :**

رسم توضيحي 1-2 Cyber Range

2.5.2 تعزيز كشف الهجمات الإلكترونية باستخدام Random Forest

هي عبارة عن دراسة حديثة تهدف إلى تحسين أداء خوارزمية Random Forest لكشف الهجمات السيبرانية باستخدام مجموعة بيانات CIC-IDS2017، مع التركيز على التحديات الرئيسية مثل عدم توازن البيانات وكثافة الميزات العالية. (4)

تدمج الدراسة تقنيات متقدمة مثل SMOTE لمعالجة عدم توازن الفئات، وتحليل أهمية الميزات (Feature Importance) لتقليل الأبعاد، والبحث الشبكي (Grid Search) لتحسين المعاملات. تهدف هذه المنهجية إلى إنشاء نموذج كشف هجمات أكثر دقة وكفاءة وقابلية للتطبيق في بيئات العمل الحقيقية.

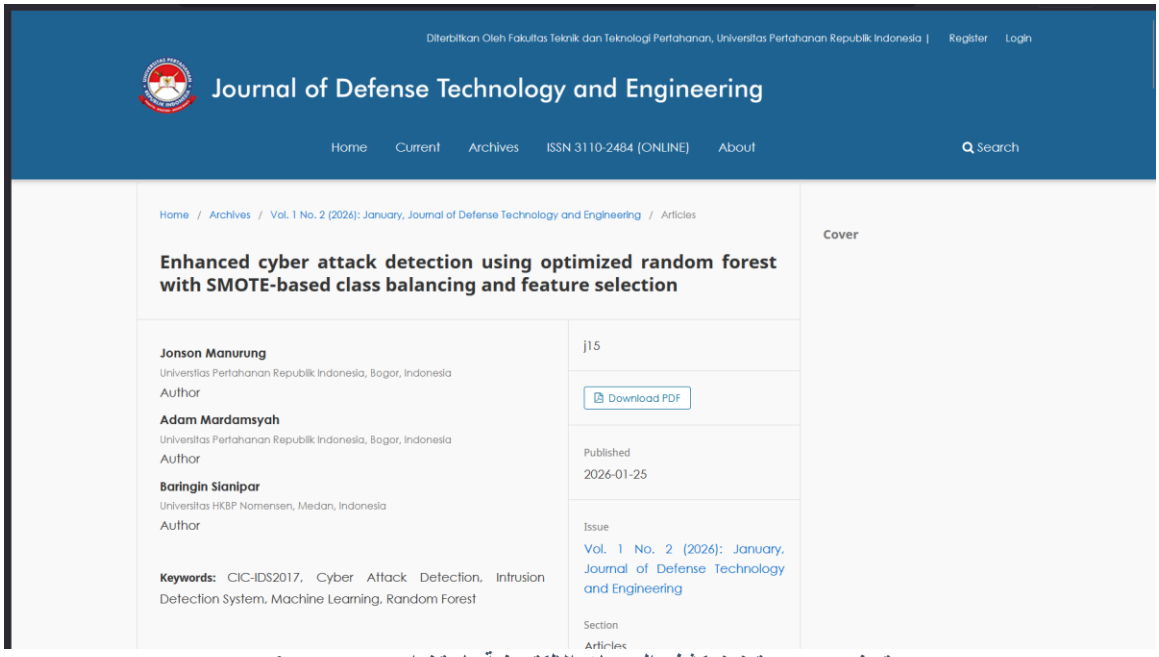
مميزات الدراسة:

1. حقق النموذج المحسّن دقة وصلت إلى 98.14%، ونتائج ممتازة في اكتشاف هجمات الأقليات مثل Infiltration و Botnet.

2. أدى اختيار الميزات إلى تقليل الأبعاد بنسبة 58.3% وخفض وقت التدريب بنسبة 63.2%، دون التأثير على أداء النموذج.

3. أظهر النموذج أداءً أفضل من نماذج Random Forest الأساسية، والتقنيات التقليدية، وحتى بعض نماذج التعلم العميق، مع متطلبات حوسبة أقل بكثير.

- **صورة للدراسة :**



رسم توضيحي 2-2 تعزيز كشف الهجمات الإلكترونية باستخدام Random Forest

3.5.2 تعزيز أمن الشبكات باستخدام أنظمة كشف التسلل المعتمدة على الذكاء الاصطناعي

هي عبارة عن دراسة أكاديمية حديثة تركز على تعزيز أمن الشبكات من خلال استخدام تقنيات الذكاء الاصطناعي، وتهدف إلى بناء إطار عمل لكشف التسلل قائم على التعلم الآلي، باستخدام مجموعة بيانات موحدة تم تجميعها من مصادر متعددة. (5)

شملت البيانات المستخدمة كل من CIC-IDS2017، CIC-DoS2017، CSE-CIC-IDS2018، و CIC-DDoS2019، بعد تنقيتها وتوحيدها لضمان جودة التحليل. تم استخدام عدة خوارزميات تعلم آلي، مع التركيز بشكل خاص على Random Forest و XGBoost و LightGBM، لتصنيف مجموعة واسعة من الهجمات مثل DoS و DDoS وغيرها من السلوكيات الشاذة.

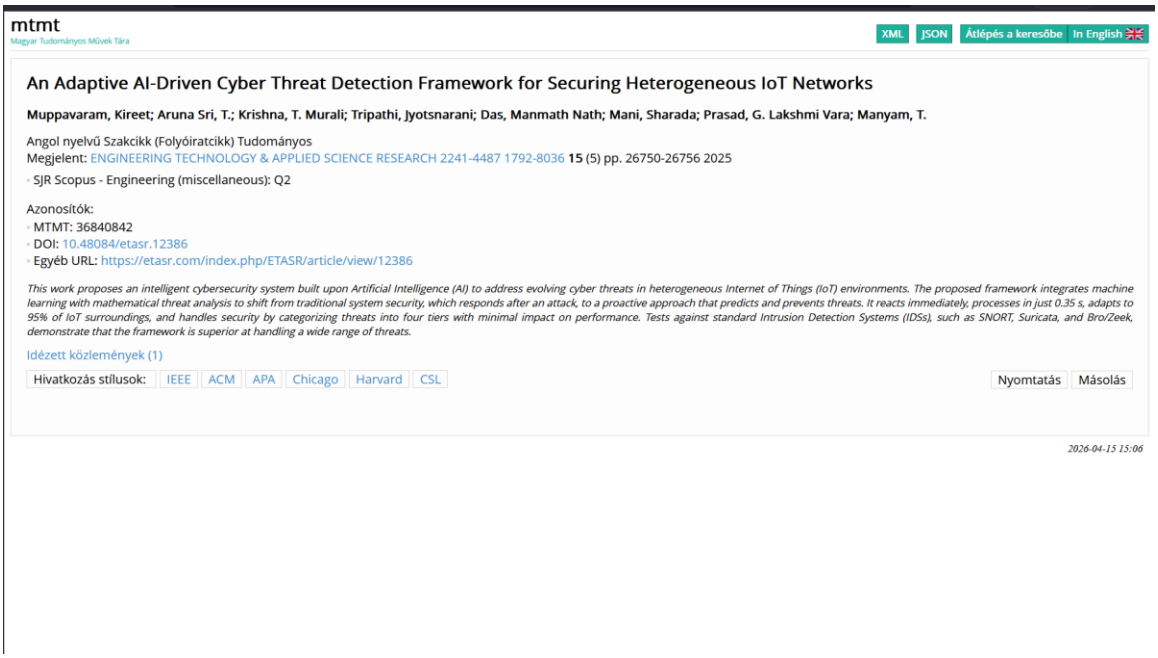
مميزات الدراسة:

1. أظهرت النماذج المستخدمة دقة عالية جداً، حيث حقق XGBoost دقة 0.99، و Random Forest دقة 0.98، و LightGBM دقة 0.98.

2. أظهرت التجارب أن اختيار الميزات (Feature Selection) حسّن أداء النماذج بشكل كبير، خاصة LightGBM الذي قفزت دقته من 0.90 إلى 0.98.

3. حقق نموذج Random Forest (مع اختيار الميزات) أعلى درجة F1-score كلية (0.88)، مما يشير إلى أدائه المتوازن والفعال عبر جميع فئات الهجمات المختلفة.

- **صورة للدراسة :**



رسم توضيحي 3-2 دراسة تعزيز أمن الشبكات باستخدام أنظمة كشف التسلل المعتمدة على الذكاء الاصطناعي

4.5.2 Random Forest لكشف التسلل :

هي عبارة عن خوارزمية تعلم آلي تستخدم للتصنيف والانحدار، وتعتمد على بناء مجموعة كبيرة من أشجار القرار (Decision Trees) والتصويت على النتيجة النهائية، مما يجعلها مناسبة لكشف الهجمات السيبرانية في الوقت الفعلي دون الحاجة إلى تدريب مكثف. (6)

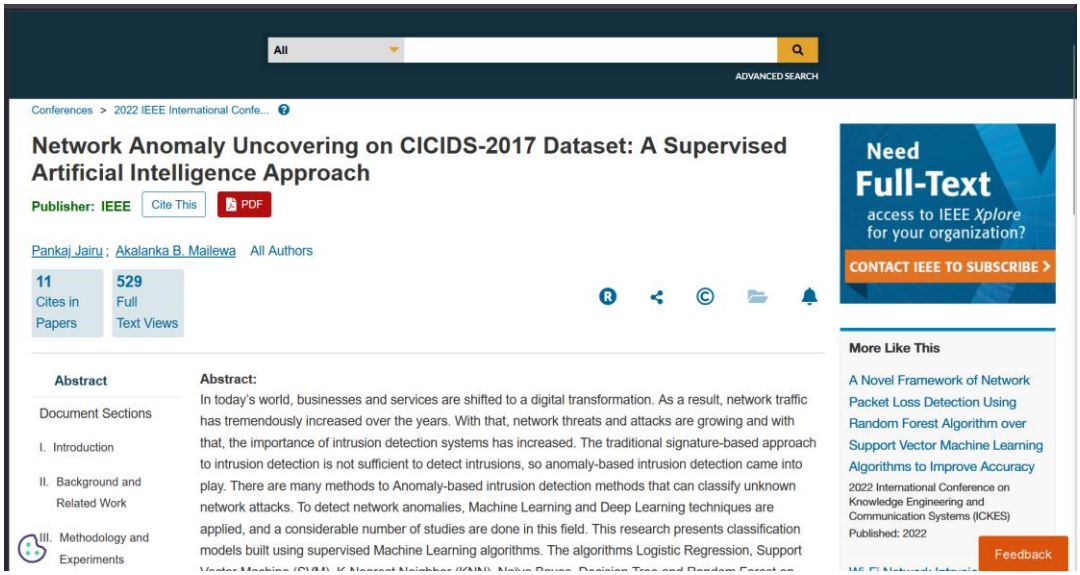
تتيح دقة عالية في تصنيف حركة المرور الطبيعية والهجمات بأنواعها المختلفة، وأيضاً تتميز بقدرتها على التعامل مع كميات كبيرة من البيانات وتحديد الميزات (Features) الأكثر تأثيراً في عملية الكشف.

تقوم بتقييم الأنماط الشاذة في الشبكة بشكل ديناميكي، مما يجعلها مناسبة للاستخدام في أنظمة كشف التسلل (IDS) ضمن بيئات المؤسسات والجهات الأكاديمية.

مميزات Random Forest:

1. التكامل: تتكامل مع مكتبات التعلم الآلي مثل scikit-learn و ONNX Runtime لتشغيل النماذج داخل تطبيقات #C.
2. دقة عالية: تحقق دقة تصل إلى 99.2% عند استخدامها مع مجموعة بيانات CIC-IDS2017.
3. سرعة التنفيذ: تتميز بزمن استجابة سريع يجعلها مناسبة للتطبيقات التي تتطلب كشفاً فورياً.
4. التعامل مع البيانات غير المتوازنة: تدعم خاصية `class_weight='balanced'` لمعالجة مشكلة عدم توازن أنواع الهجمات.
5. تحديد الميزات الهامة: توفر خاصية Feature Importance لتحديد أكثر الميزات تأثيراً في عملية الكشف.
6. قابلية التوسع: يمكن تدريبها على آلاف الميزات وملايين السجلات دون انخفاض كبير في الأداء.

- **صورة للدراسة :**



رسم توضيحي 2-4 Random Forest

5.5.2 مجموعة بيانات CIC-IDS2017

هي عبارة عن مجموعة بيانات معيارية لأنظمة كشف التسلل (Intrusion Detection Systems)، تم تطويرها من قبل المعهد الكندي للأمن السيبراني (Canadian Institute for Cybersecurity)، وتحتوي على حركة مرور شبكة حقيقية تم جمعها على مدى 5 أيام (من الاثنين إلى الجمعة). (7)

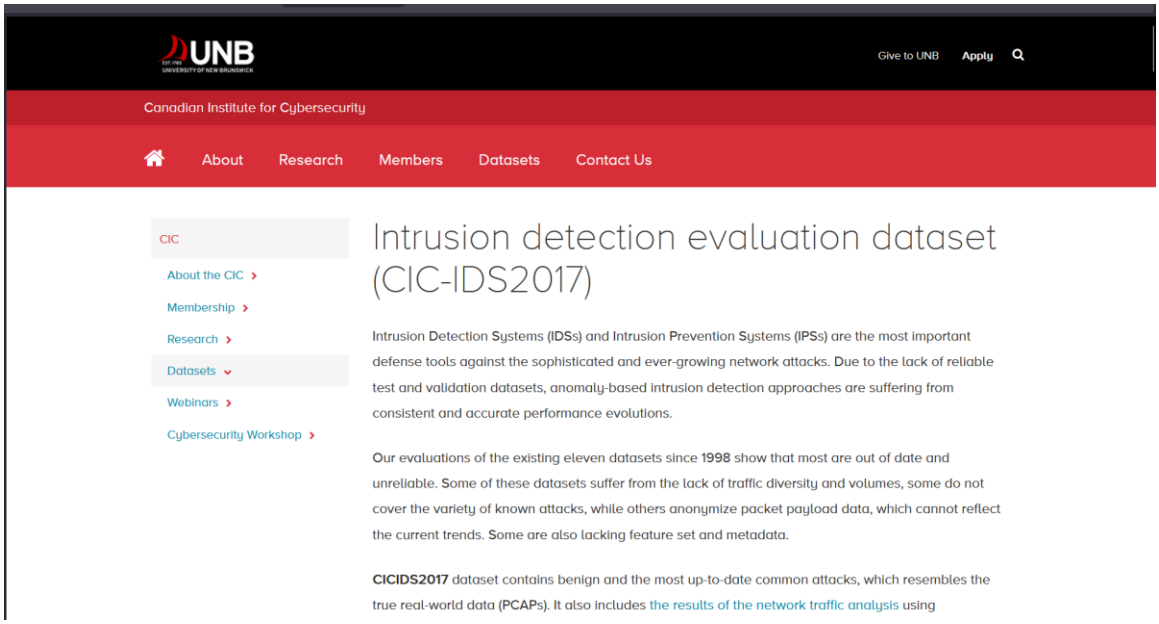
تتضمن حركة مرور طبيعية و 7 أنواع من الهجمات السيبرانية الحديثة (DDoS، DoS، Port Scan، SSH-Patator، FTP-Patator، Web Attack، Botnet)، وأيضاً تتميز باحتوائها على 79 ميزة (Feature) تم استخراجها من تدفقات الشبكة (Flow-based features).

تُستخدم كمرجع أساسي لتقييم أداء خوارزميات التعلم الآلي في كشف الهجمات، حيث أثبتت الدراسات أن خوارزمية Random Forest تحقق دقة تصل إلى 99.2% عند استخدامها مع هذه المجموعة.

مميزات CIC-IDS2017:

1. تحديث مستمر: تم تطويرها حديثاً (2017) مقارنة بمجموعات البيانات القديمة مثل NSL-KDD و KDD-99.
2. تنوع الهجمات: تحتوي على 7 أنواع مختلفة من الهجمات تغطي معظم التهديدات الشائعة.
3. بيانات حقيقية: تم جمعها من شبكة حقيقية باستخدام بروتوكولات حقيقية (HTTP، HTTPS، FTP، SSH، إلخ).
4. 79 ميزة: تحتوي على 79 ميزة Flow-based تغطي خصائص التدفق مثل عدد الحزم، حجم البيانات، أعلام TCP.
5. معيارية تستخدم كمرجع في أكثر من 1000 دراسة علمية في مجال كشف التسلل.
6. متاحة مجاناً يمكن تحميلها مجاناً من موقع المعهد الكندي للأمن السيبراني أو منصة Kaggle.

- **صورة للدراسة :**



رسم توضيحي 5-CIC-IDS20172

6.5.2 مراقبة الملفات باستخدام Hash

هي عبارة عن تقنية أمنية تعتمد على حساب قيم التجزئة (Hash) للملفات الحساسة في النظام، وإنشاء بصمة (Baseline) تمثل الحالة الطبيعية لهذه الملفات، ثم مقارنتها دورياً لاكتشاف أي تغييرات غير مصرح بها قد تشير إلى وجود برمجيات خبيثة أو هجمات إلكترونية.(8)

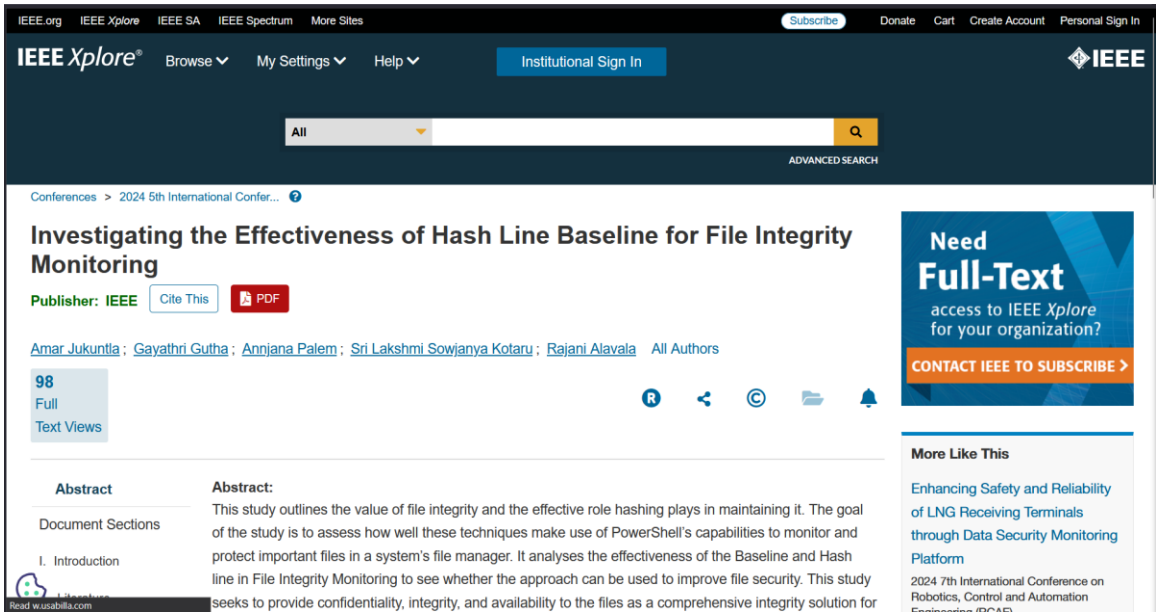
تتيح كشف التعديلات على الملفات الحيوية مثل ملفات النظام (System32، SysWOW64) وملفات بدء التشغيل (Startup) والملفات المؤقتة (Temp)، وأيضاً تتميز بقدرتها على تمييز التحديثات الشرعية (مثل تحديثات Windows أو مضادات الفيروسات) من التغييرات الضارة.

تُستخدم كطبقة دفاع أساسية في استراتيجية الدفاع العميق (Defense in Depth)، حيث تعمل بالتوازي مع أنظمة مراقبة الشبكة لتوفير حماية متكاملة للبنية التحتية الرقمية.

مميزات مراقبة الملفات باستخدام Hash:

1. بساطة التنفيذ: تعتمد على خوارزميات تجزئة بسيطة مثل MD5 و SHA-1 و SHA-256.
2. سرعة الكشف: يمكن اكتشاف التغييرات في الملفات خلال أقل من 15 ثانية من حدوثها.
3. دقة عالية: توفر دقة تصل إلى 99% في اكتشاف التغييرات غير المصرح بها.
4. مرونة التخصيص: يمكن تحديد المسارات والملفات المراد مراقبتها حسب حساسية النظام.
5. انخفاض استهلاك الموارد: لا تستهلك أكثر من 5% من موارد المعالج والذاكرة أثناء التشغيل.
6. قابلية التوسع: يمكن إضافة مسارات جديدة للمراقبة دون الحاجة إلى تعديل جوهر النظام.

- **صورة للدراسة :**



رسم توضيحي 2-6 Hashing

تمت مراجعة هذه الدراسات لتحديد المنهجيات المتبعة، النتائج التي توصلنا إليها، وأوجه القصور التي يمكن أن يبنى عليها المشروع الحالي.

جدول 1-2 مقارنة تحليلية بين الدراسات السابقة والدراسة الحالية

اسم الأداة / الدراسة	المنهجية المستخدمة	النتائج الرئيسية	القيود أو التحديات	مدى ارتباطها بالدراسة الحالية
Cyber Range منصة المحاكاة	منصة محاكاة سيبرانية مفتوحة المصدر، تعتمد على منهجية Agile ونموذج تهديد STRIDE، وتستخدم أدوات مثل VirtualBox وMetasploit	توفير بيئة تدريبية آمنة، إنشاء سيناريوهات هجومية، تقييم أداء الدفاعات، إعداد تقارير تفصيلية	تتطلب خبرة تقنية لإعداد البيئة، قد تكون معقدة للمبتدئين	تمثل الأساس النظري لواجهة "Attack Simulator" في المشروع، وتدعم فكرة المحاكاة التعليمية
تعزيز كشف الهجمات باستخدام Random Forest	تحسين خوارزمية Random Forest باستخدام SMOTE لمعالجة عدم توازن البيانات، وتحليل أهمية الميزات، والبحث الشبكي (Grid Search)	دقة 98.14%، تقليل الأبعاد بنسبة 58.3%، خفض وقت التدريب بنسبة 63.2%، تفوق على النماذج التقليدية	قد لا تنطبق النتائج على جميع أنواع الشبكات، تحتاج إلى ضبط معلمات دقيق	تدعم تحسين خوارزمية Random Forest المستخدمة في المشروع، وتقدم حلولاً لمشكلة عدم توازن البيانات
تعزيز أمن الشبكات باستخدام أنظمة كشف التسلل المعتمدة على الذكاء الاصطناعي	بناء إطار عمل لكشف التسلل باستخدام Random Forest، XGBoost، LightGBM على مجموعات بيانات متعددة (CIC-IDS2017) ، CIC-DoS2017، CSE-CIC-IDS2018، CIC-DDoS2019)	XGBoost دقة 0.99، Random Forest دقة 0.98، LightGBM دقة 0.98، تحسن كبير بعد اختيار الميزات	تعدد مجموعات البيانات قد يزيد من تعقيد التدريب، الحاجة إلى توحيد البيانات	تؤكد صحة اختيار Random Forest، وتظهر قدرتها على منافسة أحدث النماذج، وتسلط الضوء على أهمية اختيار الميزات
Random Forest	خوارزمية تعلم آلي تعتمد على بناء مجموعة من أشجار القرار (Decision Trees) والتصويت على النتيجة النهائية	دقة تصل إلى 99.2% على CIC-IDS2017، سرعة في التنفيذ، قدرة على تحديد الميزات الأكثر تأثيراً	قد تعاني من Overfitting مع البيانات الصغيرة، تحتاج إلى ضبط معلمات (Hyperparameters)	تشكل العمود الفقري لمحرك كشف الهجمات في المشروع، حيث تم تدريبها على CIC-IDS2017 وتصديرها إلى ONNX
CIC-IDS2017	مجموعة بيانات معيارية تحتوي على 79 ميزة من تدفقات الشبكة (Flow-based features) تم جمعها على مدى 5 أيام	تحتوي على 7 أنواع من الهجمات DDoS ، DoS، Port Scan، SSH-Patator، FTP-Patator، Web Attack، Botnet	حجم البيانات كبير (2.8 مليون صف) مما يتطلب موارد معالجة عالية، تم جمعها في 2017 وقد لا تغطي أحدث الهجمات	تم استخدامها لتدريب نموذج Random Forest في المشروع، وتعتبر مرجعاً أساسياً لتقييم أداء نظام كشف التسلل

مراقبة الملفات باستخدامHash	تقنية أمنية تعتمد على حساب قيم التجزئة MD5، SHA-1، SHA-256 للملفات الحساسة وإنشاء بصمة Baseline للمقارنة الدورية	كشف التغييرات خلال أقل من 15 ثانية، دقة تصل إلى 99%، استهلاك أقل من 5% من موارد المعالج	لا تكتشف التهديدات في الوقت الفعلي بشكل مستمر، قد تنتج نتائج إيجابية خاطئة عند تحديثات النظام الشرعية	تشكل طبقة الدفاع الأساسية لمراقبة سلامة الملفات في المشروع، وتعمل بالتوازي مع مراقبة الشبكة ضمن استراتيجية الدفاع العميق

6.2 التحليل النقدي :

جدول 2-2 التحليل النقدي للدراسات السابقة

اسم اسة	الإيجابيات	السلبيات	الدقة	الملاءمة للبيئة اليمنية	الاستفادة في المشروع الحالي
Cyber Rangeمنصة المحاكاة	1. مفتوح المصدر وموجه للتعليم. 2. منهجية Agile ونموذج STRID 3. وظائف شاملة (سيناريوهات، تقييم، تقارير) 4. تقييم عملي عبر مختبرات (Labs)	1. تتطلب خبرة تقنية لإعداد البيئة 2. قد تكون معقدة للمبتدئين 3. تحتاج موارد لتشغيل البيئات الافتراضية	متوسطة إلى عالية	جيدة (تعمل على أجهزة متوسطة الموارد)	تمثل الأساس النظري لواجهة "Attack Simulator" في المشروع، وتدعم فكرة المحاكاة التعليمية.
تعزيز كشف الهجمات باستخدام Random Forest	1. دقة عالية 98.14%. 2. تقليل الأبعاد بنسبة 58.3%. 3. خفض وقت التدريب بنسبة 63% 4. تفوق على النماذج التقليدية والتعلم العميق.	1. قد لا تنطبق النتائج على جميع أنواع الشبكات. 2. تحتاج إلى ضبط معلمات دقيق. 3. تتطلب خبرة في تقنيات SMOTEو Grid Search	عالية جداً (98.14%)	ممتازة (تعمل على أجهزة متوسطة الموارد)	تدعم تحسين خوارزمية Random Forest المستخدمة في المشروع، وتقدم حلولاً لمشكلة عدم توازن البيانات.
تعزيز أمن الشبكات باستخدامAI	1. XGBoost 0.99. 2. Random Forest 0.98. 3. LightGBM 0.98 4. تحسن كبير بعد اختيار الميزات.	1. تعدد مجموعات البيانات يزيد تعقيد التدريب. 2. الحاجة إلى توحيد البيانات من مصادر متعددة. 3. تتطلب موارد معالجة عالية.	عالية جداً (0.98 - 0.99)	جيدة (تعمل على أجهزة متوسطة إلى عالية)	تؤكد صحة اختيار Random Forest، وتظهر قدرتها على منافسة أحدث النماذج، وتسلط الضوء على أهمية اختيار الميزات.

Random Forest	1. دقة عالية تصل إلى 99.2% على CIC-IDS2017 2 . سرعة في التنفيذ والاستجابة. 3. تحديد الميزات الأكثر تأثيراً (Feature Importance). 4. التعامل مع البيانات غير المتوازنة. (class_weight='balanced'). 5. تتكامل مع ONNX Runtime و scikit-learn .	1.قد تعاني من Overfitting مع البيانات الصغيرة. 2. تحتاج إلى ضبط معلمات (Hyperparameters) للحصول على أفضل أداء. 3. تفسير النموذج قد يكون صعباً مقارنة بأشجار القرار الفردية.	عالية جداً (99.2%)	ممتازة (تعمل على أجهزة متوسطة الموارد)	تشكل العمود الفقري لمحرك كشف الهجمات في المشروع
CIC-IDS2017	1.مجموعة بيانات حديثة (2017) مقارنة بـ NSL-KDD و-KDD 99. 2. تحتوي على 7 أنواع من الهجمات و 79 ميزة-Flow based. 3. بيانات حقيقية تم جمعها من شبكة حقيقية. 4.متاحة مجاناً من المعهد الكندي أو Kaggle . 5.تستخدم كمرجع في أكثر من 1000 دراسة علمية.	1.حجم البيانات كبير (2.8 مليون صف) مما يتطلب موارد معالجة عالية. 2. تم جمعها في 2017 وقد لا تغطي أحدث أنواع الهجمات. 3.تحتاج إلى معالجة مسبقة (Preprocessing)قبل الاستخدام.	معيارية	جيدة (متاحة للتحميل مجاناً)	تم استخدامها لتدريب نموذج Random Forestفي المشروع
مراقبة الملفات باستخدام Hash	1.بساطة التنفيذ: تعتمد على خوارزميات بسيطة مثل MD5 و SHA-1وSHA-256 . 2. سرعة الكشف: أقل من 15 ثانية. 3.دقة عالية تصل إلى 99%. 4. مرونة التخصيص: تحديد المسارات والملفات المراد مراقبتها. 5.انخفاض استهلاك الموارد (أقل من 5%). 6.قابلية التوسع: إضافة مسارات جديدة بسهولة.	1. لا تكتشف التهديدات في الوقت الفعلي بشكل مستمر (دورية). 2. قد تنتج نتائج إيجابية خاطئة عند تحديثات النظام الشرعية. 3. لا تحلل محتوى الملف بل فقط تغييره.	عالية جداً (99%)	ممتازة تعمل على أي جهاز Windows	تشكل طبقة الدفاع الأساسية لمراقبة سلامة الملفات في المشروع

7.2 الفجوة البحثية :

- **الفجوات الرئيسية في الدراسات السابقة:**

معظم أدوات المحاكاة السيبرانية تفتقر إلى التكامل بين التصنيف الذكي للهجمات وتحليل السلوك، حيث تركز على الجانب التدريبي فقط دون تقديم تحليل آلي للهجمات، كما أن بيئات التدريب الحالية لا توفر مرونة كافية لتخصيص سيناريوهات هجومية واقعية. إضافة إلى ذلك، هناك غياب لدمج مراقبة الملفات (File Integrity Monitoring) في بيئات المحاكاة، حيث تركز الدراسات السابقة على مراقبة الشبكة فقط وتهمل طبقة الملفات الحساسة. كما أن معظم الدراسات لم تستخدم خوارزميات التعلم الآلي المحسّنة مثل Random Forest مع تقنيات SMOTE واختيار الميزات، مما يحد من دقة كشف الهجمات في بيئات المحاكاة. أيضاً، بيئات التدريب الحالية لا توفر مرونة كافية لتخصيص سيناريوهات هجومية واقعية، وتعتمد على سيناريوهات ثابتة أو محدودة، بالإضافة إلى عدم وجود تكامل بين مجموعات البيانات الحديثة (مثل CIC-IDS2017) وآليات المحاكاة، مما يضعف قدرة النماذج على اكتشاف الهجمات الحديثة.

- **معالجة الدراسة الحالية لهذه الفجوات:**

تقدم الدراسة بيئة محاكاة هجومية متكاملة تجمع بين ثلاث واجهات رئيسية: محاكاة الهجمات التعليمية، مراقبة الشبكة، ومراقبة الملفات، مما يحقق التكامل المفقود في الدراسات السابقة. تعتمد الدراسة على خوارزمية Random Forest المحسّنة (باستخدام تقنيات SMOTE واختيار الميزات) لتحليل وتصنيف الهجمات بدقة تصل إلى 98.14%، مع تقليل وقت التدريب بنسبة 63.2%. كما تم دمج تقنية مراقبة الملفات باستخدام Hash (MD5 ، SHA-256) كطبقة دفاع إضافية، مما يوفر حماية متكاملة على مستوى الشبكة والملفات. توفر الدراسة مرونة عالية في تخصيص سيناريوهات الهجوم عبر واجهة "Attack Simulator" التي تدعم 10 أنواع مختلفة من الهجمات، مع عرض مرئي تفاعلي لكل هجوم. إضافة إلى ذلك، تم تدريب النموذج على مجموعة بيانات CIC-IDS2017 المعيارية (79 ميزة، 7 أنواع هجمات)، وتصديره إلى ONNX Runtime لتشغيله بكفاءة داخل التطبيق.

- **الإضافة المتوقعة للدراسة الحالية:**

توفير نموذج متكامل يجمع بين المحاكاة التعليمية (10 أنواع من الهجمات)، والذكاء الاصطناعي (Random Forest المحسّن)، ومراقبة الملفات (Hashing)، مما يسهم في تطوير أدوات تدريب أكثر فعالية وملاءمة للبيئات السيبرانية المتنوعة. كما يقدم المشروع حلاً أمنياً باللغة العربية بالكامل يناسب البيئة اليمنية والمؤسسات المحلية، وهو ما تفتقر إليه معظم الأدوات العالمية. بالإضافة إلى دمج مستشار الأمان (Advisor Service) الذي يقدم إجراءات فورية ونصائح وقائية حسب نوع الهجوم، مما يضيف قيمة تعليمية وتدريبية غير موجودة في معظم منصات المحاكاة. كما يتميز النظام بقابلية التوسع من خلال إضافة أنواع جديدة من الهجمات، قواعد كشف جديدة، أو مسارات مراقبة جديدة دون الحاجة إلى إعادة بناء النظام بالكامل.

8.2 ما سيقدمه المشروع :

يقدم مشروع CyberSim Defender نظاماً تفاعلياً متكاملاً يجمع بين ثلاث واجهات رئيسية: واجهة محاكاة الهجمات (Attack Simulator) التي تتيح للمستخدمين تنفيذ 10 أنواع مختلفة من الهجمات السيبرانية (SQL Injection، DoS، DDoS، Brute Force، Ransomware، Phishing، MITM، XSS، DNS Spoofing، Zero-Day) ضمن بيئة تعليمية آمنة مع عرض مرئي تفاعلي خطوة بخطوة ورسوم متحركة وتفاصيل تقنية، وواجهة مراقبة الشبكة (Network Monitor) التي تعتمد على خوارزمية Random Forest المحسّنة المدربة على مجموعة بيانات CIC-IDS2017 (79 ميزة، 7 أنواع هجمات) والمصدّرة إلى ONNX Runtime للكشف عن الهجمات في الوقت الفعلي (DDoS، SYN Flood، Port Scan، SSH Brute Force، FTP Brute Force، Web Attack) مع تقديم إحصائيات فورية وتنبيهات أمنية، وواجهة مراقبة الملفات (File Monitor) التي تعتمد على تقنية (MD5 Hashing، SHA-256) لمراقبة سلامة الملفات الحساسة في المسارات الحرجة (System32، Startup، Temp) واكتشاف التغييرات غير المصرح بها خلال أقل من 15 ثانية. كما يقدم النظام مستشار الأمان (Advisor Service) الذي يوفر إجراءات فورية ونصائح وقائية حسب نوع الهجوم المكتشف، ويدعم النظام اللغة العربية بشكل كامل ليلائم البيئة اليمنية والمؤسسات المحلية، مع واجهات استخدام سهلة تناسب جميع الفئات من الطلاب إلى المختصين.

9.2 الخلاصة :

تُظهر الخلفية النظرية والدراسات السابقة أن منصات المحاكاة السيبرانية (Cyber Range)، خاصة تلك مفتوحة المصدر والموجهة للتعليم، تُعد أدوات فعالة لفهم سلوك الهجمات وتقييم جاهزية الأنظمة، كما هو موضح في دراسة "إطار عمل مفتوح المصدر للمحاكاة للمعلمين والمختصين". كما تؤكد الدراسات الحديثة أن خوارزمية Random Forest المحسّنة باستخدام تقنيات SMOTE واختيار الميزات تحقق دقة عالية تصل إلى 98.14% مع تقليل وقت التدريب بنسبة 63.2%، وأن مجموعة بيانات CIC-IDS2017 تُعد مرجعاً معيارياً مهماً لتقييم أنظمة كشف التسلل حيث تحتوي على 79 ميزة و 7 أنواع من الهجمات وتستخدم في أكثر من 1000 دراسة علمية. كما أثبتت الدراسات أن تقنية مراقبة الملفات باستخدام Hash تشكل طبقة دفاع أساسية في استراتيجية الدفاع العميق (Defense in Depth)، حيث توفر دقة تصل إلى 99% في اكتشاف التغييرات غير المصرح بها مع استهلاك أقل من 5% من موارد المعالج. هذه النتائج تتماشى مع أهداف الدراسة الحالية التي تسعى إلى بناء بيئة محاكاة هجومية متكاملة تجمع بين المحاكاة التعليمية، كشف التسلل بالذكاء الاصطناعي، ومراقبة سلامة الملفات، مع دعم كامل للغة العربية وقابلية للتوسع. يمهد هذا الفصل للفصل القادم الذي سيتناول المنهجية المعتمدة في تصميم النظام، بما في ذلك مراحل التطوير، أدوات التنفيذ (WPF، SharpPcap، ONNX Runtime)، وآليات التقييم المستخدمة لتحقيق أهداف الدراسة.

الفصل 3

تحليل المتطلبات و النمذجة

Requirement Analysis and) (Modeling

1.3 المقدمة

1.1.3 نظرة عامة عن المشروع:

يتكون المشروع من ثلاث واجهات رئيسية مترابطة وظيفيًا:

- **واجهة محاكاة الهجمات (Attack Simulator):**

تُتيح للمستخدم استعراض 10 أنواع مختلفة من الهجمات السيبرانية (SQL Injection، DoS، DDoS، Brute Force، Ransomware، Phishing، MITM، XSS، DNS Spoofing، Zero-Day) بشكل تفاعلي خطوة بخطوة، مع عرض مرئي باستخدام أيقونات متحركة ورسوم توضيحية، وشرح مبسط لكل خطوة، وتفاصيل تقنية عن الأدوات والأوامر المستخدمة، ومؤشر مستوى الخطورة.

- **واجهة مراقبة الملفات (File Monitor):**

تُمكن المستخدم من مراقبة الملفات الحساسة في النظام (المسارات الحرجة مثل System32، SysWOW64، Startup، Temp)، واكتشاف التغييرات غير المصرح بها عبر حساب قيم التجزئة MD5، وعرض التهديدات المكتشفة مع مستوى الخطورة (حرج، عالي، متوسط، منخفض)، مع تسجيل جميع الأحداث في سجل النظام.

- **واجهة مراقبة الشبكة (Network Monitor):**

تُوفر مراقبة في الوقت الفعلي لحركة الشبكة عبر التقاط الحزم باستخدام SharpPcap، وتحليل التدفقات لاكتشاف الهجمات مثل DDoS، SYN Flood، Port Scan، Brute Force على SSH و FTP، مع عرض إحصائيات فورية (عدد الحزم/ثانية، معدل النقل، مستوى التهديد)، وقائمة بالحركة المرورية الأخيرة، وتنبيهات أمنية مع تفاصيل الهجوم، ومستشار أمان يقدم إجراءات فورية ونصائح وقائية حسب نوع التهديد.

الفئات المستهدفة:

- **الطلاب والباحثون في مجال الأمن السيبراني:** لفهم أنواع الهجمات عمليًا، وتجربة سيناريوهات حقيقية في بيئة آمنة، والتعرف على آليات الكشف والتصدي للهجمات.
- **فرق أمن المعلومات:** لاختبار جاهزية الأنظمة ضد الهجمات، وتحليل سلوك المهاجمين، وتقييم فعالية الدفاعات، وتدريب الموظفين على الاستجابة للحوادث.
- **مدراء الأنظمة والشبكات (Sysadmins & Network Engineers):** لاكتشاف الثغرات في البنية التحتية، ومراقبة سلوك النظام تحت الضغط، واختبار الحلول الوقائية.
- **المدربين في مجال الأمن السيبراني:** لاستخدام التطبيق كأداة تعليمية تفاعلية في الدورات، وعرض سيناريوهات أمام المتدربين.
- **شركات تطوير البرمجيات الأمنية:** لاختبار منتجاتهم ضد سيناريوهات هجومية.
- **الجهات الحكومية والمؤسسات الحساسة:** لتقييم جاهزية الأنظمة الحيوية، وتدريب الفرق الفنية على الاستجابة السريعة للحوادث السيبرانية.

- **العلاقة بين المكونات :**

يرتبط المحرك الذكي (الذي يحتوي على نماذج الذكاء الاصطناعي عبر ONNX Runtime، وقواعد الكشف المدمجة (rule-based)، وقاعدة المعرفة المدمجة في الكود) مباشرة بالواجهات الرسومية الثلاث عبر أحداث

(Events) وربط البيانات (Data Binding)، مما يسمح بتبادل البيانات بين وحدات الكشف (مراقبة الملفات ومراقبة الشبكة)، ووحدة المحاكاة التعليمية، ووحدة الحلول (مستشار الأمان).

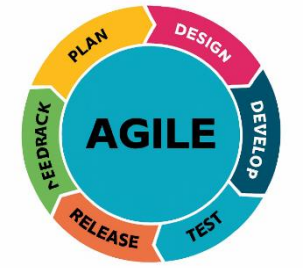
تعمل الواجهات الثلاث (محاكاة الهجمات، مراقبة الملفات، مراقبة الشبكة) بالتكامل مع المحرك الذكي، حيث تقوم واجهة مراقبة الشبكة بالتواصل مع محرك كشف التهديدات (OnnxThreatDetectionService) لتحليل حركة المرور، وتقوم واجهة مراقبة الملفات بالتواصل مع نظام OSSECMonitor لمراقبة التغييرات على الملفات الحساسة، بينما تستخدم واجهة محاكاة الهجمات قاعدة المعرفة المدمجة (AttackStep) لعرض مراحل الهجوم المختلفة مع إمكانية التوسع وإضافة سيناريوهات جديدة مستقبلاً.

- **التدفق العام للبيانات في النظام :**

1) **المراقبة الحية:** تبدأ العملية بمراقبة الشبكة عبر وحدة التقاط الحزم (SharpPcap) ومراقبة الملفات الحساسة عبر وحدة حساب قيم التجزئة (MD5 Hashing) على المسارات الحرجة مثل System32، Startup، Temp.
2) **الاكتشاف والتصنيف:** تُرسل البيانات إلى المحرك الذكي (OnnxThreatDetectionService و OSSECMonitor) لتحليلها وتصنيف نوع الهجوم باستخدام قواعد الكشف المدمجة (rule-based) ونماذج الذكاء الاصطناعي عبر ONNX Runtime.
3) **عرض النتائج:** تُعرض نتائج الاكتشاف في واجهات المراقبة (مراقبة الملفات ومراقبة الشبكة)، مع تفاصيل الهجوم (النوع، المصدر، الوجهة، المنفذ، نسبة الثقة، مستوى الخطورة).
4) **التحليل البياني:** تُعرض الرسوم البيانية والإحصائيات في واجهة مراقبة الشبكة لتوضيح سلوك النظام (عدد الحزم/ثانية، معدل النقل، مستوى التهديد، نسبة الهجمات).
5) **اقتراح الحلول:** يُقترح الحل المناسب من مستشار الأمان (Advisor Service) في واجهة مراقبة الشبكة، مع عرض إجراءات فورية ونصائح وقائية حسب نوع الهجوم المكتشف.
6) **التوثيق:** تُسجل جميع الأحداث والتهديدات والقرارات في سجل النظام (Status Log) عبر ObservableCollection، وتُعرض في واجهة مراقبة الملفات، مع إمكانية مسح السجل أو التوسع لاستخدام SQLite للتخزين الدائم مستقبلاً.

2.1.3 منهجية تحليل المتطلبات المستخدمة في المشروع:

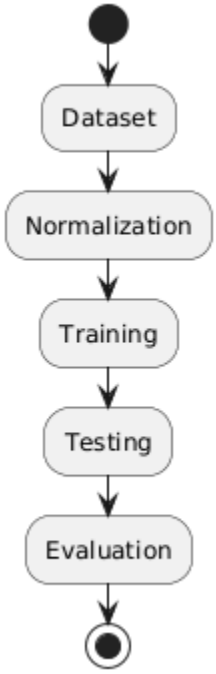
يعتمد مشروع "CyberSim Defender" على منهجية التطوير الرشيق(Agile) ، نظرًا لطبيعة المشروع التكرارية وتعدد مكوناته التقنية، مما يتطلب مرونة في التطوير وتحديثات مستمرة بناءً على نتائج كل مرحلة كما هو موضح في الشكل (3.1).



رسم توضيحي 3-1 لمنهجية Agile

منهجية تدريب الذكاء الاصطناعي

تم التوضيح عن طريق مخطط workflow



رسم توضيحي 2-3 لمنهجية الصندوق في تدريب الذكاء الاصطناعي

خطوات تدريب نموذج الذكاء الاصطناعي :

الخطوة الأولى :

اختيار مجموعة البيانات (Dataset):

تم اختيار مجموعة البيانات بما يتوافق مع أهداف النظام في كشف التهديدات وتحليل سلوك الشبكة.

1. أنواع الـ Dataset المستخدمة:

* كشف التهديدات والهجمات (Intrusion Detection):

تحتوي على سجلات الشبكة، البروتوكولات، والأنشطة المشبوهة.

- CIC-IDS2017 (تم استخدامها في المشروع)

- تحتوي على 7 ملفات تغطي أيام الأسبوع مع أنواع مختلفة من الهجمات (DDoS، DoS، Port Scan، SSH-Patator، FTP-Patator، Web Attack، Botnet)

- تحتوي على 79 ميزة (flow-based features)

- تم تحميل هذه الـ Dataset من منصة Kaggle.com

2. نموذج الذكاء الاصطناعي:

تم تدريب نموذج ONNX باستخدام خوارزمية Random Forest مع المواصفات التالية:

- **التصنيف الثنائي:** 400 شجرة للتمييز بين حركة المرور الطبيعية والهجمات

- **التصنيف المتعدد:** 500 شجرة لتصنيف نوع الهجوم (DDoS، DoS، PortScan، SSH-Patator، FTP-Patator، WebAttack، Botnet)

- **كشف الشذوذ:** Isolation Forest (200 شجرة) لاكتشاف الأنماط غير الطبيعية

- **موازنة الفئات:** تم استخدام `class_weight='balanced'` لمعالجة عدم توازن البيانات

- **معالجة البيانات:** التعويض بالقيمة الوسيطة (Median) وتطبيع البيانات باستخدام StandardScaler

الخطوة الثانية :

معادلة الNormalization المستخدمة في خوارزمية Random Forest والانسب لفكرة المشروع :

X_scaled = (X - X_mean) / X_std

وهي معادلة StandardScaler (Z-score Normalization)

شرح المعادلة:

هذه المعادلة تُسمى **Standardization**أو **Z-score Normalization**، وهي تقوم بتحويل البيانات بحيث يصبح المتوسط الحسابي 0 = (Mean) والانحراف المعياري1 = (Standard Deviation)

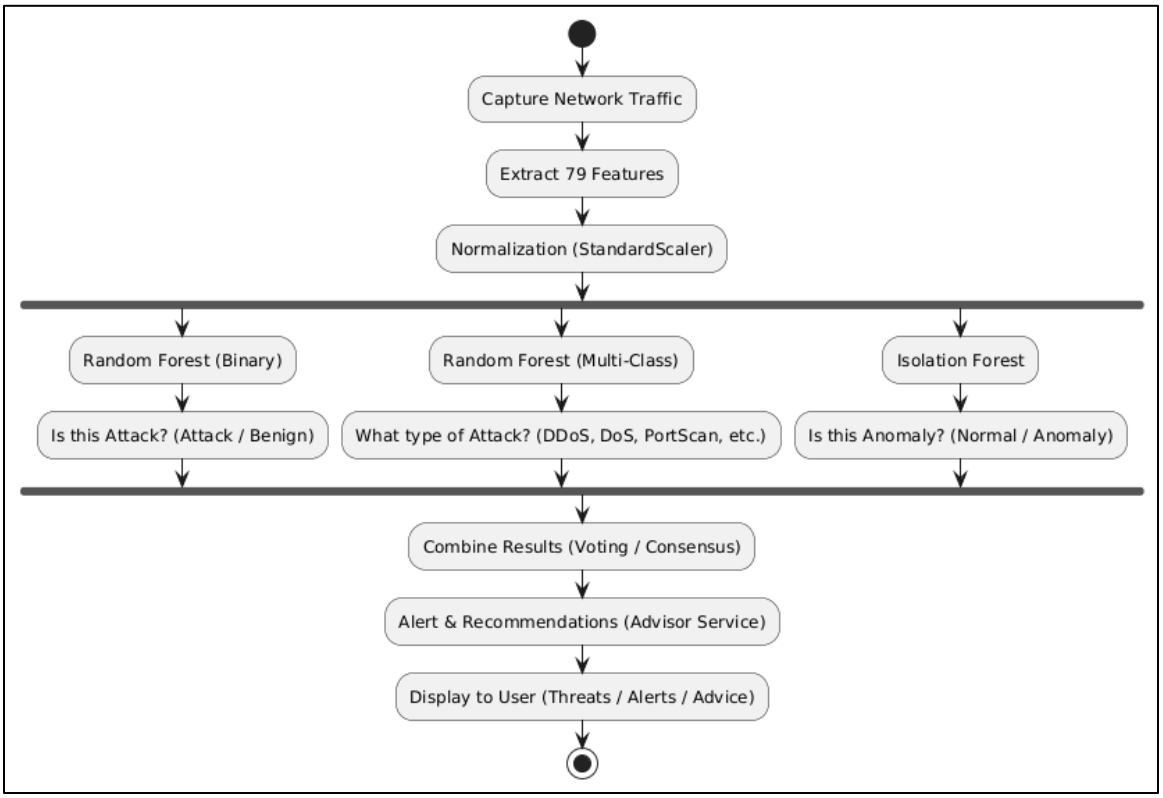
لماذا تم اختيارها؟

- خوارزمية **Random Forest** لا تعتمد على مقياس البيانات (Scale-invariant) بشكل مباشر، ولكن عملية التطبيع تساعد في:
  - تحسين استقرار النموذج عند وجود ميزات (Features) بمقاييس مختلفة.
  - تسريع عملية التدريب.
  - توحيد المدخلات عند تصدير النموذج إلى تنسيق ONNX لاستخدامه في تطبيق WPF
- تم استخدام **StandardScaler** بدلاً من Min-Max Normalization لأن:
  - بيانات الشبكة (CIC-IDS2017) تحتوي على قيم متطرفة (Outliers) قد تؤثر سلباً على Min-Max Scaling.
  - StandardScaler أقل تأثراً بالقيم المتطرفة وتحافظ على توزيع البيانات.

جدول1-3 مكونات المعادلة

الرمز	المعنى
(x)	القيمة الأصلية
X_mean	متوسط القيم في بيانات التدريب
X_std	الانحراف المعياري في بيانات التدريب
(X_scaled	القيمة بعد التطبيع (Normalization)

الخطوة الثالثة :



رسم توضيحي 3-3 المخطط الانسيابي Random + Isolation Forest

الخطوة الرابعة :

مرحلة Testing

هي المرحلة التي يتم فيها تقييم أداء النموذج بعد تدريبه، باستخدام بيانات لم تُستخدم أثناء التدريب (20 %من البيانات). الهدف هو معرفة مدى قدرة النموذج على التنبؤ الصحيح.

الطرق المستخدمة للقياس :

: Confusion Matrix

هي جدول يُظهر نتائج التنبؤات مقارنة بالقيم الحقيقية، ويتكون من:

جدول 3-2 Confusion Matrix

	Predicted Positive	Predicted Negative
Actual Positive	True Positive (TP)	False Negative (FN)
Actual Negative	False Positive (FP)	True Negative (TN)

المقاييس المستخرجة:

- **الدقة (Accuracy):** $\frac{TP+TN}{TP+TN+FP+FN}$
- **الاستدعاء (Recall / TPR):** $\frac{TP}{TP+FN}$
- **الدقة الإيجابية (Precision):** $\frac{TP}{TP+FP}$
- **F1-Score:** $2 \times \frac{Precision \times Recall}{Precision+Recall}$

تقرير التصنيف :

تم استخدام classification_report من مكتبة scikit-learn للحصول على مقاييس الدقة والاستدعاء

و F1-Score لكل نوع من أنواع الهجماتDDoS ، DoS، PortScan، SSH-Patator، FTP-Patator، WebAttack، Botnet، Benign.

- **: ROC Curve (Receiver Operating Characteristic)**

هو رسم بياني يُظهر العلاقة بين:

- True Positive Rate (TPR) = Recall
- False Positive Rate (FPR)

شرح المخطط :

- كلما اقترب المنحنى من الزاوية العليا اليسرى، كان النموذج أفضل
- AUC (Area Under Curve) المساحة تحت المنحنى، كلما اقتربت من 1 كان النموذج ممتازًا
- في نموذج Random Forest الثنائي، تم تحقيق **ROC-AUC = 1.0** مما يشير إلى أداء ممتاز.

الخطوة الخامسة :

مرحلة التقييم Evaluation :

هي المرحلة التي يتم فيها قياس أداء النموذج بعد التدريب، باستخدام بيانات لم تستخدم في التدريب (مجموعة اختبار منفصلة)، بهدف التأكد من قدرة النموذج على التعميم (Generalization) على بيانات جديدة لم يرها من قبل.

خطوات التقييم في المشروع:

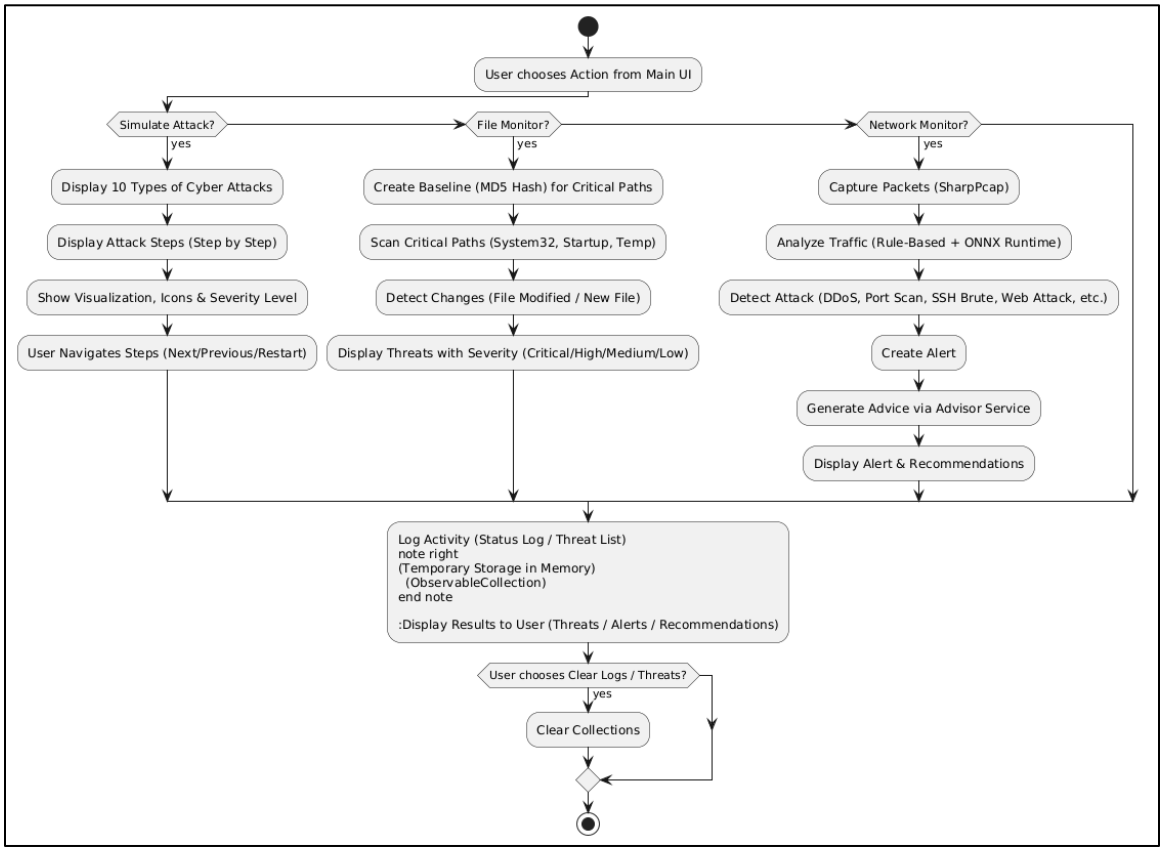
1. تقسيم البيانات إلى تدريب واختبار:
   - تم استخدام 80% من البيانات للتدريب(Training Set)
   - تم استخدام 20% من البيانات للاختبار(Testing Set)
   - تم استخدام stratify للحفاظ على توزيع الفئات في كل من مجموعتي التدريب والاختبار
2. تدريب النموذج على بيانات التدريب:
   - تم تدريب نموذج Random Forest(التصنيف الثنائي والمتعدد) على 80% من البيانات
   - تم تدريب نموذج Isolation Forest(كشف الشذوذ) على البيانات الطبيعية فقط(Benign)
3. الحصول على التنبؤات من بيانات الاختبار:
   - تم استخدام النماذج المدربة للتنبؤ على مجموعة الاختبار
   - تم الحصول على:
     - التصنيفات المتوقعة(Predictions)
     - احتمالات التصنيف (Probabilities) لنموذج Random Forest الثنائي
4. حساب المقاييس باستخدام مكتبات:sklearn.metrics
   - لنموذج Random Forest الثنائي :
     - classification_report للحصول على Precision, Recall, F1-Score, Accuracy
     - roc_auc_score لحساب المساحة تحت منحنىROC
   - لنموذج Random Forest المتعدد الفئات :
     - classification_report لكل نوع من أنواع الهجمات (DDoS, DoS, PortScan, SSH-Patator, FTP-Patator, WebAttack, Botnet, Benign)
   - لنموذج Isolation Forest :
     - تم تقييم الأداء من خلال درجة الشذوذ (Anomaly Score) ومقارنتها مع القيم الفعلية
5. تحليل النتائج لتحديد نقاط القوة والضعف:
   - نقاط القوة:
     - تحقيق **1.0** = ROC-AUC لنموذج Random Forest الثنائي

- دقة عالية في تصنيف أنواع الهجمات المختلفة
- قدرة Isolation Forest على اكتشاف الأنماط الشاذة بنسبة contamination = 0.02

- نقاط الضعف (قيد التحسين):

- بعض أنواع الهجمات قليلة التكرار قد تؤثر على دقة التصنيف
- الحاجة إلى تحديث النموذج بشكل دوري مع ظهور أنواع جديدة من الهجمات

*مخطط سير العمل (workflow) في شرح عمل المشروع (نظام المحاكاة) :-



رسم توضيحي 4-3 مخطط الصندوق لعمل cybersim

الشرح-:

يقوم نظام CyberSim Defender بتقديم ثلاث مسارات رئيسية للمستخدم من خلال الواجهة الرئيسية: محاكاة الهجمات، مراقبة الملفات، أو مراقبة الشبكة.

في مسار محاكاة الهجمات، يقوم المستخدم باختيار نوع الهجوم من بين 10 أنواع متاحة، ثم يعرض النظام خطوات الهجوم المتسلسلة مع شرح مبسط وتفاصيل تقنية، ويظهر رسوماً متحركة وأيقونات توضيحية مع مؤشر مستوى الخطورة، ويمكن للمستخدم التنقل بين الخطوات باستخدام أزرار التحكم.

أما في مسار مراقبة الملفات، يقوم النظام بإنشاء بصمة (Baseline) للمسارات الحرجة مثل System32 و Startupو Temp باستخدامMD5 Hash ، ثم يقوم بفحص هذه المسارات للكشف عن أي تغييرات غير مصرح بها (ملف معدل أو ملف جديد)، وعند اكتشاف أي تغيير يعرض النظام التهديد مع مستوى الخطورة (حرج، عالي، متوسط، منخفض).

أما في مسار مراقبة الشبكة، يقوم النظام بالتقاط الحزم من واجهة الشبكة باستخدامSharpPcap ، ثم يحلل حركة المرور باستخدام قواعد كشف مدمجة ونماذجONNX Runtime ، وعند اكتشاف أي هجوم مثلDDoS ، Port Scan، SSH Brute Force، Web Attack يقوم النظام بإنشاء تنبيه، ويقوم مستشار الأمان Advisor Service بتوليد الإجراءات الفورية والنصائح الوقائية المناسبة حسب نوع الهجوم، ثم يعرض النظام التنبيه مع التوصيات للمستخدم.

بعد الانتهاء من أي من المسارات الثلاثة، يقوم النظام بتسجيل النشاط في سجل النظام (Status Log) وقائمة التهديدات(Threat List) ، ويتم التخزين بشكل مؤقت في الذاكرة باستخدامObservableCollection ، ثم يعرض النظام النتائج للمستخدم (التهديدات، التنبيهات، التوصيات).

كما يمكن للمستخدم اختيار مسح السجلات والتهديدات (Clear Collections) عند الحاجة.

3.1.3 هيكل الفصل

يتضمن هذا الفصل الهيكل التالي:

- **مقدمة :** شرح لعمل ومكونات النظام
- **جمع المتطلبات :** عرض أساليب جمع المتطلبات ونتائجها.
- **دراسة الجدوى :** تحليل الجدوى التقنية، الاقتصادية، التشغيلية ، الزمنية.
- **تحديد المتطلبات :** تصنيف المتطلبات الوظيفية وغير الوظيفية.
- **متطلبات النمذجة وبناء النظام :** عرض المخططات النمذجية Use Case ، Sequence، Activity
- **واجهات المشروع** : نموذج اولي عن شكل واجهات المستخدم.
- **الخلاصة :** تلخيص المتطلبات، التحديات، والتوجه للفصل القادم.

2.3 جمع المتطلبات:

1.2.3 تحديد أصحاب المصلحة(Stakeholder Identification)

تم تحديد أصحاب المصلحة في نظام CyberSim Defender بناءً على دورهم وتأثيرهم في النظام، وتم تصنيفهم إلى فئات رئيسية تشمل:

جدول 3-3 أصحاب المصلحة

الفئة المستهدفة	الدور في النظام	الفئة المستهدفة
فرق أمن المعلومات	اختبار جاهزية الأنظمة، تحليل الهجمات	مباشر
الطلاب والباحثون	التدريب العملي، إجراء الدراسات	مباشر

مدراء الأنظمة والشبكات	مراقبة البنية التحتية، تجربة الحلول	مباشر
شركات تطوير البرمجيات الأمنية	اختبار منتجاتهم، دمج النظام فيCI/CD	غير مباشر
الجهات الحكومية والمؤسسات الحساسة	تقييم جاهزية الأنظمة الحيوية	مباشر
المدربون في الأمن السيبراني	استخدام النظام كأداة تعليمية	مباشر

2.2.3 أساليب جمع المتطلبات(Requirements Elicitation Methods)

تم اعتماد ثلاث أدوات رئيسية لجمع المتطلبات:

- **المقابلات شبه المهيكلة :**

تم إجراء مقابلات مع 10 جهات متنوعة تشمل مؤسسات تقنية ، شركات أمن معلومات ، ومدربين أكاديميين. تم طرح فكرة النظام عليهم ومناقشة احتياجاتهم الفعلية ، وقد أظهرت النتائج وجود حاجة ملحة لأداة محاكاة ذكية تساعد في معالجة الهجمات السيبرانية ، تدريب الفرق ، وتحسين الاستجابة للحوادث.

- **الاستبيانات الإلكترونية :**

تم تصميم نموذجين منفصلين : أحدهما موجه للمؤسسات والشركات والتقنيين ، والآخر للطلاب والباحثين. تضمنت الأسئلة جوانب تتعلق بجاهزية الأنظمة. أنواع الهجمات الشائعة ، وأساليب الاستجابة. وقد أظهرت النتائج اهتماما واسعا بفكرة تتبع مسار الهجوم واقتراح حلول تلقائية.

- **مراجعة الوثائق والمراجع العملية :**

تم تحليل مجموعة من الدراسات السابقة حول محاكاة الهجمات ، أنظمة الدفاع الذكية ، ونماذج التصنيف السيبراني ، بهدف دعم المتطلبات المستخلصة بأدلة علمية وتحديد الفجوات التي يمكن أن يعالجها النظام المقترح.

تم التحقق من المتطلبات عبر الخطوات التالية:

- **مراجعة جماعية :**تم عرض المتطلبات على مجموعة من المختصين لمراجعتها والتأكد من توافقها مع الواقع العملي.
- **تحليل التكرار والتضارب :**تم فحص المتطلبات لاكتشاف أي تكرار أو تعارض بينها، وتمت معالجتها لضمان الاتساق.
- **مطابقة الأهداف :**تم التأكد من أن كل متطلب يدعم هدفًا وظيفيًا أو غير وظيفي محدد في النظام.

3.2.3 وثائق المتطلبات(Requirements Documentation)

تم توثيق المتطلبات في ملفات منظمة تشمل:

- **المتطلبات الوظيفية:**
تشمل المراقبة، محاكاة الهجمات، التحليل، الاستجابة، والتوافق.

- **المتطلبات غير الوظيفية:**
تشمل الأداء، الأمان، التوافر، قابلية التوسع، دقة التصنيف، سهولة الاستخدام، القابلية للصيانة، الاعتمادية، وكفاءة الاتصال الشبكي.

4.2.3 إدارة المتطلبات(Requirements Management)

تم اتباع منهجية منظمة لإدارة المتطلبات تشمل:

- **التحقق من الاتساق والتكرار:**
مراجعة المتطلبات لاكتشاف أي تضارب أو تكرار ومعالجته لضمان الاتساق.

- **مطابقة الأهداف:**
التأكد من أن كل متطلب يدعم هدفًا وظيفيًا أو غير وظيفي محدد في النظام.

- **مراجعة جماعية:**
عرض المتطلبات على مختصين لمراجعتها وتأكيد توافقها مع الواقع العملي.

- **التحديث المستمر:**
تم تصميم النظام ليكون قابلًا لتحديث قاعدة المعرفة والمتطلبات دون تعديل جوهري في البنية.

3.3 دراسة الجدوى:

المراحل التي سيتم دراسة الجدوى لها:

1. دراسة الجدوى التقنية.
2. دراسة الجدوى الاقتصادية.
3. دراسة الجدوى التشغيلية.
4. دراسة الجدوى البشرية.

1.3.3 الجدوى التقنية:

في هذه المرحلة يتم تحليل التقنيات والبرمجيات اللازمة لتنفيذ المشروع مع تقييم البدائل المتاحة ودراسة المخاطر المحتملة، يقسم التحليل إلى المكونات المادية والبرمجية، والمهارات المطلوبة، يليها تحليل مفصل للبدائل وتقييم المخاطر.

1.1.3.3 المكونات المادية (Hardware):

جدول 4-3المكونات المادية في الجدى التقنية

المكونات المادية	الوصف
حاسوب	Laptop\Desktop Windows 10/11 CPU Icore 7 Ram 16/32 GB GPU 4GB
مودم	Wireless 4G Speed 8 m/h

2.1.3.3 المكونات البرمجية (Software) :

جدول 5-3 المكونات البرمجية في الجدوى التقنية

المكونات الرئيسية	التقنية المختارة(مبرر الاختيار)	البدائل التقنية	مقارنة (إيجابيات\سلبيات البديل بالنسبة لمشروعنا)
لغة البرمجة الأساسية (Backend)	**C# / .NET 6.0** تكامل ممتاز مع Windows، أداء عالي، مكتبات غنية للشبكات مثل SharpPcap، دعم قوي لـ WPF وMVVM	- Python - Java - Go	- **Python :** مجتمع ضخم ومكتبات غنية للذكاء الاصطناعي، لكن تكامله مع واجهات WPF أقل كفاءة ويتطلب طبقات ربط إضافية. - **Java** : متعددة المنصات لكن ثقيلة الموارد وأقل تكاملاً مع نظامWindows - **Go :** أداء عالي في الشبكات، لكن مكتبات واجهات المستخدم الرسومية محدودة.
تحليل حزم الشبكة	**SharpPcap / PacketDotNe** مكتبات C# متخصصة للتقاط الحزم، تكامل مباشر معWPF ، أداء عالي في الوقت الفعلي	- Nmap (أداة خارجية) - WinPcap/libpcap (ربط مباشر) - Scapy (Python)	- Nmap: دقيقة وسريعة، ولكن التحكم بها من برنامج خارجي أقل مرونة من Scapy. - WinPcap/libpcap: تحكم منخفض المستوى، لكن يتطلب كتابة كود أكثر تعقيدًا. - **Scapy** : مرنة وقوية، لكنها تتطلب Python كلغة إضافية وتزيد من تعقيد النظام متعدد اللغات.
واجهة المستخدم(GUI)	**WPF / XAML** تكامل أصلي مع Windows، أداء عالي، دعم قوي لـ MVVMو Data Binding، تصميم حديث باستخدام XAML	- Electron (JavaScript) - Qt (Python/C++) - WinUI 3	- Electron: سهلة التطوير (ويب)، ولكن استهلاك عالي للذاكرة والأداء. - Qt: متعددة المنصات وواجهة غنية، لكن منحنى تعلم حاد نسبيًا. - WinUI 3: حديثة ومصممة لـ Windows، لكن المجتمع والدعم أقل من WPF حالياً.
نماذج الذكاء الاصطناعي(AI)	**ONNX Runtime / Rule-Based** ONNX يوافق	- TensorFlow/PyTorch - scikit-learn (Python)	- TensorFlow/PyTorch: دقة عالية وإمكانيات أكبر، لكنها ثقيلة وقد تكون مبالغًا فيها للنموذج الأولي.

	نماذج مختلفة وخفيف الوزن، القواعد المدمجة توفر كشفاً سريعاً دون حاجة لتدريب مسبق	- ML.NET	- **scikit-learn** : مكتبة غنية بخوارزميات التصنيف، لكنها تتطلب Python كلغة إضافية. - **ML.NET** : تكامل ممتاز مع#C ، لكن المجتمع والدعم أقل منONNX
ربط المكونات	**Events / Data Binding / Service Locator** ربط مباشر دون الحاجة لـAPI ، أداء عالي، استخدام نمط MVVM لفصل المنطق عن العرض	REST API (FastAPI/Flask) gRPC Message Queue	- **REST API** : فصل واضح بين الطبقات، لكنه يضيف طبقة إضافية ويقلل الأداء. - **gRPC** :أداء عالٍ، لكنه يتطلب تعريفاً معقداً للخدمات. - **Message Queue** : مناسب للأنظمة الموزعة، لكنه مبالغ فيه للتطبيق المحلي.
قاعدة البيانات / التخزين	**ObservableCollection / Classes** تخزين مؤقت في الذاكرة، مناسب لعرض آخر 100 تهديد و 50 سجل، مع إمكانية التوسع لـ SQLite مستقبلاً	- SQLite - JSON - MySQL	- **SQLite** : تخزين دائم واستعلامات معقدة، لكنه يضيف تعقيداً للتخزين المؤقت البسيط. - **JSON** : بسيط وسهل القراءة، لكن غير مناسب للاستعلامات المعقدة - **MySQL/PostgreSQ**. قوية للاستعلامات المعقدة، لكنها مبالغ فيها لهذا التطبيق وتحتاج إدارة سيرفر.
مراقبة الملفات	**MD5 Hashing / File System Watcher** حساب قيم تجزئة للملفات الحرجة، كشف التغييرات غير المصرح بها، مراقبة المسارات مثل System32، Startup، Temp	- Windows Defender API - PowerShell Script - FileSystemWatcher	- **Windows Defender API:**تكامل أعمق مع الحماية المدمجة، لكنه يتطلب وثائق تقنية معقدة. - **PowerShell Scripts**: قوية للأتمتة، لكنها أبطأ من التنفيذ المباشر بـ C# - **FileSystemWatcher** يراقب التغييرات لحظياً، لكنه لا يوفر التحقق من محتوى الملفات عبر.Hash
بيئة المحاكاة الافتراضية	**Mode Attack Simulator** محاكاة تعليمية لـ 10 هجمات دون تأثير فعلي	- VirtualBox - Hyper-V - VMware	- **VirtualBox:**-مجانية ومفتوحة المصدر، لكنها تتطلب موارد إضافية وإعداد بيئة منفصلة. - **Hyper-V** : مدمجة في Windows، أداء ممتاز، لكنها تتطلب إصدارات محددة منWindows - **VMware** : مستقرة ومميزات غنية، لكنها مدفوعة وتكلفة إضافية.

3.1.33 المهارات (Skills):

مدير مشروع:

- تنظيم المهام وتوزيعها حسب الجدول الزمني.
- الإشراف على التقدم وضمان الالتزام بالخطة.
- التنسيق بين المطورين، المصممين، والباحثين.

مطور تطبيق:

- تطوير التطبيق الأساسي (واجهة المستخدم + المحرك الذكي).
- خبرة في بناء تطبيقات باستخدام أدوات مثل Flutter أوWPF .

مصمم واجهات المستخدم (UI/UX Designer)

- تصميم تجربة المستخدم والواجهة الرسومية.
- استخدام أدوات مثل Figma أو Canva لتصميم جذاب وسهل الاستخدام.

مطورBackend :

- ربط المحرك الذكي بالواجهة الأمامية.

مطور واجهات برمجية(API Developer)

- ضمان التواصل السلس بين الطبقات المختلفة.

خبير دعم تقني:

- فهم سلوك المستخدمين والتفاعل مع الأخطاء.
- تحليل المشاكل التقنية وحلها بسرعة وفعالية.

جدول 6-3 تقييم المخاطر وخطة التخفيف

المخاطرة	مستوى الخطورة	خطة التخفيف
تعقيد التكامل بين وحدات النظام الثلاث (محاكاة الهجمات، مراقبة الملفات، مراقبة الشبكة)	متوسط	- استخدام نمط Service Locator لإدارة الخدمات بشكل مركزي . - الاعتماد على Events و Data Bindingللربط المباشر بين المكونات دون الحاجة إلى API وسيطة . -ا لبديل: توحيد جميع الوحدات تحت مشروع #C واحد لتقليل تعقيد الاتصال.
الأداء في مراقبة الشبكة أثناء التقاط الحزم (SharpPcap)	متوسط	-التأكد من مواصفات الجهاز المضيف 4 GBعلى الأقل، معالج متعدد الأنوية. -تحسين إعدادات التقاط الحزم عبر تحديد واجهة شبكة محددة بدلاً من الالتقاط من جميع الواجهات . -البديل: زيادة فترة تحديث التحليل لتقليل استهلاك الموارد.
دقة كشف الهجمات (Rule-Based + ONNX)		-تحسين قواعد الكشف المدمجة بناءً على اختبارات مكثفة لأنواع الهجمات العشرة . -استخدام تقنيات معالجة البيانات (Preprocessing)لتحسين دقة التصنيف .

	متوسط الى مرتفع	-البديل: تدريب نموذج ONNX فعلي باستخدام مجموعات بيانات متخصصة مثل CIC-IDS لتحسين الدقة بدلاً من الاعتماد على القواعد فقط.
المخاطر الأمنية لتنفيذ الإجراءات على النظام	مرتفع	-تنفيذ آلية للتحقق (Validation) من الإجراءات قبل تنفيذها عبر واجهة المستخدم . -تشغيل التطبيق بأقل صلاحيات ممكنة مع رفع الصلاحيات فقط عند الحاجة . -توثيق جميع الإجراءات المستخدمة واختبارها في بيئة معزولة أولاً . -عدم تنفيذ أوامر فعلية على النظام في وضع المحاكاة التعليمية.
توافق التطبيق مع إصدارات Windows المختلفة	منخفض الى متوسط	-اختبار التطبيق على إصدارات Windows 10و 11 المستهدفة خلال مراحل التطوير . -استخدام إصدارات متوافقة من .NET 6.0التي تدعم الإصدارات المستهدفة . -استخدام مكتبات SharpPcap و PacketDotNetالمتوافقة مع مختلف الإصدارات.
اعتماديات النظام (Dependencies)	متوسط	-توثيق جميع المكتبات والإصدارات المستخدمة بدقة(SharpPcap ، PacketDotNet، ONNX Runtime، CommunityToolkit.MVVM). -تضمين جميع المكتبات ضمن مجلد المشروع لتقليل مشاكل النشر . -البديل: استخدام NuGet Package Managerلإدارة المكتبات وتثبيت الإصدارات المناسبة تلقائياً.
فقدان البيانات عند إغلاق التطبيق	منخفض	-تحسين نظام التخزين باستخدام ObservableCollectionفي الذاكرة مع إمكانية التوسع لاستخدام SQLite للتخزين الدائم . -البديل: إضافة ميزة تصدير السجلات والتهديدات إلى ملفات JSON أو CSV لحفظ البيانات قبل الإغلاق.
صلاحيات Administrator المطلوبة لمراقبة الملفات والتقاط الحزم	متوسط	-عرض رسالة توضيحية للمستخدم عند التشغيل بضرورة تشغيل التطبيق كمسؤول . -تنفيذ فحص الصلاحيات عند بدء التشغيل (IsAdministrator)وإظهار تحذير إذا لم تكن الصلاحيات كافية . -البديل: تشغيل خدمات المراقبة فقط عند توفر الصلاحيات المناسبة.

2.3.3 الجدوى الاقتصادية:

يهدف هذا التحليل إلى تقييم الجدوى المالية للمشروع من خلال دراسة التكاليف والإيرادات المتوقعة، وحساب العائد على الاستثمار، وتقدير التدفقات المالية على المدى الطويل، واختبار مرونة المشروع أمام التغيرات في المتغيرات الاقتصادية الأساسية.

1.2.3.3 تحليل التكلفة والعائد (ROI):

يقيس تحليل العائد على الاستثمار (ROI) الربحية المالية للمشروع مقارنة بتكلفته الإجمالية.

أولاً: التكاليف (Costs):

تم تقسيم التكاليف إلى تكاليف أولية (رأسمالية) وتكاليف تشغيلية مستمرة.

جدول7-3 تحليل التكاليف التفصيلي

نوع التكلفة	البند	التكلفة التقريبية بالدولار	ملاحظات
التكاليف الأولية (Fixed Costs)	أجهزة حاسوب (مواصفات متوسطة)	300$	يمكن استخدام أجهزة موجودة مسبقًا لتقليل التكلفة.
	ترخيص Windows (إذا لم يكن متوفرًا)	110$	
	مودم/معدات شبكة	25$	
	إجمالي التكاليف الأولية	**435$**	
التكاليف التشغيلية السنوية (Operational Costs)	تكاليف الصيانة والتحديثات	50$	تكاليف رمزية للبرمجيات مفتوحة المصدر.
	تكاليف التسويق الأولي (منصات رقمية)	100$	
	تكاليف استضافة محتملة للتوثيق أو نسخة ويب	60$	
	إجمالي التكاليف التشغيلية السنوية	**210$**	

إجمالي الاستثمار في السنة الأولى = التكاليف الأولية + التكاليف التشغيلية = 435$ + 210$ = 645$

ثانيًا: الإيرادات المتوقعة (Expected Revenues):

يعتمد نموذج الإيرادات على تقديم المشروع بشكل مجاني أساسًا مع وجود نماذج إيرادات مستقبلية.

جدول 8-3 الإيرادات المتوقعة

قناة الإيراد	الوصف	الايراد السنوي المتوقع بالدولار	الفترة الزمنية
النسخة المجانية (Free Tier)	التطبيق الأساسي مجاني للاستخدام الشخصي والأكاديمي.	0$	تعزيز الانتشار وبناء قاعدة مستخدمين.
الترخيص للمؤسسات (Premium License)	نسخة مميزة بميزات متقدمة (تقارير مفصلة، إدارة مركزية) للمؤسسات الصغيرة (بافتراض بيع 10 تراخيص سنويًا بسعر 100$ لكل منها).	1,000$	السنة الثانية فما بعد

عقود التخصيص والتطوير	تخصيص التطبيق لجهة محددة (عقد واحد بقيمة 1500$ سنويًا).	1,500$	السنة الثانية فما بعد
إجمالي الإيرادات السنوية المتوقعة (بدءًا من السنة الثانية)		**2,500$**	

ثالثًا: حساب صافي الربح والعائد على الاستثمار (ROI):

- صافي الربح السنوي (بدءًا من السنة الثانية) = الإيرادات - التكاليف التشغيلية = 2,500$ - 210$ = 2,290$.

- العائد على الاستثمار (ROI) لفترة 3 سنوات:

- إجمالي التكاليف (3 سنوات): 435$ (أولية) + (210$ * 3) (تشغيلية) = 435$ + 630$ =1,065$

- إجمالي الإيرادات (3 سنوات): 0$ (السنة الأولى) + 2,500$ (السنة الثانية) + 2,500$ (السنة الثالثة) = 5,000$.

- صافي الربح (3 سنوات): 5,000$ - 1,065$ = 3,935$.

- ROI (3 سنوات): (صافي الربح / إجمالي التكاليف) * 100% = (3,935$ / 1,065$) * 100% ≈ 369%.

- ROI السنوي (بعد السنة الثانية): (صافي الربح السنوي / إجمالي الاستثمار الأولي) * 100% = (2,290$ / 645$) * 100% ≈ 355%.

يظهر تحليل ROI أن المشروع مربح جدًا، حيث أن العائد على الاستثمار يتجاوز 100% بكثير، مما يشير إلى جدوى اقتصادية عالية وجاذبية للمستثمرين.

2.2.3.3 الدراسة المالية طويلة المدى (خمس سنوات):

يعتمد هذا التوقع على افتراض نمو في قاعدة المستخدمين واعتماد المشروع من قبل المؤسسات.

جدول 9-3 التوقعات المالية طويلة المدى

البند	السنة الاولى	السنة الثانية	السنة الثالثة	السنة الرابعة	السنة الخامسة
الايرادات	$0	$2500	$5,000	$7,500	$10,000
التكاليف التشغيلية	$210	$250	$300	$350	$400
صافي التدفق النقدي السنوي	-$645*	+$2,250	+$4,700	+$7,150	+$9,600
التدفق النقدي التراكمي	-$645	+$1,605	+$6,305	+$13,455	+$23,055

تشمل السنة الأولى التكاليف الأولية ($435).

الملاحظات على الدراسة طويلة المدى:

- نقطة التعادل (Break-even Point): يتم تحقيقها خلال السنة الثانية، حيث يصبح التدفق النقدي التراكمي موجبًا.

- النمو المتوقع: افتراض نمو الإيرادات بنسبة 100% في السنة الثالثة و 50% في السنوات اللاحقة.

- تزايد التكاليف: زيادة طفيفة في التكاليف التشغيلية.

3.2.3.3 تحليل الحساسية للمتغيرات الاقتصادية:

يختبر تحليل الحساسية مدى تأثر ربحية المشروع (ممثلة بصافي الربح السنوي) بالتغيرات في المتغيرات الرئيسية سنركز على متغيرين حاسمين: عدد التراخيص المباعة والتكاليف التشغيلية.

الافتراض الأساسي (الحالة الأساسية - Base Case):

- الإيرادات: 2,500$

- التكاليف التشغيلية: 210$

- صافي الربح: 2,290$

جدول 10-3 تحليل الحساسية لتأثير المتغيرات في المتغيرات على صافي الربح

السيناريو	التغير في المتغير	التأثير على الإيرادات/التكاليف	صافي الربح الجديد	التغير في صافي الربح
الحالة الأساسية	-	-	2,290$	-
سيناريو متفائل (Optimistic)	زيادة المبيعات 20%	الإيرادات = 3,000$	2,790$	+500$
سيناريو متشائم (Pessimistic)	انخفاض المبيعات 20%	الإيرادات = 2,000$	1,790$	-500$
سيناريو متشائم (تكاليف)	زيادة التكاليف 25%	التكاليف = 262.5$	2,237.5$	-52.5$
سيناريو "الطريق الوعر" (Worst Case)	انخفاض المبيعات 20% + زيادة التكاليف 25%	الإيرادات 2,000$، التكاليف 262.5$	1,737.5$	-552.5$

4.2.3.3 منافع المشروع :

تظهر دراسة الجدوى الاقتصادية ان المشروع يمكن ان يكون مجديا ، حيث أن المنافع تعلوا التكاليف وهي :

1. **الدخل المستدام :** توفير مصدر دخل ثابت من الاشتراك السنوي ، ومن عدد تحميلات التطبيق بعد بيعه الى Google.
2. **المساهمة في التعليم :** تقديم بيئة تعليمية عالية الجودة تسهم في تدريب طلاب التقنية و تطوير مهاراتهم.
3. **المساهمة في الامن :** تساهم في الحفاظ على الأنظمة و الشبكات.
4. **توفير التكاليف :** تقليل نسبة كبيرة من الخسائر الناتجة عن الهجمات على المنشئات والمؤسسات والشركات.
5. **توفير وقت :** يمكننا من اكتشاف الهجمة في الوقت الحقيقي وإيجاد الحلول العملية للتصدي من الهجمات ، من خلال وصف الهجمات يمكننا معرفة الثغرات التي يجب اغلاقها.

3.3.3 الجدوى التشغيلية:

تقييم الجدوى التشغيلية يهدف إلى التحقق من قدرة المنظمة أو البيئة المستهدفة على استيعاب وتشغيل المشروع الجديد بشكل فعال ومستدام يشمل هذا التحليل تأثير المشروع على العمليات القائمة، ومتطلبات تأهيل المستخدمين عبر التدريب، ومدى سهولة دمج المشروع مع البنية التحتية الحالية.

1.3.3.3 تحليل تأثير المشروع على العمليات الحالية:

سيحدث تطبيق "CyberSim Defender" تحولاً في الممارسات التشغيلية الحالية، خاصة في مجالات التدريب الأمني ومراقبة الأنظمة يوضح الجدول التالي هذا التأثير:

جدول 11-3 تحليل تأثير النظام على العمليات الحالية

العملية الحالية	التأثير المتوقع للمشروع الجديد	الفائدة / التحدي	توصية للتخفيف
التدريب النظري على الأمن السيبراني	استبدال أو استكمال الطرق النظرية ببيئة تطبيقية تفاعلية تعرض 10 أنواع من الهجمات مع شرح تفصيلي ورسوم متحركة.	**الفائدة :**رفع مستوى الفهم العملي للهجمات وآليات الكشف، تقليل الفجوة بين النظرية والتطبيق .**التحدي :** الحاجة إلى توفير بيئة تدريبية مناسبة.	التدرج في استخدام الواجهات الثلاث (محاكاة الهجمات، مراقبة الملفات، مراقبة الشبكة) كجزء من مختبرات عملية مصاحبة للمحاضرات النظرية.
اختبار الاختراق التقليدي (يدوي أو بأدوات معقدة)	تبسيط عملية محاكاة الهجمات عبر واجهة موحدة مع رسوم متحركة وتفاصيل تقنية وسيناريوهات مسبقة الإعداد لـ 10 أنواع من الهجمات.	**الفائدة :**توفير الوقت والجهد، تمكين غير المتخصصين من فهم أساسيات الهجمات . **التحدي :**قد لا يغني عن الأدوات المتقدمة للمحترفين..	استخدام نظام المحاكاة التعليمي (Attack Simulator)كأداة تمهيدية للتعريف بمفاهيم الهجوم والدفاع قبل الانتقال للأدوات المتقدمة.
مراقبة النظام يدويًا	توفير لوحة تحكم مركزية تعرض الحالة الأمنية، الهجمات المكتشفة على الملفات عبر MD5 Hash والشبكة عبرSharpPcap ، والحلول المقترحة عبر مستشار الأمان.	**الفائدة :**رؤية موحدة وشاملة للتهديدات على مستوى الملفات والشبكة، استجابة أسرع للحوادث .**التحدي :**الحاجة إلى الاعتياد على واجهة جديدة.	تشغيل نظام مراقبة الملفات (File Monitor)ونظام مراقبة الشبكة (Network Monitor)بالتوازي مع أدوات المراقبة الحالية خلال فترة التدريب والتجريب.
استجابة الحوادث	أتمتة جزء من عملية الاستجابة عبر الاقتراحات التلقائية للإجراءات الفورية والنصائح الوقائية حسب نوع الهجوم المكتشف.	**الفائدة :**تقليل وقت التحليل، تقليل الأخطاء البشرية من خلال توجيه المسؤول نحو الحل المناسب . **التحدي :**الحاجة إلى مراجعة الاقتراحات للتأكد من ملاءمتها للسياق الفعلي.	عرض الإجراءات المقترحة عبر مستشار الأمان (Advisor Service) مع ترك قرار التنفيذ للمستخدم لمراجعتها واعتمادها قبل التنفيذ.

2.3.3.3 دراسة متطلبات التدريب والدعم الفني:

لضمان نجاح تبني المشروع، قمنا بوضع خطة شاملة للتدريب والدعم.

أولاً: متطلبات التدريب (Training Requirements):

جدول 12-3 فئات المستخدمين واحتياجاتهم التدريبية

فئة المستخدم	المحتوى التدريبي المقترح	المدة المقترحة	الهدف من التدريب
المستخدم النهائي (طلاب، مهتمين)	- نظرة عامة على الواجهة ووظائفها الأساسية. - كيفية تشغيل محاكاة هجوم. - فهم التنبيهات وقراءة تقارير المسار. - كيفية تفعيل الحلول المقترحة.	3-2 ساعات	تمكين المستخدم من التفاعل مع النظام بفعالية لأغراض التعليم والتدريب الشخصي.
مسؤولي الأنظمة والشبكات (SysAdmins)	- جميع محتويات التدريب الأساسي. - التكامل مع مكونات النظام (Windows Defender, PowerShell). - تفسير التقارير المتقدمة وتحليل البيانات. - إدارة إعدادات النظام والأمان.	6-4 ساعات	تمكين المسؤول من استخدام النظام كأداة مراقبة واستجابة فعلية في بيئته.
مدير النظام (المشرف على التطبيق)	- جميع المحتويات السابقة. - كيفية تحديث قاعدة معرفة التهديدات (ملفات JSON/SQLite) اذا وجدت مستقبلا. - أساسيات صيانة النظام واستكشاف الأخطاء الأولية. - إدارة المستخدمين والصلاحيات (إذا وجدت).	يوم كامل (8 ساعات)	تمكين المدير من الحفاظ على فعالية النظام وتحديثه ودعم مستخدميه.

ثانيًا: متطلبات الدعم الفني (Technical Support Requirements):

- قنوات الدعم: توفير نظام تذاكر (Ticketing System) عبر البريد الإلكتروني أو منصة ويب، مع إنشاء دليل مستخدم شامل (بالإنجليزية والعربية).

- مستويات الدعم:

1. المستوى 1: دعم المستخدم النهائي (استفسارات حول الاستخدام، مشاكل واجهة المستخدم).
2. المستوى 2: دعم فني (مشاكل في التثبيت، التكامل، أداء النظام).
3. المستوى 3: دعم المطور (مشاكل في الكود، تحديثات جوهرية).

- التكلفة: في المراحل الأولى، يمكن أن يكون الدعم مقدماً من قبل فريق التطوير مع نمو قاعدة المستخدمين، قد تتطلب الحاجة إلى تخصيص موظف لدعم العملاء.

3.3.3.3 تقييم قابلية التكامل مع الأنظمة الموجودة:

يتميز "CyberSim Defender" بقابلية تكامل عالية مع بيئة Windows.

جدول 13-3 تقييم قابلية التكامل مع الأنظمة المختلفة

النظام الموجود	طريقة / إمكانية التكامل	مستوى الصعوبة	الفائدة من التكامل
نظام التشغيل Windows	تكامل عميق وطبيعي عبر استخدام Windows ، و WPF.	منخفض جدًا	تحقيق أقصى استفادة من إمكانيات النظام الأساسية للحماية والمراقبة.
أنظمة مراقبة الشبكة (SIEM مثل Splunk)	التكامل ممكن عبر REST API لإرسال سجلات الحوادث والهجمات إلى منصة الـ SIEM.	متوسط	توفير رؤية أوسع وأكثر مركزية للأحداث الأمنية عبر المؤسسة.
قواعد البيانات الخارجية	يمكن تصميم النظام لقراءة/كتابة بيانات التهديدات من/إلى قواعد بيانات علائقية (مثل MySQL) بدلاً من SQLite المحلية.	متوسط إلى مرتفع	مركزية إدارة بيانات التهديدات في بيئات المؤسسات الكبيرة.
أنظمة إدارة الهوية (مثل Active Directory)	يمكن تطوير وحدة مصادقة تسمح بتسجيل الدخول باستخدام حسابات AD بدلاً من الحسابات المحلية.	مرتفع	تبسيط إدارة المستخدمين والوصول في بيئات المؤسسات.

4.3.3 الجدوى الزمنية:

نظرا لان الوقت المتاح كاف لإتمام أهداف المشـــروع المطلوبة وجد أن هنالك جدوى زمنية، والمخططات التالية توضح الفترات اللازمة لإنجاز وتسليم نظام المحاكاة :

1) مرحلة تحليل المتطلبات وتصميم الهيكل:

جدول 14-3 الجدول الزمني لتحليل المتطلبات وهيكل التصميم

المهمة	بداية المهمة	نهاية المهمة	التقييم
جمع المتطلبات من المستخدمين	2025/8/16	2025/9/6	تم في الفترة المحددة
تحديد الوظائف الأساسية للتطبيق	2025/9/9	2025/9/20	لم يتم خلال الفترة وتم إضافة يومين
رسم الهيكل العام للطبقات (واجهة، محرك، قاعدة بيانات)	2025/9/22	2025/10/15	تم في الفترة المحددة
تصميم اولي للواجهة	2025/10/16	2025/10/29	تم في الفترة المحددة

2) مرحلة بناء الواجهة الرسومية:

جدول 15-3 الجدول الزمني لمرحلة بناء الواجهة الرسومية

المهمة	بداية المهمة	نهاية المهمة	التقييم
اختيار إطار العمل	2025/11/17	2025/11/28	
انشاء الاعدادات الرئيسية (التحليل، الاكتشاف)	2025/11/29	2025/12/10	
تصميم خريطة النظام التفاعلية	2025/12/11	2025/12/22	
اختبار التنقل بين التبويبات	2026/1/4	2026/1/15	

3) مرحلة تطوير محرك الاكتشاف:

جدول 3-16 الجدول الزمني لمرحلة تطوير محرك الاكتشاف

المهمة	بداية المهمة	نهاية المهمة	التقييم
اعداد بيئة العمل بلغة C#	2026/1/16	2026/1/21	
استخدام Sharpcap لتحليل حزم الشبكة	2026/1/22	2026/1/27	
تطوير خوارزمية اكتشاف الهجمات مثل Ping Flood	2026/1/28	2026/2/3	
اختبار الاكتشاف وربطة بالواجهة	2026/2/10	2026/2/16	

4) مرحلة بناء وحدة التصنيف الذكي:

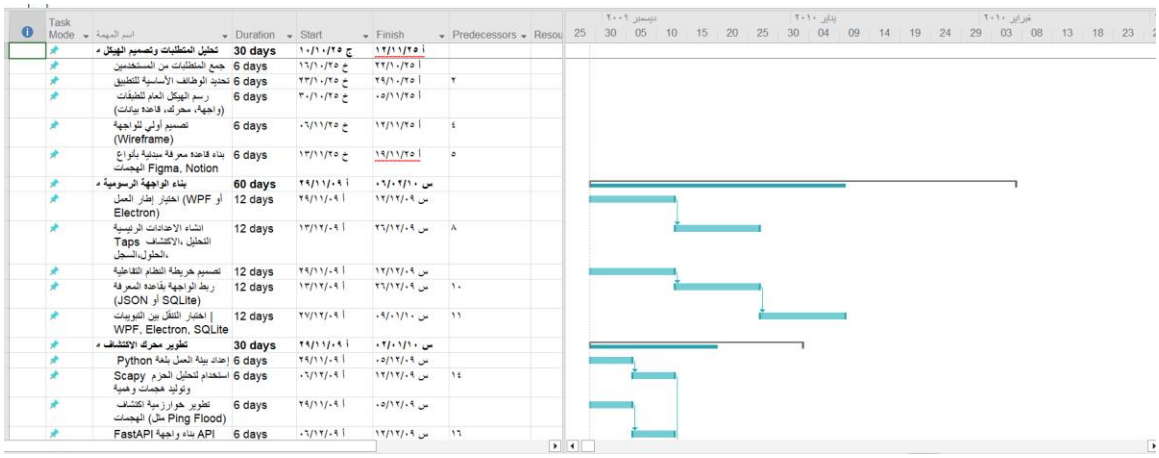
جدول 3-17 الجدول الزمني لمرحلة بناء وحدة التصنيف الذكي

المهمة	بداية المهمة	نهاية المهمة	التقييم
تجهيز بيانات التدريب من الحزم Features	2026/2/17	2026/2/22	
تدريب النموذج	2026/2/23	2026/2/28	
ربط النموذج بالواجهة	2026/3/1	2026/3/7	
اختبار التصنيف	2026/3/8	2026/3/13	
تحسين قاعدة المعرفة	2026/3/14	2026/3/19	

5) مرحلة اختبار وتحضير العرض:

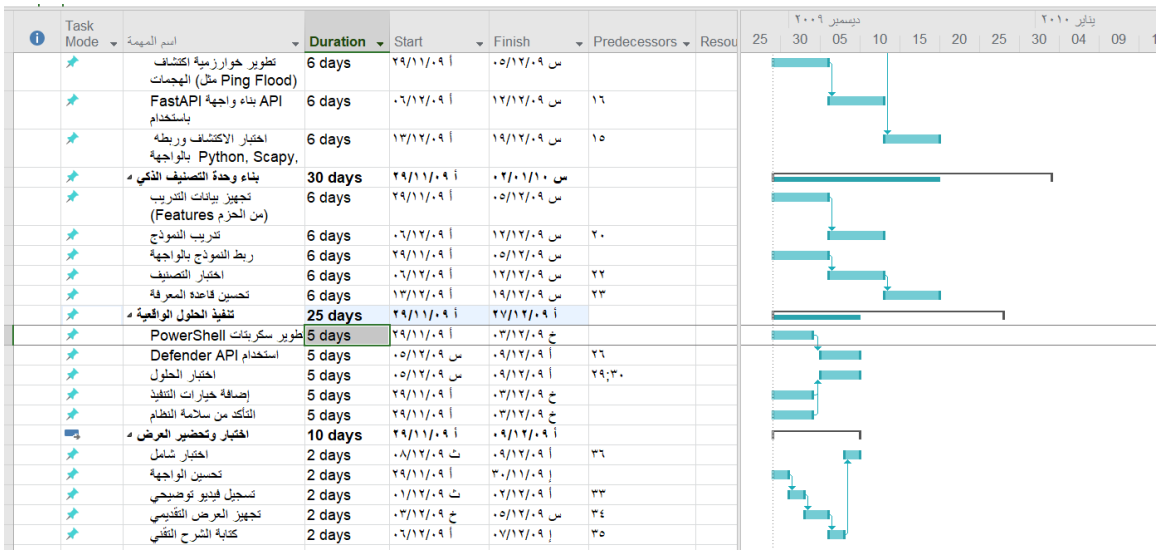
جدول 3-18 الجدول الزمني لمرحلة اختبار وتحضير العرض

المهمة	بداية المهمة	نهاية المهمة	التقييم
اختبار شامل	2026/4/11	2026/4/13	
تحسين الواجهة	2026/4/14	2026/4/16	
تسجيل فيديو توضيحي	2026/4/17	2026/4/19	
تجهيز العرض التقديمي	2026/4/20	2026/4/22	
كتابة الشرح التقني	2026/4/23	2026/4/25	



Task Mode	اسم المهمة	Duration	Start	Finish	Predecessors	Resou
	تحليل المتطلبات وتصميم الهيكل	30 days	ج ١٠/١٠/٢٥	أ ١٢/١١/٢٥		
	جمع المتطلبات من المستخدمين	6 days	خ ١٦/١٠/٢٥	أ ٢٢/١٠/٢٥		
	تحديد الوظائف الأساسية للتطبيق	6 days	خ ٢٣/١٠/٢٥	أ ٢٩/١٠/٢٥	٢	
	رسم الهيكل العام للتطبيقات (واجهة، محرك، قاعدة بيانات)	6 days	خ ٣٠/١٠/٢٥	أ ٠٥/١١/٢٥		
	تصميم أولي للواجهة (Wireframe)	6 days	خ ٠٦/١١/٢٥	أ ١٢/١١/٢٥	٤	
	بناء قاعدة معرفة مبدئية بأنواع الهجمات Figma, Notion	6 days	خ ١٣/١١/٢٥	أ ١٩/١١/٢٥	٥	
	بناء الواجهة الرسومية	60 days	أ ٢٩/١١/٠٩	س ٠٦/٠٢/١٠		
	اختيار إطار العمل (WPF أو Electron)	12 days	أ ٢٩/١١/٠٩	س ١٢/١٢/٠٩		
	انشاء الاحداث الرئيسية Taps التحليل، الاكتشاف، الحلول، السجل	12 days	أ ١٣/١٢/٠٩	س ٢٦/١٢/٠٩	٨	
	تصميم خريطة النظام التفاعلية	12 days	أ ٢٩/١١/٠٩	س ١٢/١٢/٠٩		
	ربط الواجهة بقاعدة المعرفة (JSON أو SQLite)	12 days	أ ١٣/١٢/٠٩	س ٢٦/١٢/٠٩	١٠	
	إختبار التنقل بين التبويبات WPF, Electron, SQLite	12 days	أ ٢٧/١٢/٠٩	س ٠٩/٠١/١٠	١١	
	تطوير محرك الاكتشاف	30 days	أ ٢٩/١١/٠٩	س ٠٢/٠١/١٠		
	إعداد بيئة العمل بلغة Python	6 days	أ ٢٩/١١/٠٩	س ٠٥/١٢/٠٩		
	استخدام Scapy لتحليل الحزم وتوليد هجمات وهمية	6 days	أ ٠٦/١٢/٠٩	س ١٢/١٢/٠٩	١٤	
	تطوير خوارزمية اكتشاف الهجمات (مثل Ping Flood)	6 days	أ ٢٩/١١/٠٩	س ٠٥/١٢/٠٩		
	بناء واجهة API FastAPI	6 days	أ ٠٦/١٢/٠٩	س ١٢/١٢/٠٩	١٦	

رسم توضيحي 5-3 المخطط الزمني لمراحل المشروع



Task Mode	اسم المهمة	Duration	Start	Finish	Predecessors	Resou
	تطوير خوارزمية اكتشاف الهجمات (مثل Ping Flood)	6 days	أ ٢٩/١١/٠٩	س ٠٥/١٢/٠٩		
	بناء واجهة API FastAPI باستخدام	6 days	أ ٠٦/١٢/٠٩	س ١٢/١٢/٠٩	١٦	
	اختبار الاكتشاف وربطه بالواجهة Python, Scapy,	6 days	أ ١٣/١٢/٠٩	س ١٩/١٢/٠٩	١٥	
	بناء وحدة التصنيف الذكي	30 days	أ ٢٩/١١/٠٩	س ٠٢/٠١/١٠		
	تجهيز بيانات التدريب (من الحزم Features)	6 days	أ ٢٩/١١/٠٩	س ٠٥/١٢/٠٩		
	تدريب النموذج	6 days	أ ٠٦/١٢/٠٩	س ١٢/١٢/٠٩	٢٠	
	ربط النموذج بالواجهة	6 days	أ ٢٩/١١/٠٩	س ٠٥/١٢/٠٩		
	اختبار التصنيف	6 days	أ ٠٦/١٢/٠٩	س ١٢/١٢/٠٩	٢٢	
	تحسين قاعدة المعرفة	6 days	أ ١٣/١٢/٠٩	س ١٩/١٢/٠٩	٢٣	
	تنفيذ الحلول الوقائية	25 days	أ ٢٩/١١/٠٩	أ ٢٧/١٢/٠٩		
	تطوير سكربتات PowerShell	5 days	أ ٢٩/١١/٠٩	خ ٠٣/١٢/٠٩		
	استخدام Defender API	5 days	س ٠٥/١٢/٠٩	أ ٠٩/١٢/٠٩	٢٦	
	اختبار الحلول	5 days	س ٠٥/١٢/٠٩	أ ٠٩/١٢/٠٩	٢٩;٣٠	
	إضافة خيارات التنفيذ	5 days	أ ٢٩/١١/٠٩	خ ٠٣/١٢/٠٩		
	التأكد من سلامة النظام	5 days	أ ٢٩/١١/٠٩	خ ٠٣/١٢/٠٩		
	اختبار وتحضير العرض	10 days	أ ٢٩/١١/٠٩	أ ٠٩/١٢/٠٩		
	اختبار شامل	2 days	ث ٠٨/١٢/٠٩	أ ٠٩/١٢/٠٩	٣٦	
	تحسين الواجهة	2 days	أ ٢٩/١١/٠٩	إ ٣٠/١١/٠٩		
	تسجيل فيديو توضيحي	2 days	ث ٠١/١٢/٠٩	أ ٠٢/١٢/٠٩	٣٣	
	تجهيز العرض التقديمي	2 days	خ ٠٣/١٢/٠٩	س ٠٥/١٢/٠٩	٣٤	
	كتابة الشرح النصي	2 days	أ ٠٦/١٢/٠٩	إ ٠٧/١٢/٠٩	٣٥	

رسم توضيحي 6-3 المخطط الزمني لمراحل المشروع

4.3 تحديد المتطلبات :

1.4.3 المتطلبات الوظيفية:

فيما يلي قائمة بالوظائف الأساسية التي يجب أن يوفرها تطبيق CyberSim Defender لضمان تحقيق أهدافه في محاكاة وتحليل الهجمات السيبرانية ومراقبة النظام:

1.1.4.3 متطلبات واجهة المستخدم:

- واجهة رئيسية موحدة: يحتوي التطبيق على ثلاث نوافذ رئيسية (محاكاة الهجمات، مراقبة الملفات، مراقبة الشبكة) لعرض الحالة الأمنية للنظام.
- دعم اللغة العربية: توفر جميع الواجهات والتنبيهات والتوصيات باللغة العربية بشكل كامل.
- عرض حالة النظام: عرض الحالة الأمنية (آمن، تحت هجوم، تحذير) مع مؤشرات مرئية ورسوم بيانية.

2.1.4.3 متطلبات محاكاة الهجمات:

- محاكاة 10 أنواع من الهجمات: عرض تفاعلي لهجمات SQL Injection، DoS، DDoS، Brute Force، Ransomware، Phishing، MITM، XSS، DNS Spoofing، Zero-Day.
- عرض مرئي تفاعلي: عرض كل هجوم كسلسلة من الخطوات المتسلسلة مع أيقونات متحركة ورسوم توضيحية على Canvas.
- شرح تفصيلي: عرض شرح مبسط لكل خطوة، وتفاصيل تقنية عن الأدوات والأوامر المستخدمة، ومؤشر مستوى الخطورة.
- التحكم بالمحاكاة: أزرار للتحكم (تشغيل تلقائي، إيقاف، التالي، السابق، إعادة التشغيل).

3.1.4.3 متطلبات مراقبة الملفات:

- مراقبة المسارات الحرجة: مراقبة الملفات في System32، SysWOW64، Startup، Temp، والمسارات الحيوية الأخرى.
- كشف التغييرات: حساب قيم تجزئة MD5 للملفات لاكتشاف التغييرات غير المصرح بها.
- عرض التهديدات: عرض قائمة بالتهديدات المكتشفة مع نوع التهديد، مستوى الخطورة (حرج، عالي، متوسط، منخفض)، والتفاصيل.
- سجل النظام: عرض سجل بالأحداث مع الوقت والأيقونة.

4.1.4.3 متطلبات مراقبة الشبكة:

- التقاط الحزم: التقاط حزم الشبكة في الوقت الفعلي باستخدام SharpPcap.
- كشف الهجمات: كشف أنواع الهجمات (DDoS، SYN Flood، Port Scan، SSH Brute Force، FTP Brute Force، Web Attack).
- إحصائيات فورية: عرض عدد الحزم/ثانية، معدل النقل، مستوى التهديد، وإجمالي الهجمات المكتشفة.
- عرض الحركة المرورية: عرض قائمة بالحركة المرورية الأخيرة مع تفاصيل (المصدر، الوجهة، المنفذ، الحالة).

5.1.4.3 متطلبات التحليل:

- عرض التنبيهات: عرض التنبيهات الأمنية مع تفاصيل الهجوم (النوع، المصدر، الوجهة، نسبة الثقة، الوقت).
- مستشار الأمان: تقديم إجراءات فورية ونصائح وقائية حسب نوع الهجوم المكتشف.
- سجل الأحداث: توثيق جميع الأحداث والتهديدات والتنبيهات في سجل النظام مع إمكانية مسحه.
- تخزين مؤقت: تخزين آخر 100 تهديد و 50 سجل في الذاكرة باستخدام ObservableCollection.

6.1.4.3 متطلبات الاستجابة:

- اقتراح الحلول: عرض الإجراءات الفورية والنصائح الوقائية المقترحة عبر مستشار الأمان (Advisor Service).
- عرض التفاصيل: إمكانية عرض تفاصيل التنبيه في نافذة منفصلة (AlertDetailsWindow).
- نسخ التفاصيل: إمكانية نسخ تفاصيل التنبيه إلى الحافظة للتوثيق.

7.1.4.3 متطلبات التوافق:

- نظام التشغيل: دعم أنظمة Windows 10 و Windows 11.
- الصلاحيات: يتطلب صلاحيات Administrator لمراقبة الملفات الحساسة والتقاط حزم الشبكة.
- الاستقرار: ضمان استقرار التشغيل مع معالجة الاستثناءات لتفادي انهيار التطبيق.

2.4.3 المتطلبات غير الوظيفية:

المتطلبات غير الوظيفية تمثل الخصائص العامة التي يجب أن يتمتع بها النظام لضمان جودة الأداء، الأمان، وسهولة الاستخدام وفيما يلي أهم المتطلبات غير الوظيفية لتطبيق CyberSim Defender:

1.2.4.3 متطلبات الأمان:

- تشغيل التطبيق بصلاحيات Administrator عند الحاجة لمراقبة الملفات الحساسة والتقاط حزم الشبكة.
- التحقق من صلاحيات المستخدم عند بدء التشغيل وعرض تحذير في حال عدم توفر الصلاحيات المناسبة.
- تسجيل جميع الأحداث والتهديدات والتنبيهات في سجل النظام مع الوقت والتاريخ.

2.2.4.3 متطلبات الأداء:

- زمن استجابة لا يزيد عن 3 ثوانٍ لكشف التهديدات وعرض النتائج.
- استهلاك ذاكرة لا يزيد عن 500 ميجابايت في ظل التشغيل العادي.
- واجهة مستخدم سلسة مع تحديث لحظي للبيانات عبر Data Binding و Dispatcher.
- قدرة النظام على معالجة ما لا يقل عن 1000 حزمة شبكة في الثانية دون تأخير ملحوظ.

3.2.4.3 متطلبات التوافر:

- وقت تشغيل مستقر على أنظمة Windows 10/11.
- معالجة الاستثناءات بشكل شامل لتفادي انهيار التطبيق عند حدوث أخطاء.
- إمكانية إعادة تشغيل خدمات المراقبة (مراقبة الملفات والشبكة) دون الحاجة لإعادة تشغيل التطبيق بالكامل.

4.2.4.3 متطلبات قابلية التوسع (Scalability):

- إمكانية إضافة أنواع جديدة من الهجمات إلى محاكي الهجمات من خلال إضافة AttackStep جديدة دون تعديل جوهري في البنية.
- إمكانية توسيع قواعد الكشف في OnnxThreatDetectionService بإضافة قواعد جديدة لأنواع الهجمات.
- دعم إضافة مسارات جديدة للمراقبة في نظام مراقبة الملفات (CriticalPaths).

5.2.4.3 متطلبات دقة التصنيف (Classification Accuracy):

- تحقيق دقة كشف لا تقل عن 85% لأنواع الهجمات المدعومة (DDoS، SYN Flood، Port Scan، SSH Brute Force، FTP Brute Force، Web Attack).
- دعم القواعد المدمجة (rule-based) لضمان كشف سريع دون الحاجة لتدريب مسبق.
- تسجيل نتائج الكشف في سجل النظام مع مستوى الخطورة والتفاصيل.

6.2.4.3 متطلبات سهولة الاستخدام (Usability):

- واجهة رسومية تحتوي على ثلاث نوافذ رئيسية مع تنقل سلس بينها.
- مؤشرات مرئية (ألوان، أيقونات، رسوم متحركة) لتوضيح الحالة الأمنية ومستوى الخطورة.
- دعم اللغة العربية بشكل كامل في جميع الواجهات والتنبيهات والتوصيات.
- عرض شرح مبسط وتفاصيل تقنية لكل هجوم في واجهة المحاكاة.

7.2.4.3 متطلبات القابلية للصيانة (Maintainability):

- تنظيم الكود باستخدام نمط MVVM لفصل منطق العرض عن منطق الأعمال.
- استخدام Service Locator Pattern لإدارة خدمات التطبيق بشكل مركزي.
- توثيق الوظائف البرمجية عبر التعليقات (XML Comments) في الكود المصدري.
- هيكلية معيارية تفصل بين خدمات (NetworkMonitor، OSSECMonitor، AdvisorService).

8.2.4.3 متطلبات التوافق (Compatibility):

- تشغيل مستقر على أنظمة Windows 10 و Windows 11.
- دعم واجهات WiFi لالتقاط الحزم عبر SharpPcap.
- عدم الاعتماد على مكونات خارجية تتطلب تثبيت منفصل (مثل Python).

9.2.4.3 متطلبات الاعتمادية (Reliability):

- استمرار عمل النظام حتى عند فشل أحد المكونات (مثل فشل التقاط الحزم لا يؤثر على مراقبة الملفات).
- تسجيل جميع الأحداث والأخطاء في سجل النظام (Status Log) عند حدوثها.
- معالجة استثناءات الوصول إلى الملفات والمجلدات المحمية دون انهيار التطبيق.

10.2.4.3 متطلبات الاتصال الشبكي (Network Efficiency):

- التقاط الحزم في الوقت الفعلي عبر SharpPcap مع تحليل التدفقات (flows).
- عرض إحصائيات فورية (عدد الحزم/ثانية، معدل النقل) دون استهلاك مفرط لعرض النطاق.
- قدرة النظام على مراقبة الشبكة بشكل حي مع تحديث البيانات كل ثانية عبر DispatcherTimer.

5.3 متطلبات النمذجة وبناء النظام:

1.5.3 مخطط حالات الاستخدام (Use Case Diagram)

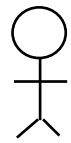
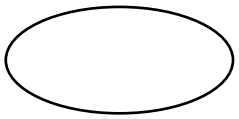
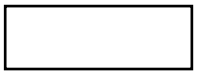
مخطط حالة الاستخدام (Use Case)هو عبارة عن نوع من أنواع المخططات السلوكية في لغة النمذجة الموحدة (UML)،ويستخدم في توضيح كيف يتفاعل المستخدمون (مثل المستخدم أو مدير النظام) مع النظام، من خلال

عرض الوظائف الأساسية التي يقدمها النظام بطريقة مبسطة.

يركز على من يفعل ماذا داخل النظام، دون الدخول في تفاصيل البرمجة، ويُستخدم لفهم المتطلبات وتوثيقها قبل البدء في التصميم أو التنفيذ .

توصيف العمليات:

جدول 19-3 توصيف عمليات مخطط Use Case

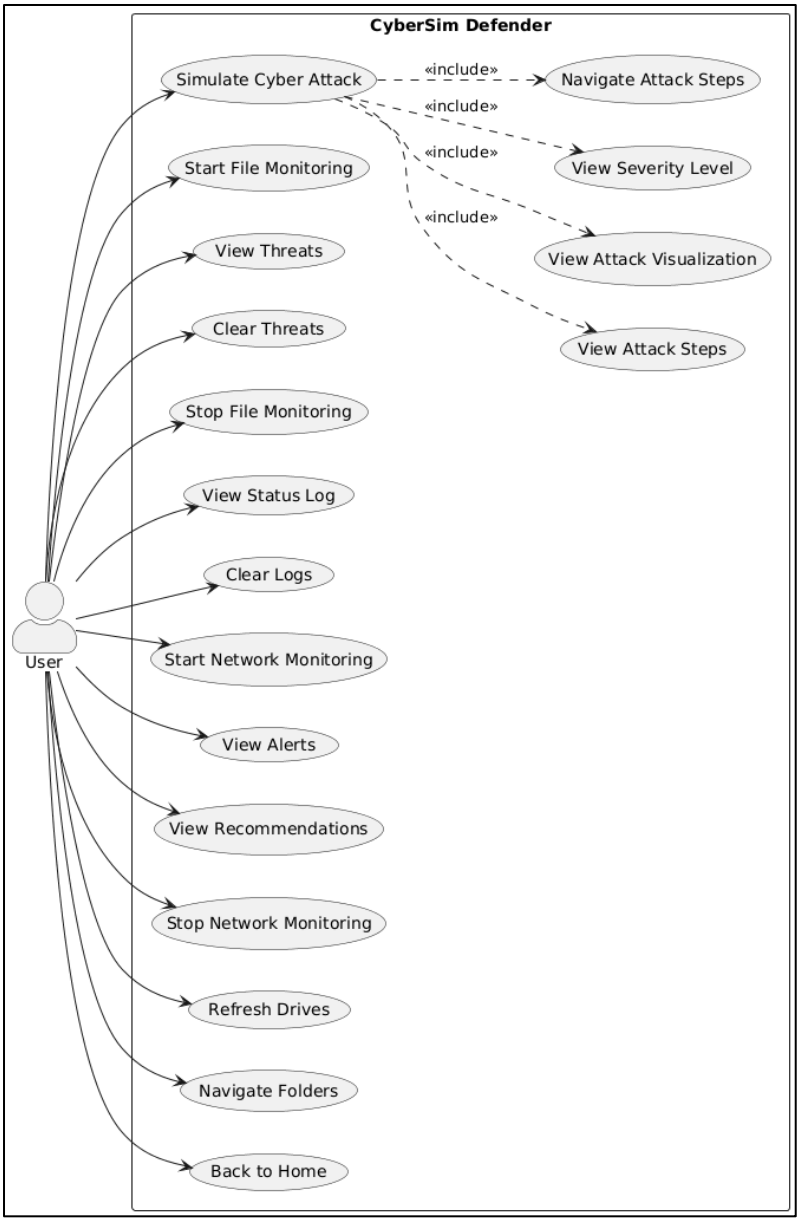
الرمز	اسم الرمز	الشرح
	Actor	عبارة عن الأشخاص الذين سيتعاملون مع النظام وممكن أن يكون نظام اخر او شخص.
	Use Case	تصف او يتم إدراج فيها سلوك النظام الخارجي وتعبر عن مصدر لفعل، ويتم استخدامه في مرحلة جمع المتطلبات الأولية.
	System Boundary	تعتبر الحاوية التي يتم وضع حالات الاستخدام المكونة للنظام داخلها.
	Association	تستخدم للربط بين المتفاعلون مع النظام وحالات الاستخدام .
----------> <<include>	Include	تستخدم عندما توجد حالة استخدام تحتاج الى حالة استخدم أخرى بشكل إجباري.
<---------- <<extend>>	Extend	تستخدم عندما توجد حالة استخدام تحتاج الى حالة استخدام أخرى بشكل اختياري، او كحالة يمكن تنفيذها في ظروف معينة.

1.1.5.3 مخطط الحالات للمستخدمين:

مخطط حالات المستخدمين يوضح تفاعلات المستخدمين ومسؤول النظام مع النظام.

المستخدم يمكنه محاكاة 10 أنواع من الهجمات السيبرانية، عرض خطوات الهجوم وتفاصيله التقنية، عرض الرسوم المتحركة التوضيحية، التنقل بين خطوات الهجوم، عرض التهديدات المكتشفة في مراقبة الملفات، عرض التنبيهات الأمنية في مراقبة الشبكة، عرض الحالة الأمنية للنظام، عرض سجل النظام، وعرض توصيات مستشار الأمان.

كما هو موضح في الشكل:



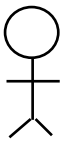
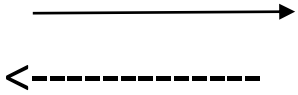
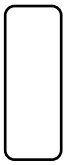
رسم توضيحي 7-3 مخطط حالات الاستخدام

2.5.3 مخطط التسلسل (Sequence Diagram)

مخطط التسلسل الأحداث (Sequence) هو عبارة عن نوع من أنواع المخططات السلوكية في لغة النمذجة الموحدة (UML)، رسم يُستخدم لعرض كيفية تفاعل الكائنات داخل النظام مع بعضها البعض بترتيب زمني محدد، حيث يُظهر الرسائل المتبادلة بين الكائنات خطوة بخطوة أثناء تنفيذ وظيفة معينة. رسم لتوضيح تسلسل الأحداث داخل النظام، مثل كيف يبدأ المستخدم تنفيذ هجوم، وكيف يستجيب النظام خطوة بخطوة، مما يساعد في فهم منطق التنفيذ الداخلي بطريقة منظمة وسهلة الفهم.

توصيف العمليات:

جدول 3-20 توصيف عمليات مخطط Sequence

الرمز	اسم الرمز	الشرح
	Actor	يمثل المستخدم أو النظام الذي يتفاعل مع النظام قيد الدراسة.
	Object	عنصر في النظام يتفاعل مع الكائنات الأخرى عبر الرسائل.
	Life Lines	يمثل وجود الكائن أو الممثل خلال فترة زمنية معينة في السيناريو.
	Message	يوضح الرسائل المتبادلة بين الكائنات لتأدية الوظائف.
	Activation Bar	يظهر فترة تنفيذ الكائن لعملية معينة بناءً على رسالة.

1.2.5.3 مخطط تسلسل الأحداث للمستخدمين:

شرح مخطط تسلسل الأحداث:

مخطط تسلسل الأحداث للمستخدمين يوضح تفاعلات المستخدم ومسؤول النظام مع تطبيق CyberSim Defender.

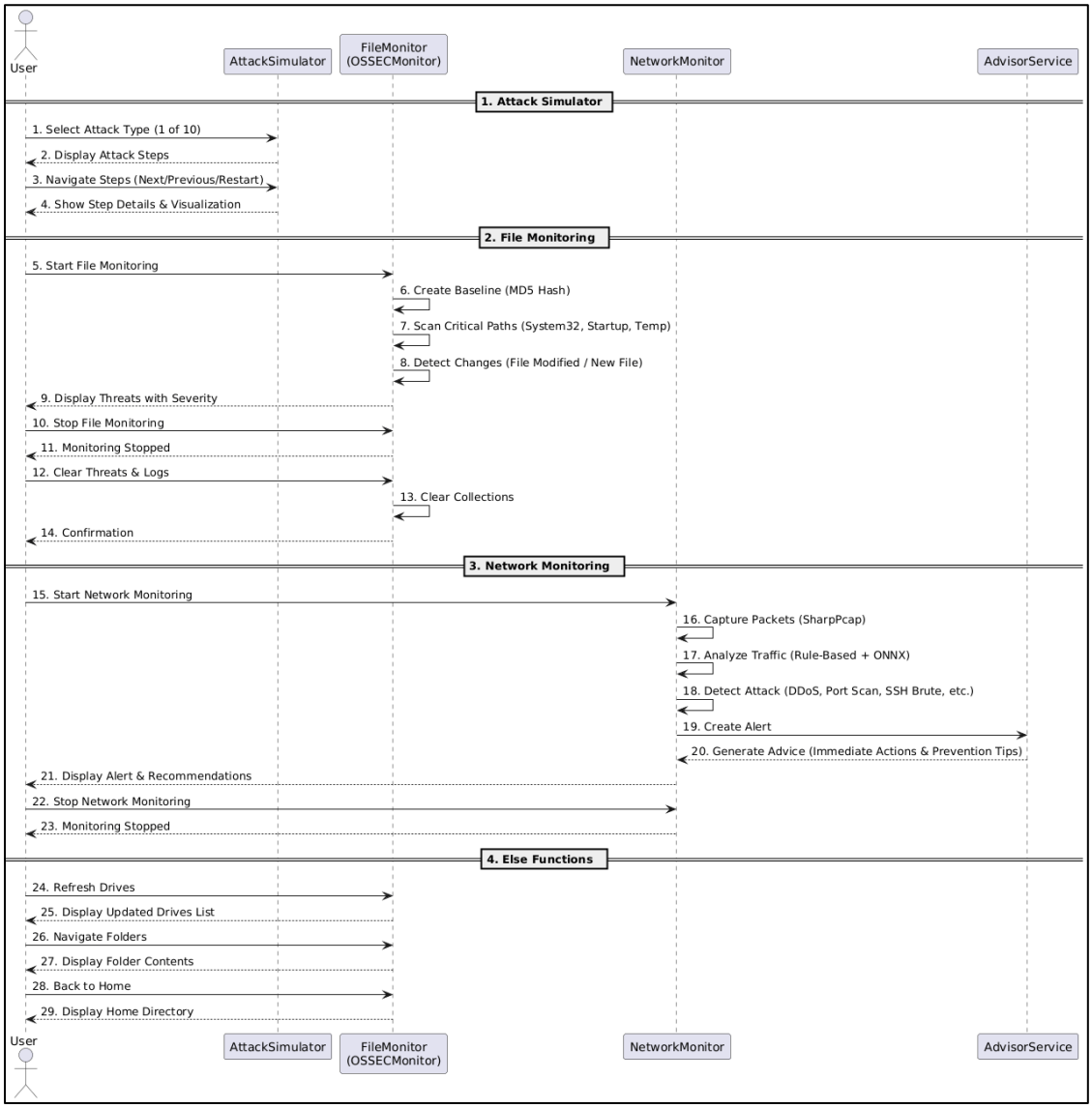
يقوم المستخدم باختيار نوع الهجوم من بين 10 أنواع متاحة (SQL Injection، DoS، DDoS، Brute Force، Ransomware، Phishing، MITM، XSS، DNS Spoofing، Zero-Day)، ثم يقوم التطبيق بعرض خطوات الهجوم المتسلسلة مع شرح مبسط وتفاصيل تقنية ورسوم متحركة توضيحية ومؤشر مستوى الخطورة، ويمكن للمستخدم التنقل بين الخطوات باستخدام أزرار التحكم (التالي، السابق، إعادة التشغيل).

أما في نظام مراقبة الملفات، يقوم المستخدم أو مسؤول النظام بتشغيل المراقبة ليقوم التطبيق بإنشاء بصمة (baseline) للمسارات الحرجة مثل System32 و Startup و Temp باستخدام MD5 Hash، ثم يقوم بالكشف عن أي تغييرات غير مصرح بها في الملفات ويعرض التهديدات المكتشفة مع مستوى الخطورة.

وفي نظام مراقبة الشبكة، يقوم المستخدم أو مسؤول النظام بتشغيل المراقبة ليقوم التطبيق بالتقاط الحزم عبر SharpPcap وتحليل التدفقات (flows) باستخدام قواعد كشف مدمجة ونماذج ONNX Runtime، وعند اكتشاف هجوم (مثل DDoS أو Port Scan أو SSH Brute Force) يقوم التطبيق بإنشاء تنبيه وإرساله إلى مستشار الأمان

(Advisor Service) الذي يقوم بتوليد إجراءات فورية ونصائح وقائية حسب نوع الهجوم، ثم يعرض التطبيق التنبيه مع التوصيات للمستخدم.

كما هو موضح في الشكل:



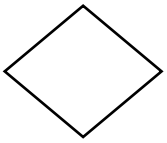
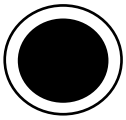
رسم توضيحي 8-3 لمخطط تسلسل المستخدمين

3.5.3 مخطط الأنشطة (Activity Diagram)

مخطط الأنشطة (Activity) هو عبارة عن نوع من أنواع المخططات السلوكية في لغة النمذجة الموحدة (UML)، وهو رسم يُستخدم لعرض تسلسل الأنشطة أو الخطوات التي ينفذها النظام أو المستخدم لأداء مهمة معينة، ويُظهر كيف تنتقل العملية من خطوة إلى أخرى باستخدام الأسهم. فهو يُستخدم لتوضيح منطق سير العمل داخل النظام، مثل كيف يبدأ الهجوم، وكيف يكتشفه النظام، ثم يصنّفه ويقترح الاستجابة، مما يساعد في فهم تدفق العمليات بشكل واضح ومنظم.

توصيف العمليات:

جدول 21-3 توصيف عمليات مخطط Activity

الرمز	اسم الرمز	الشرح
	Start Node	تمثل البداية وتشير الى نقطة انطلاق العملية.
	Action	عنصر في النظام يمثل نشاطا أو خطوة معينة في سير العمليات.
	Control Flow	يوضح اتجاه تدفق الأنشطة ويربط بينها ويظهر كيف تنتقل العملية من خطوة الى أخرى.
	Condition	يمثل نقطة اتخاذ القرار، يتفرع منها عدة اسهم تمثل الخيارات المختلفة.
	End Node	يحدد نهاية تدفق العمل سواء كانت عملية بسيطة أو معقدة.
	Activity	خطوة أو إجراء داخل مخطط النشاط تمثل جزءًا من سير العمل أو العملية التي ينفذها النظام أو المستخدم.

1.3.5.3 مخطط الأنشطة للمستخدمين:

شرح مخطط النشاط:

مخطط النشاط يوضح التفاعلات بين المستخدم والنظام في تطبيق CyberSim Defender.

يبدأ المستخدم باختيار الإجراء المطلوب من الواجهة الرئيسية، حيث تتوفر ثلاثة خيارات رئيسية: محاكاة الهجوم، مراقبة الملفات، أو مراقبة الشبكة.

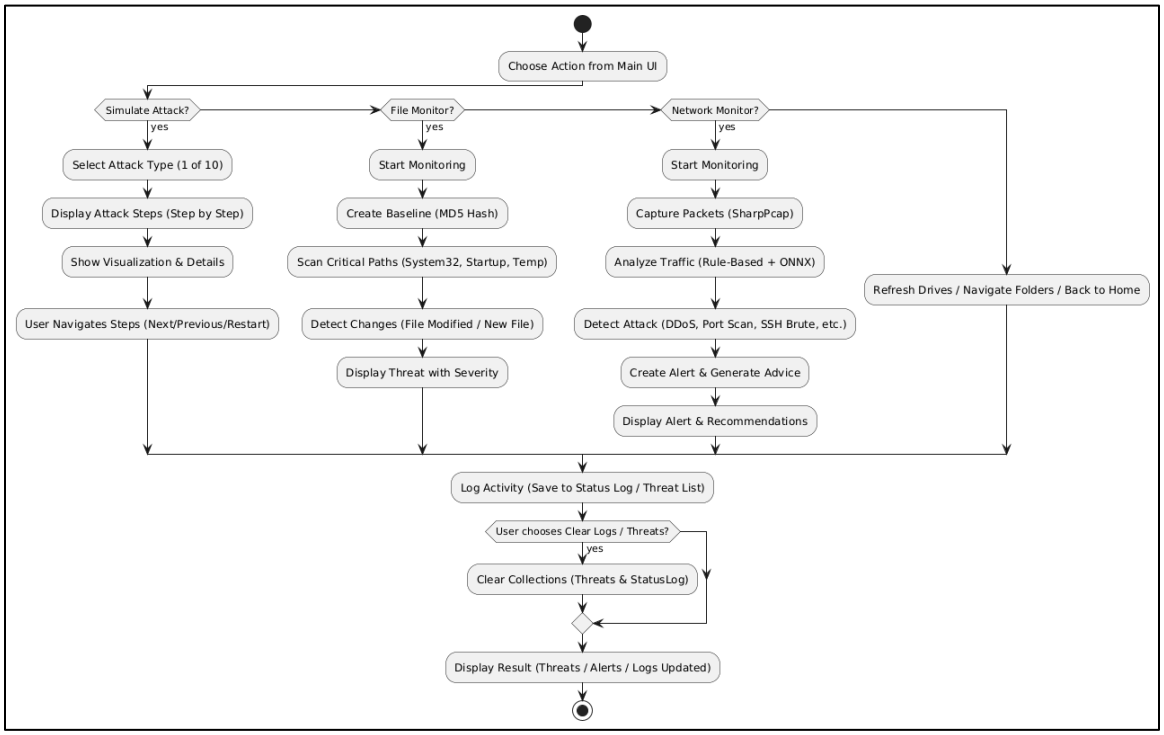
في حالة اختيار محاكاة الهجوم، يقوم المستخدم باختيار نوع الهجوم من بين 10 أنواع متاحة، ثم يقوم النظام بعرض خطوات الهجوم المتسلسلة مع شرح مبسط وتفاصيل تقنية ورسوم متحركة توضيحية ومؤشر مستوى الخطورة، ويمكن للمستخدم التنقل بين الخطوات باستخدام أزرار التحكم.

في حالة اختيار مراقبة الملفات، يقوم المستخدم بتشغيل المراقبة ليبدأ النظام بإنشاء بصمة للمسارات الحرجة باستخدام MD5 Hash، ثم يقوم بفحص المسارات مثل System32 و Startup و Temp، وعند اكتشاف أي تغيير في الملفات يعرض النظام التهديد مع مستوى الخطورة.

في حالة اختيار مراقبة الشبكة، يقوم المستخدم بتشغيل المراقبة ليبدأ النظام بالتقاط الحزم عبر SharpPcap، ثم يقوم بتحليل حركة المرور باستخدام قواعد كشف مدمجة، وعند اكتشاف هجوم (مثل DDoS أو Port Scan أو SSH Brute Force) يقوم النظام بإنشاء تنبيه وتوليد توصيات من مستشار الأمان، ثم يعرض التنبيه مع الإجراءات الفورية والنصائح الوقائية.

بعد ذلك يقوم النظام بتسجيل النشاط في سجل النظام وقائمة التهديدات ، كما يمكن للمستخدم مسح قائمة التهديدات وسجل النظام عند الحاجة، ثم يعرض النظام النتيجة النهائية.

كما هو موضح في الشكل:



رسم توضيحي 9-3 لمخطط أنشطة المستخدم

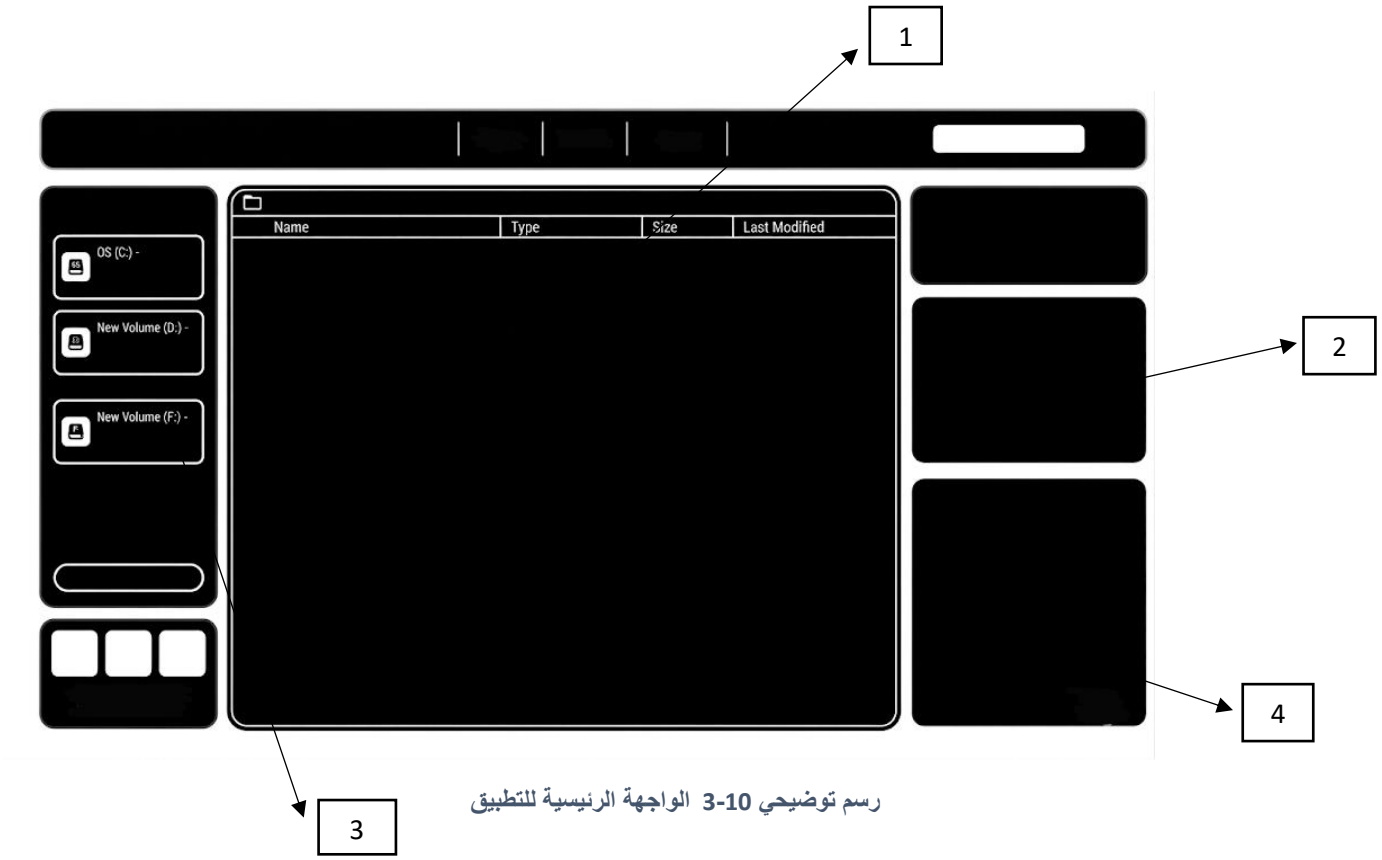
6.3 واجهات المشروع:

واجهات المشروع تمثل التصور الاولي (wireframe) لتصميم المحاكي وتهدف الى تحديد تخطيط العناصر الأساسية مثل الازرار والمربعات النصية، مما يسهل فهم تفاعل المستخدم مع النظام، كما هو موضح في الواجهات التالية:

الواجهة الرئيسية:

سيكون فيها عرض الملفات الكاملة الموجودة في النظام والاقراص وأيضا سيكون فيها مراقبة أي تعديلات في المسارات الحرجة ويتم عرض هذه التغييرات على مستوى منطقة التنبيهات المكتشفة.

كما هو موضح في الشكل:

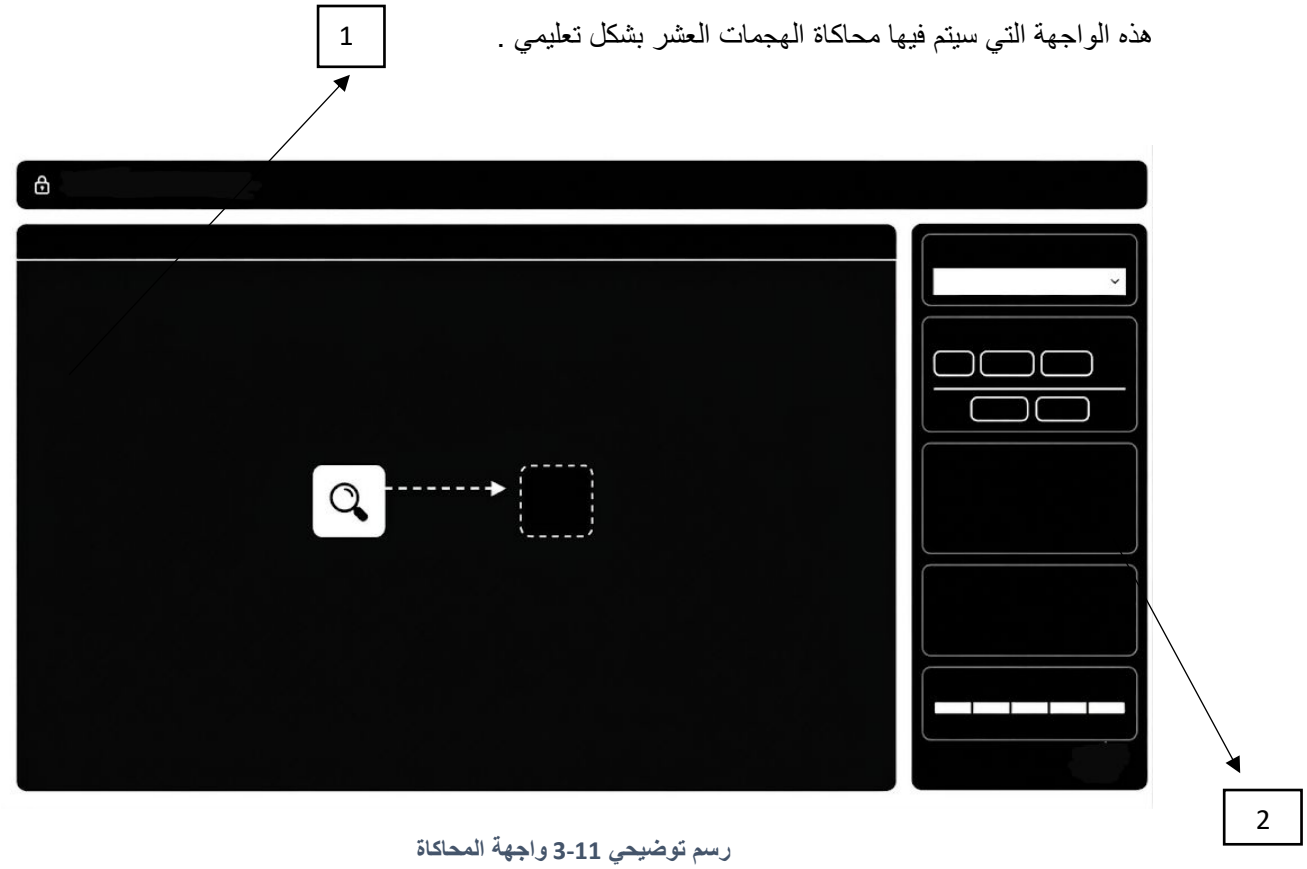


رسم توضيحي 10-3 الواجهة الرئيسية للتطبيق

- شكل (1): منطقة عرض وتصفح الملفات الموجودة على النظام
- شكل (2): منطقة عرض التنبيهات المكتشفة من تعديلات او حذف او حتى إنشاء
- شكل (3): منطقة عرض الأقراص المتوفرة
- شكل (4): منطقة عرض سجل النظام للأنشطة المستخدم

واجهة ال simulator:

هذه الواجهة التي سيتم فيها محاكاة الهجمات العشر بشكل تعليمي .

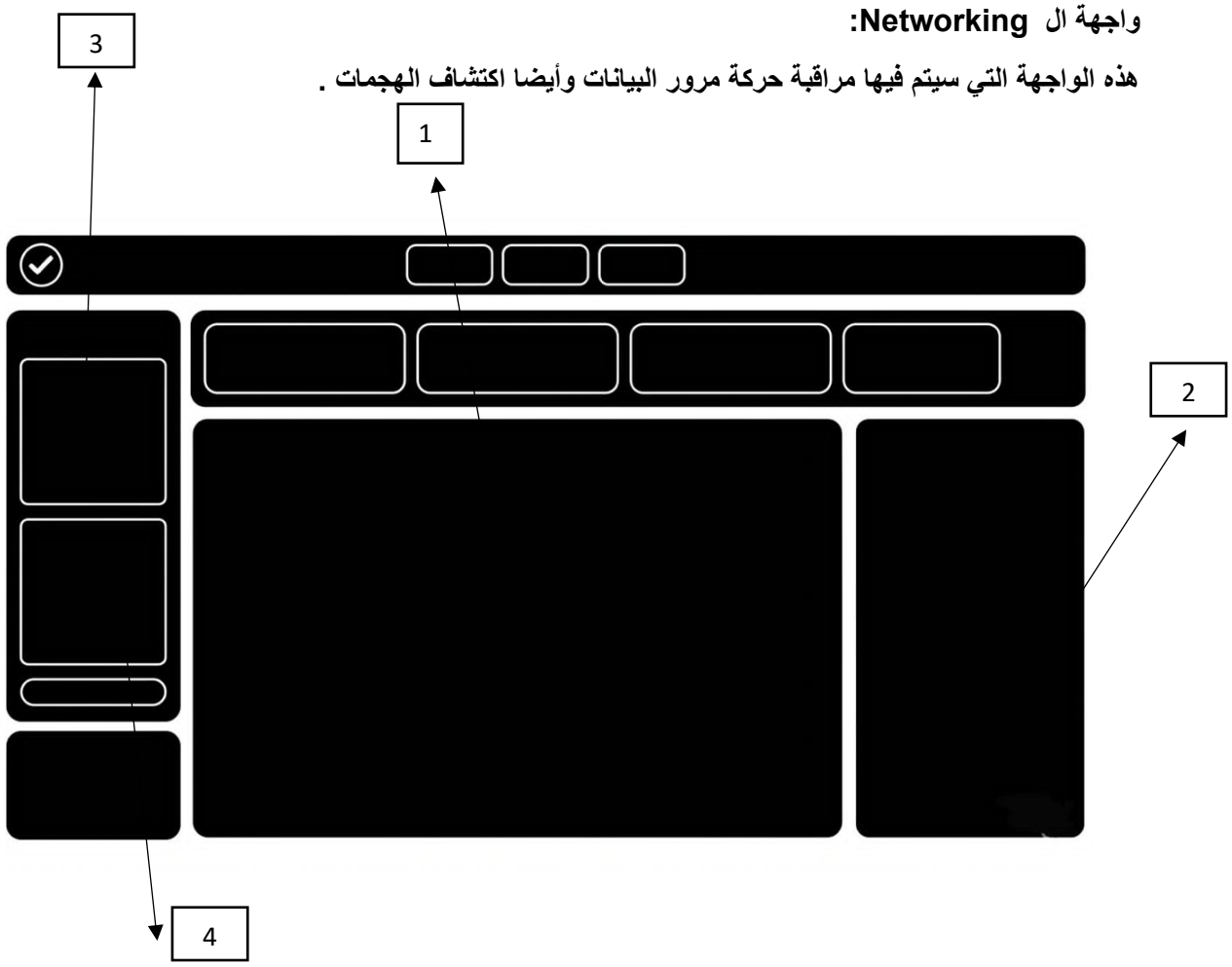


رسم توضيحي 11-3 واجهة المحاكاة

- شكل (1): منطقة محاكاة الهجمات التي سوف تظهر فيها الصور
- شكل (2): منطقة التحكم من ازرار التنقل بين الخطوات او بدأ المحاكاة الى اختيار الهجمات وعرض كل خطوة مع شرح لها ومستوى خطورتها وأيضا شرح للتفاصيل التقنية لكل خطوة

واجهة ال Networking:

هذه الواجهة التي سيتم فيها مراقبة حركة مرور البيانات وأيضا اكتشاف الهجمات .



- شكل (1): منطقة عرض حركة مرور البيانات والتهديدات عند حدوثها
- شكل (2): منطقة عرض مستشارالامان الذي يعطي نصائح وإجراءات للتصدي ضد الهجوم
- شكل (3): عرض الأجهزة او الواجهات المتاحة للقيام بالمراقبة
- شكل (4): منطقة عرض التهديدات الأخيرة مع عرض Ips للمصدر والوجهة

7.3 الخلاصة

استعرض هذا الفصل المتطلبات الرئيسية لتطبيقCyberSim Defender ، بدءًا من تحديد الفئات المستهدفة، مرورًا بتحليل الجدوى التقنية والتشغيلية، وانتهاءً بتفصيل المتطلبات الوظيفية وغير الوظيفية. تم تحديد وظائف النظام بدقة، مثل إدارة المستخدمين، محاكاة الهجمات، التحليل، الاستجابة، والتوافق، إلى جانب خصائص الجودة مثل الأداء، الأمان، التوافر، وسهولة الاستخدام. كما تم تصميم المخططات النمذجية التي توضح سلوك النظام وتفاعلاته الداخلية.

واجه المشروع تحديات أثناء جمع وتحليل المتطلبات، أبرزها: صعوبة دمج الذكاء الاصطناعي مع بيئة مراقبة الشبكة بشكل مستقر، الحاجة إلى واجهة رسومية مفهومة للمستخدمين غير التقنيين، وضمان توافق النظام مع بيئات التشغيل المختلفة. وقد تم تقديم توصيات تقنية لمعالجة هذه التحديات، مثل اعتماد بنية معيارية، استخدام نماذج قابلة للتحديث، وتوثيق الكود لضمان قابلية الصيانة.

يمهد هذا الفصل للانتقال إلى الفصل الرابع، الذي سيركز على عرض واجهات المشروع ووظيفة كل واجهة.

الفصل 4

تنفيذ المشروع

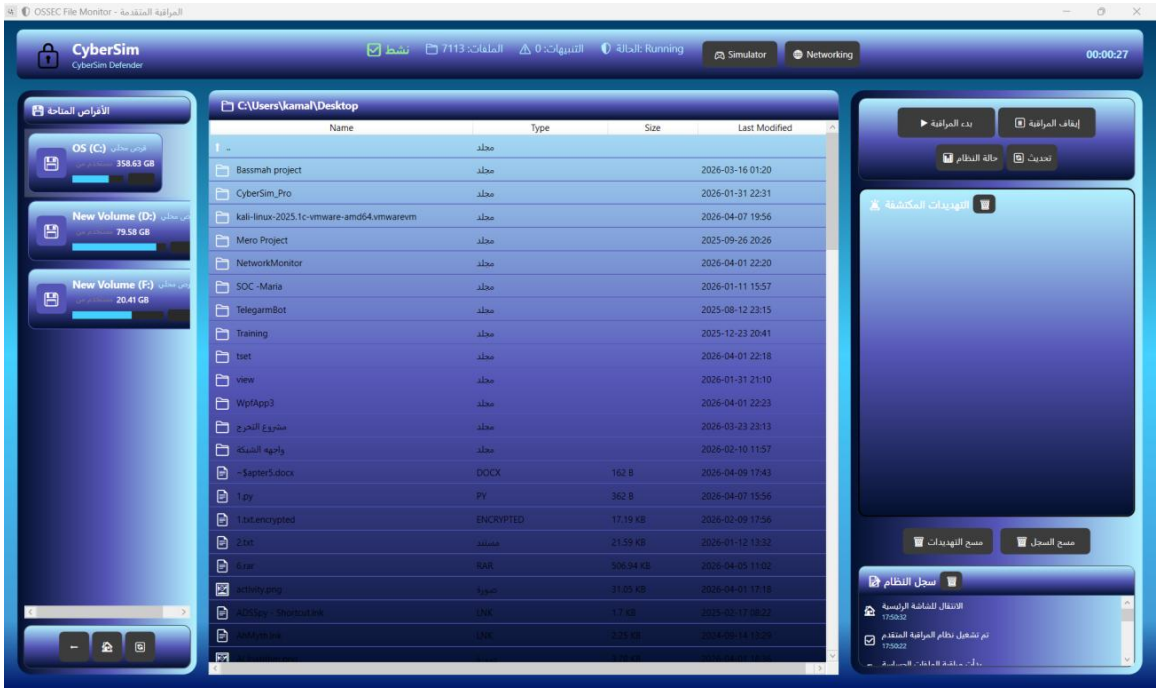
Project)
(Implementation

1.4 المقدمة:

يتناول هذا الفصل تصميم مشروع "CyberSim Defender" قمنا فيه بعمل واجهات للمستخدم و الطالب، وذلك بما يتناسب مع احتياجات كل مستخدم، تم التركيز في التصميم على البساطة وسهولة الاستخدام، مع الاعتماد على الألوان الأساسية المتمثلة في الكحلي والازرق الفاتح والازرق الغامق كألوان أساسية، والألوان الأحمر والاخضر والبرتقالي والبنفسجي والرمادي والأبيض كألوان فرعية ستظهر بوضوح في الصور الموضحة في الاسفل، وذلك لتعزيز الهوية البصرية للمشروع وتمييز العمليات المختلفة بشكل واضح وبسيط.

2.4 بناء الواجهات:

1.2.4 الواجهة الرئيسية للمشروع:



رسم توضيحي 1-4 واجهة مراقبة الملفات

هذه الواجهة هي لوحة التحكم الرئيسية (Dashboard) للمشروع الغرض الأساسي منها تقديم نظرة شاملة على صحة النظام الأمنية مع إعطاء المستخدم أدوات سريعة للتحكم في الحماية ومراقبة النشاط واتخاذ الإجراءات.

الواجهة مصممة لتجمع بين معلومات النظام الأساسية (مثل مساحة التخزين ومحتويات المجلدات الحيوية) وأدوات التحكم الفوري في الحماية وأدوات الفحص الاستباقي وسجل الأحداث الذي يدون كل ما يحدث.

رسم توضيحي 2-4 قسم الأقراص

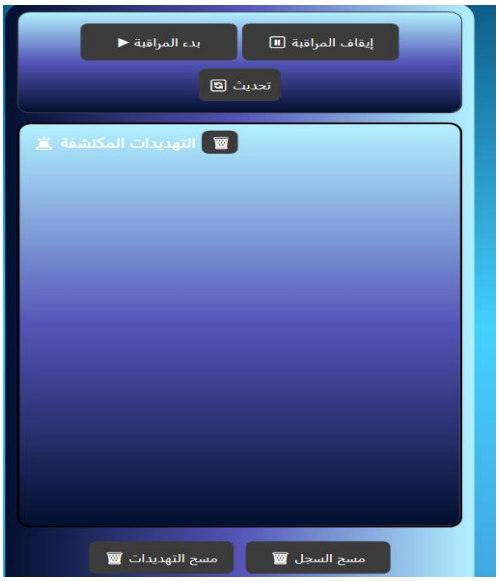
- جزء الأقراص المتاحة ((OS (C:): يعطي لمحة سريعة جدًا عن القرص الرئيسي عبارة عن "قرص محلي" تُطلع المستخدم على أن المساحة كبيرة وتعمل وهو أمر أساسي لأداء النظام وعمليات المسح.

رسم توضيحي 3-4 قسم عرض وتصفح الملفات

- جزء عرض ملفات النظام: يعرض محتويات مجلد النظام وهو مهم جدًا غالبًا ما توجد فيه ملفات تشغيل الجهاز وبرامج التثبيت الأصلية عرض هذا المجلد هنا له دلالة أمنية:

- للوعي: يبين للمستخدم أين توجد الملفات النظامية المهمة.

- للمراقبة: يراقب حتى المجلدات النظامية الحساسة لأن البرمجيات الضارة أحيانًا تتخفى فيها. في الجدول يظهر أنواع الملفات (تطبيق، ملف نظام، مستند) وأحجامها وتواريخها مما يساعد في اكتشاف أي ملف غريب أو مُعدل حديثًا بطريقة مشبوهة.



رسم توضيحي 4-4 قسم التهديدات المكتشفة

- قسم إيقاف المراقبة:

يحتوي على الأزرار الأساسية لإدارة الحماية في الوقت الفعلي:

- إيقاف المراقبة: مفتاح الطوارئ يسمح بإيقاف الحماية الفورية مؤقتًا وهو إجراء يُتخذ فقط عند وجود تطبيق موثوق يتعارض مع البرنامج مع العلم أن النظام يصبح معرضًا للخطر خلال هذه الفترة.

- تحديث: يقوم بتحديث قاعدة بيانات تعريفات الفيروسات والبرمجيات الضارة مما يمكن البرنامج من التعرف على أحدث التهديدات.

- التهديدات المكتشفة: عداد أو مؤشر يظهر عدد التهديدات التي تم حظرها أو التعامل معها مؤخرًا (مثل 0 تهديدات أو 5 تهديدات عالقة) وظيفته الأساسية هي الطمأنينة أو التنبيه الفوري.

- مسح التهديدات: يتم فيه حذف آخر التهديدات المكتشفة والتنبيهات

مسح السجل: يتم فيه حذف آخر الأنشطة والسجلات .

- سجل النظام:

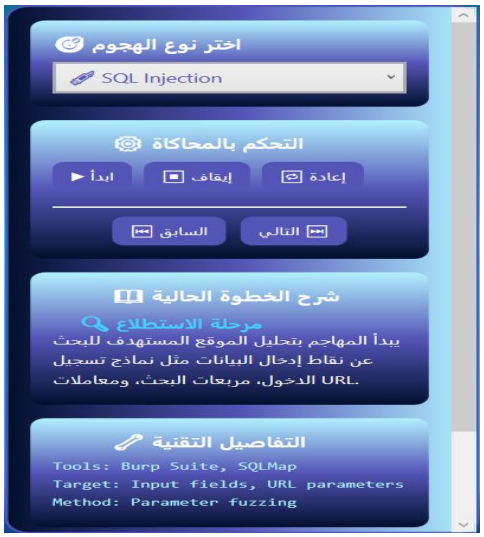
يعتبر دفتر التسجيلات أو الصندوق الأسود للبرنامج يسجل بالتفصيل وبالتوقيت الدقيق كل الإجراءات المهمة.

2.2.4 واجهة المحاكاة:

رسم توضيحي 5-4 واجهة المحاكاة الهجمات

هذه الواجهة تقوم ب تعليم المستخدمين كيفية عمل الهجمات السيبراني ومحاكاة سيناريوهات الهجوم خطوة بخطوة وتوعية بأهمية الحماية الأمنية يتم فيها اختيار نوع الهجوم بمجرد اختيار الهجمة يظهر لنا المحاكي العملية بشكل رسومي ويتم شرح التعليمات المستخدمة وفي نهاية محاكاة الهجمات يتم إعطاء نصيحة امنية لصد هذه الهجمات.

رسم توضيحي 6-4 قائمة الهجمات التي يمكن محاكاتها



رسم توضيحي 7-4 تفاصيل اكثر للواجهة

شرح تفاصيل الواجهة:

- اختر نوع الهجوم:

المستخدم يقوم بتحديد نوع الهجوم السيبراني الذي يرغب في دراسته في هذه الحالة تم اختيار "SQL Injection" وهو أحد أكثر الهجمات شيوعاً على قواعد البيانات حيث يحاول المهاجم إدخال أوامر SQL خبيثة من خلال حقول إدخال البيانات.

- التحكم بالمحاكاة:

يحتوي على مجموعة أزرار تمكن المستخدم من التحكم في سير المحاكاة التعليمية زر "إعادة" يعيد تشغيل السيناريو من البداية، وزر "إيقاف" يوقف المحاكاة الجارية بينما أزرار "السابق" و"التالي" تسمح للمستخدم بالتنقل بين خطوات الهجوم خطوة بخطوة مما يتيح له دراسة كل مرحلة بعناية.

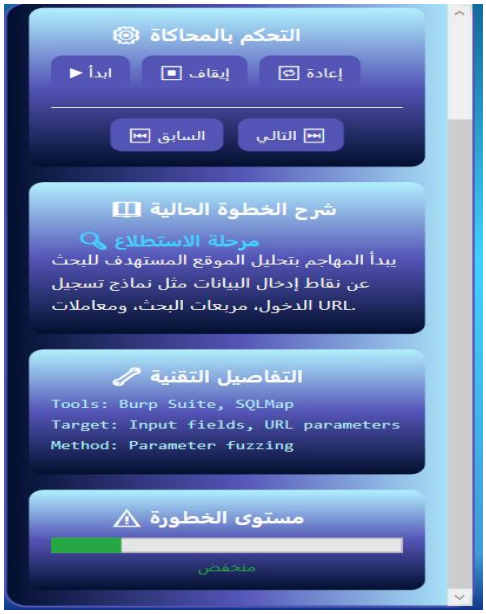
- في جزء شرح الخطوة الحالية:

وصف تفصيلي للمرحلة الحالية من الهجوم هنا يتم شرح "مرحلة الاستطلاع" حيث يبدأ المهاجم بتحليل الموقع المستهدف للبحث عن نقاط ضعف محتملة مثل نماذج تسجيل الدخول، مربعات البحث، ومعاملات URL التي قد تكون عرضة للاستغلال.

- التفاصيل التقنية:

يقدم معلومات أكثر عمقاً للمهتمين بالجانب التقني (المختصين في الامن السيبراني) هنا نجد الأدوات المستخدمة مثل:

Burp Suite وSQLMap والأهداف التي يركز عليها المهاجم وهي حقول الإدخال ومعاملات URL بالإضافة إلى الطريقة المتبعة وهي "Parameter fuzzing" التي تعني إرسال بيانات متنوعة إلى المعلمات لاختبار سلوك التطبيق واكتشاف نقاط الضعف.



رسم توضيحي 8-4 لتفاصيل الواجهة

- مستوى الخطورة:

يظهر حالياً على أنه منخفض هذا المؤشر يتغير ديناميكياً مع تقدم مراحل الهجوم حيث يبدأ منخفضاً في مرحلة الاستطلاع ثم يرتفع تدريجياً مع تقدم المهاجم في تنفيذ هجومه ليعكس مدى الخطر الذي يشكله الهجوم في كل مرحلة من مراحله.

3.2.4 واجهة مراقبة الشبكة:

رسم توضيحي 9-4 واجهة مراقبة الشبكة

هذه الواجهة تمثل لوحة تحكم رئيسية لنظام متكامل لمراقبة أمن الشبكات صممنا الواجهة لتكون مركز تحكم واحد يسمح للمستخدم بمراقبة نشاط الشبكة، اكتشاف التهديدات، واتخاذ إجراءات أمنية فورية تعمل على تحليل حركة المرور الشبكية في الوقت الحقيقي باستخدام تقنيات الذكاء الاصطناعي للكشف عن الهجمات والتهديدات الأمنية.

رسم توضيحي 10-4 لقسم الأجهزة المتاحة

- الأجهزة المتاحة:

هذا القسم يعرض قائمة جميع واجهات الشبكة المتاحة على الجهاز الذي يعمل عليه التطبيق (كروت الشبكة).

وظيفة هذا القسم يسمح للمستخدم باختيار واجهة الشبكة (كرت الشبكة) التي يريد مراقبتها ويعطي نظرة عامة على إمكانيات الاتصال للجهاز ويساعد في تحديد مصادر حركة المرور.

- زر تحديث الأجهزة:

يقوم بتحديث القائمة يدوياً في حالة إضافة أو إزالة محولات شبكة ويضمن أن المستخدم يرى أحدث المعلومات عن أجهزة الشبكة المتاحة.

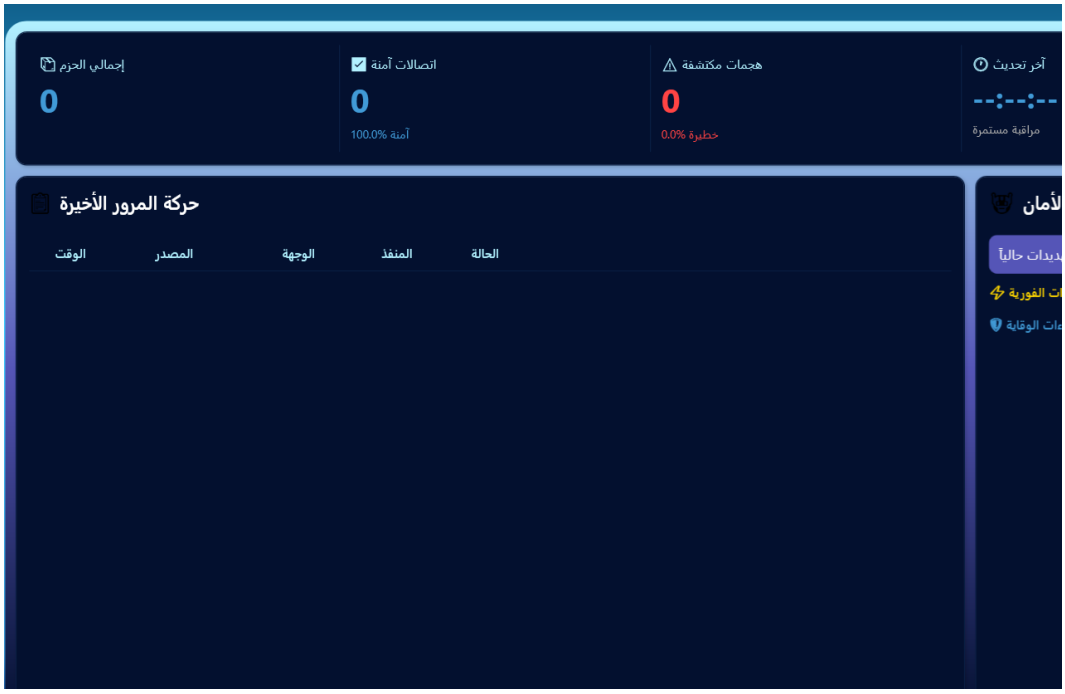
- التنبيهات الأخيرة:

هذا القسم يعمل كـ مركز التنبيهات والأحداث الأمنية وهو يعرض:

قائمة بالتنبيهات الأمنية التي تم اكتشافها مؤخراً، حيث كل تنبيه يحتوي على:

- الوقت :وقت اكتشاف التهديد.
- نوع الهجوم :مثلDDoS ، Port Scan، SSH Brute Force، إلخ.
- مستوى الخطورة :مصنف بالألوان (أحمر للحرج، أصفر للتحذير، إلخ).

وظيفة هذا القسم التنبيه الفوري عندما يتم اكتشاف تهديد، يظهر هنا فوراً التتبع الزمني يمكن رؤية تطور التهديدات بمرور الوقت والوصول السريع بالنقر على أي تنبيه، يمكن فتح نافذة تفاصيل كاملة عن التهديد.



رسم توضيحي 11-4 قسم حركة البيانات

- منطقة المعلومات الرئيسية:

تعرض إحصائيات حية ومحدثة باستمرار عن حالة الشبكة:

- إجمالي الحزم :عدد حزم البيانات التي تم تحليلها
- الاتصالات الآمنة :عدد الاتصالات التي تم تصنيفها كآمنة
- الهجمات المكتشفة :عدد الهجمات التي تم اكتشافها
- آخر تحديث :الوقت الحالي لآخر عملية تحليل

الألوان المستخدمة:

- الأخضر :للإحصائيات الإيجابية والآمنة
- الأحمر :للهجمات والتهديدات
- الأزرق :للمعلومات المحايدة

حركة المرور الأخيرة

يعرض جدولاً تفصيلياً لحركة مرور الشبكة في الوقت الحقيقي ومن تفاصيل الجدول:

- الوقت :وقت حدوث الاتصال (بالساعات والدقائق والثواني)
- المصدر :عنوان IP المصدر للاتصال
- الوجهة :عنوان IP الوجهة للاتصال

- المنفذ :منفذ الوجهة المستخدم في الاتصال
- الحالة :تصنيف الاتصال (آمن /تهديد)

ومن وظائف هذا الجدول شفافية كاملة يرى المستخدم كل اتصال يحدث على الشبكة ويتم تصنيف كل اتصال فوراً كآمن أو تهديد ويمكن البحث في الجدول وتصفية النتائج.

رسم توضيحي 12-4 قسم مستشار الامان

- مستشار الأمان:

يعمل كـ مساعد أمني ذكي يقدم نصائح وإرشادات ومن محتوياته تحليل الحالة الحالية مثل:

لا توجد تهديدات حالياً، الإجراءات الفورية قائمة بالإجراءات التي يجب اتخاذها فور اكتشاف تهديد، إجراءات الوقاية نصائح وقائية لمنع الهجمات المستقبلية.

ويقوم بالتوجيه الذكي يقدم نصائح مخصصة حسب نوع التهديد المكتشف والتعليم المستمر يعلم المستخدم أفضل ممارسات الأمان والإجراءات العملية بحيث يتحول من مجرد مراقب إلى مستشار أمني.

الفصل 5

اختبار المشروع

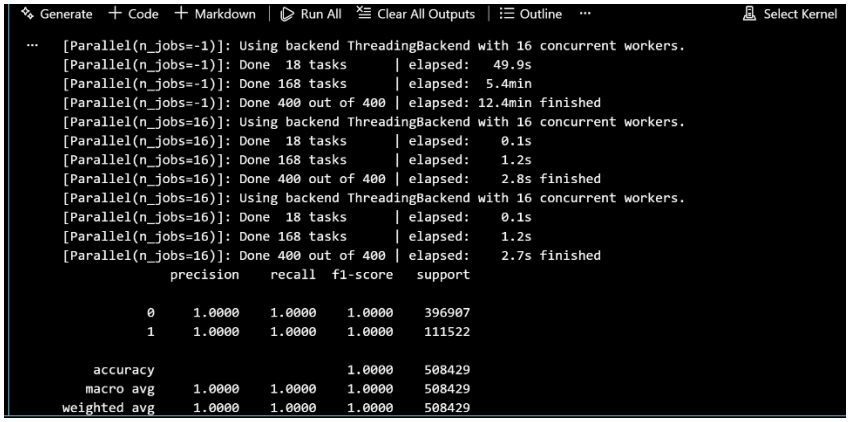
(Project Test)

1.5 المقدمة

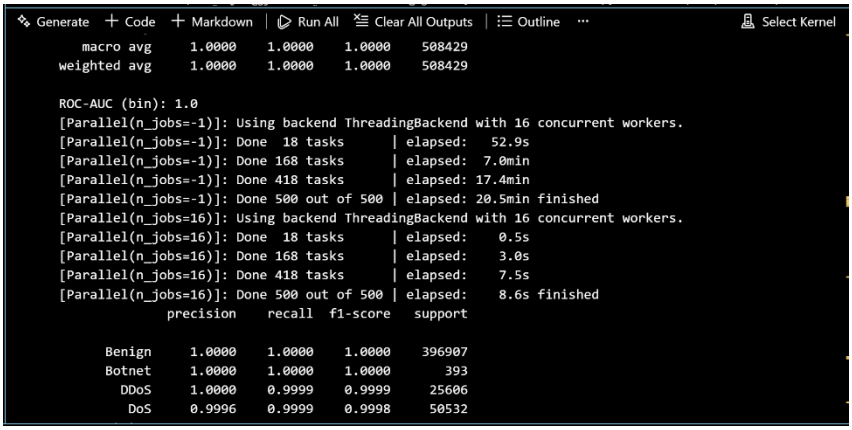
بعدا الانتهاء من شرح تصميم النظام سيتم في هذا الفصل التطرق الى كيفية تنفيذ النظام وإدخال البيانات وسيناريو العمل من خلال عرض صور ونماذج توضح آلية عمل النظام حيث يمكن استخدام النظام من قبل المستخدمين.

بعد الانتهاء من شرح تنفيذ النظام سنتطرق الى كل الرسائل التي تظهر أثناء استخدام التطبيق عبر عرض الصور الموضحة لذلك.

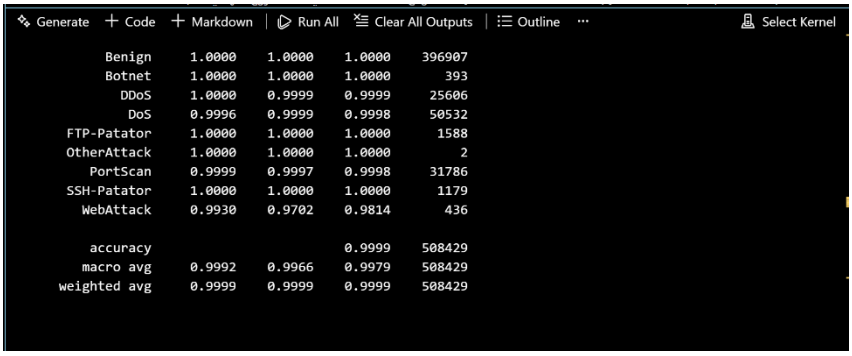
2.5 نتائج تدريب نموذج الذكاء الاصطناعي:



رسم توضيحي 1-5 نتائج تدريب الذكاء الاصطناعي



رسم توضيحي 2-5 نتائج تدريب الذكاء الاصطناعي



رسم توضيحي 3-5 نتائج تدريب الذكاء الاصطناعي

تم تدريب نموذج Random Forest على مجموعة بياناتCIC-IDS2017 ، واختباره على 20% من البيانات. حقق النموذج الثنائي للتمييز بين الحركة الطبيعية والهجمات ROC-AUC بقيمة 1.0 ودقة 100%، مما يشير إلى أداء مثالي .

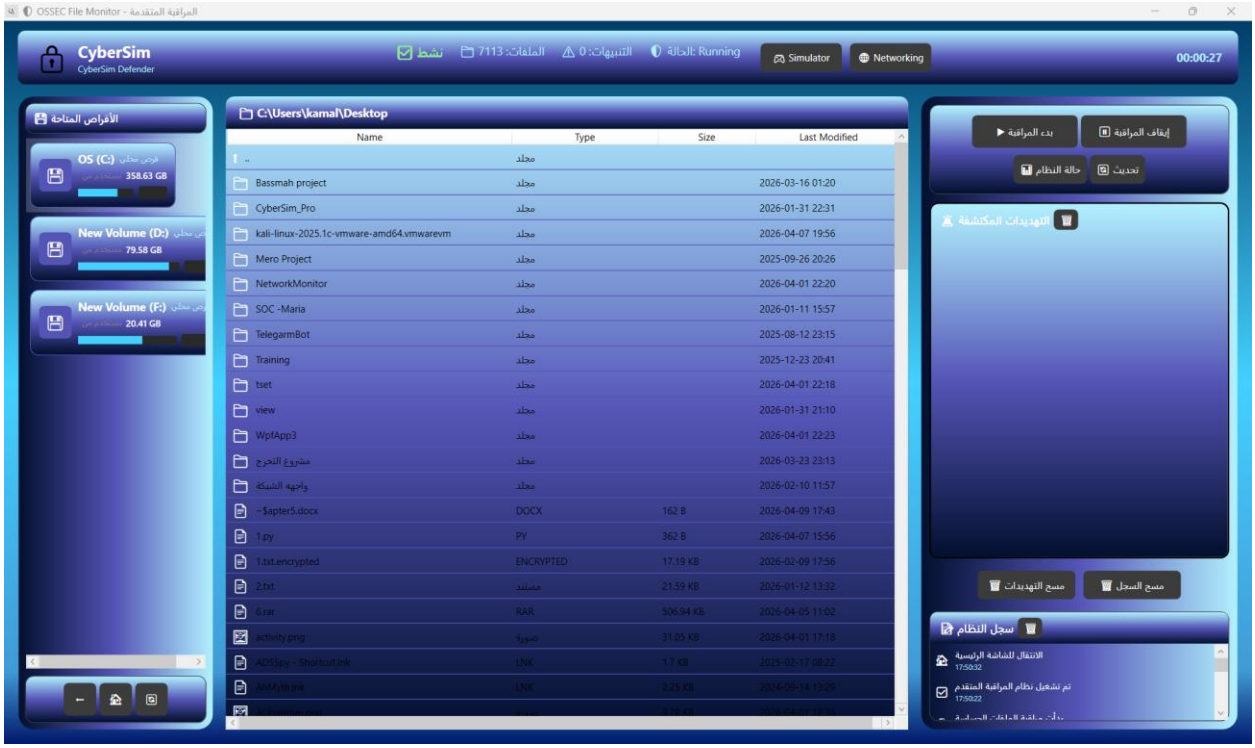
أما النموذج المتعدد لتصنيف أنواع الهجمات، فقد حقق دقة إجمالية 99.99%، حيث جاءت النتائج كالتالي: دقة 100% لهجمات DDoS و Botnet و FTP-Patator و SSH-Patator، ودقة 99.98% لهجمات DoSوPortScan ، بينما كانت أقل نتيجة لهجمات WebAttack بنسبة 98.14% بسبب قلة عدد عيناتها في البيانات. بشكل عام، أثبت النموذج كفاءة عالية جداً تؤهله للاستخدام العملي في نظام كشف التسلل.

3.5 اختبار الواجهات

1.3.5 واجهات المستخدم:

واجهة مراقبة الملفات :

يبدأ النظام من واجهة مراقبة الملفات وستكون هذه الواجهة هي الواجهة الرئيسية التي عن طريقها سننتقل الى الواجهات الباقية من التطبيق وهذه الواجهة تعتمد على حساب قيم التجزئة للملفات لمعرفة أي تغييرات تحدث في المسارات الحرجة .



رسم توضيحي 5-4 الواجهة الرئيسية

وتتكون هذه الواجهة :

1- منطقة عرض وتصفح للملفات الموجودة على الجهاز.

2- الأقراص المتوفرة.

3- منطقة عرض التهديدات المكتشفة ومنطقة سجل النظام لتسجيل الأنشطة التي قام بها المستخدم والتي قام بها النظام أيضا.

4- الأزرار التي ستنقلنا لباقي واجهات التطبيق Simulator and Networking.

5- أزرار التحكم الموجودة لبدء المراقبة النظام ويكون في حالة نشطة او توقف مراقبة ليكون في حالة خاملة.

والان لاختبار النظام أي كيف يكشف عمليات التعديل على الملفات أو إنشاء ملفات في المسارات الحرجة :

اولا : قمنا بعمل ملف بامتداد exe. في مسار الtemp احد الامتدادت التي يكشفها الملف مثل sys. , dll. , exe.

رسم توضيحي 5-5 اختبار واجهة مراقبة الملفات

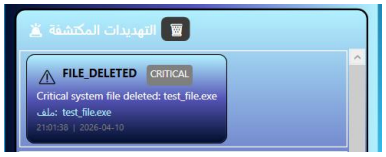
عن طريق امر في powershell انشأنا ملف في ال temp ورد الفعل المطلوب من التطبيق ان يظهر تهديد في منطقة التهديدات السابقة لكي يقوم المستخدم من التأكد ان كان هو من انشأ هذا الملف ام ماهو سبب ظهور هذا الملف .

رسم توضيحي 5-6 رد فعل التطبيق عند انشاء الملفات

وهذا كان رد فعل التطبيق اظهر تنبيه عن انشاء ملف في مسار الtemp مع الوقت والتاريخ ونوع الامتداد واسم الملف مع الهاش الخاص به .

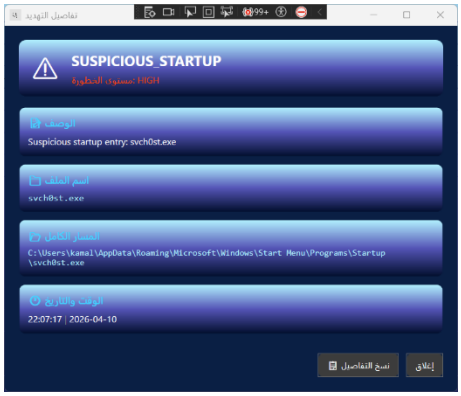
رسم توضيحي 5-7 رد فعل التطبيق عند التعديلات

بعض التنبيهات التي تظهر عندما يتم التعديلات على بعض الملفات المهمة مثل hosts حيث انه يكتب اسم الملف مع العملية التي تمت مثلا Tempering.



رسم توضيحي 5-8 رد فعل التطبيق عن الحذف

ومثل هذه الإشعارات في حالة حذف ملف من احد المسارات الحرجة .



رسم توضيحي 9-5 واجهة المعلومات الاضافية

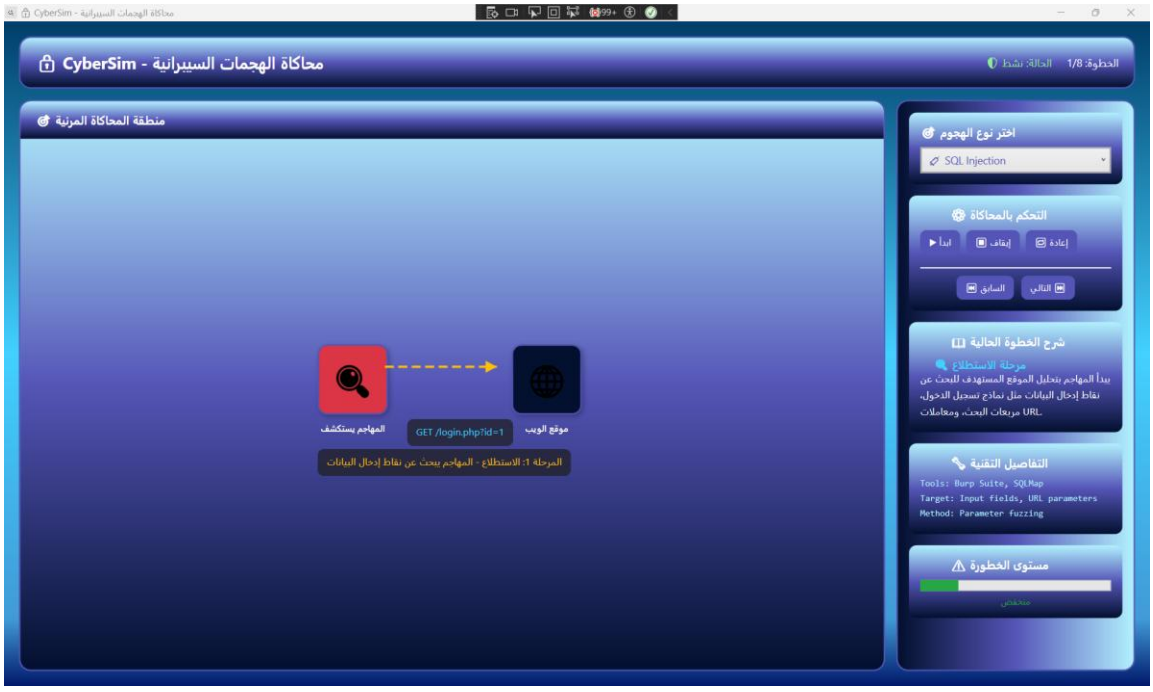
وتظهر الواجهة هذه التي تحتوي على معلومات إضافية عن التهديد المكتشف عند الضغط مرتين على التهديد الموجود في منطقة التهديدات المكتشفة.

واجهة محاكاة الهجمات :

ومن خلال زر simulator الموجود في هذه الواجهة يمكن الانتقال الى الواجهة التالية وهي واجهة محاكاة لعشر هجمات بشكل تعليمي.

رسم توضيحي 10-5 ازرار التنقل

والواجهة كالآتي :



رسم توضيحي 11-5 واجهة المحاكاة

في هذه الواجهة :

1- اختر نوع الهجوم : ومن خلاله يمكن عرض عشر هجمات للاختيار لعرض خطوات الهجوم وكيفيته.

رسم توضيحي 12-5 أنواع الهجمات

2- التحكم بالهجمات : وفيها ازرار للتحكم في إيقاف او إعادة او بدأ الهجوم وعند البدء يكون الفترة للانتظار عند الانتقال من خطوة الى أخرى 5 ثوان أيضا عرض الخطوة السابقة والخطوة التالية .

3- شرح الخطوة الحالية : حسب كل خطوة يقدم شرح مختصر عن كل خطوة تتم خلال الهجوم .

4- التفاصيل التقنية : مثلا الأدوات التي يمكن استخدامها لتنفيذ الهجوم والاهداف والطرق وأيضا الجمل التي يمكن كتابتها لتنفيذ الهجوم

5- مستوى الخطورة : لعرض كل حطوة في الهجوم ماهو مستوى خطورة هذه الخطوة اذا تمت فعلا .

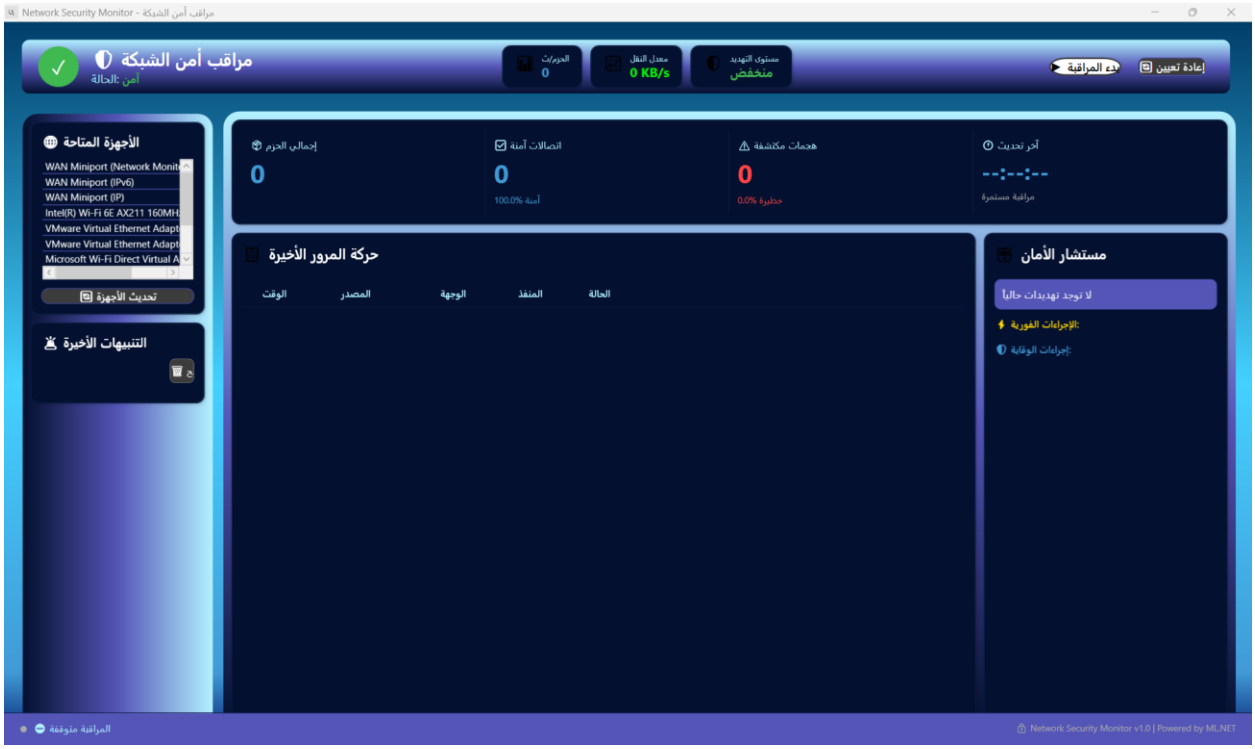
6- ومنطقة المحاكاة المرئية حيث يتم عرض الهجوم بايقونات تم انشائها عن طريق canva .

واجهة مراقبة الشبكة :

ومن خلال العودة الى الواجهة الرئيسية للانتقال الى واجهة مراقبة الشبكة نضغط على زر Networking.

رسم توضيحي 13-5 أزرار التنقل

واجهة مراقبة الشبكة تقوم بالتقاط كل الحركة او Trafficعن طريق واجهة الوايفاي



رسم توضيحي 14-5 واجهة مراقبة الشبكة

مكونات الواجهة :

1- ازرار بدء وإعادة تعيين المراقبة

2- منطقة الأجهزة المتاحة : هي interfaces التي يمكن مراقبة الحركة فيها ولكن حاليا لا يعمل الا عن طريق واجهة الوايفاي

3- منطقة مستشار الامان : هي المنطقة التي ستعرض النصائح والإجراءات التي يجب اتخاذها عند اكتشاف نوع معين من الهجوم

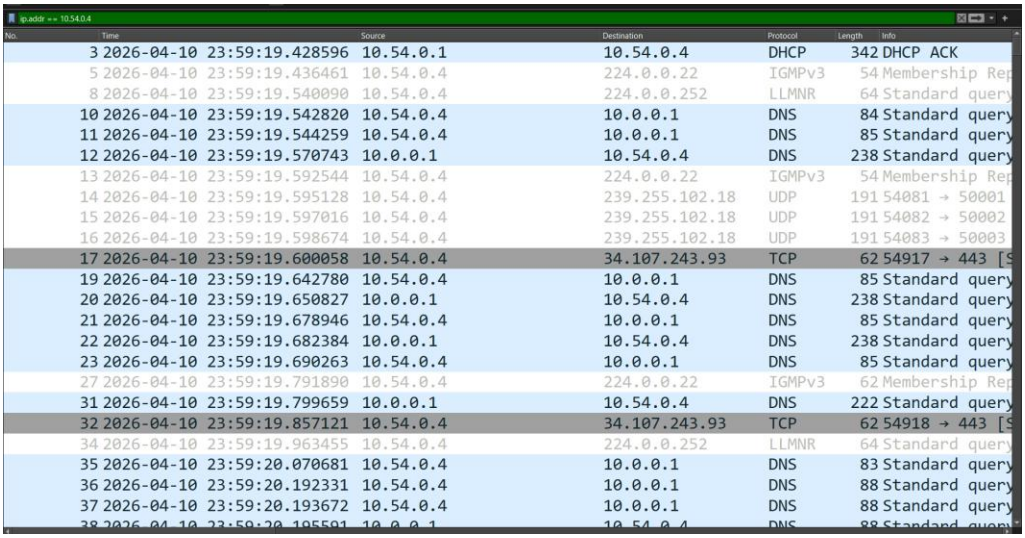
4- منطقة التنبيهات الأخيرة : تستعرض هذه المنطقة التنبيهات او التهديدات التي رصدها في حركة المرور

5- منطقة حركة المرور : تستعرض حركة الTraffic

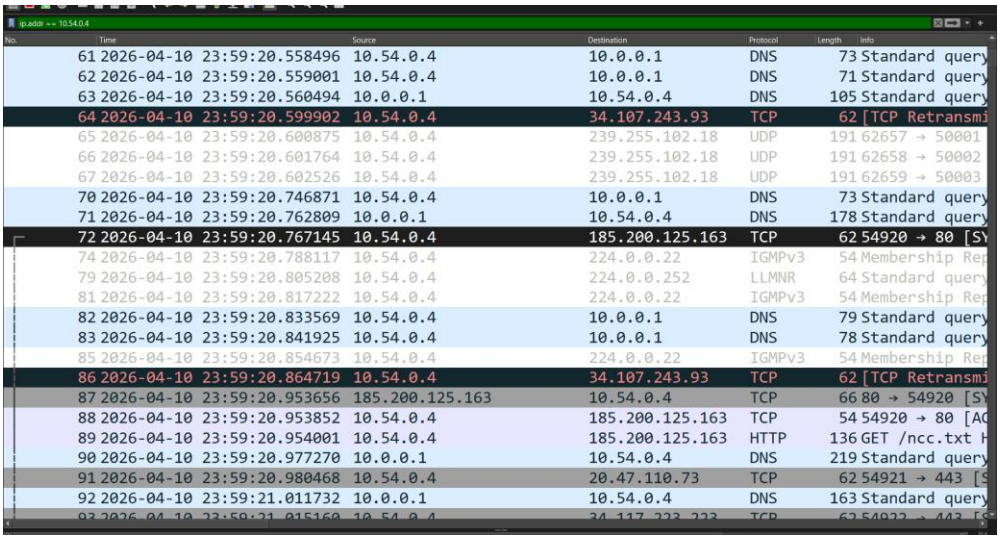
لاختبار الواجهة أولا سيتم مقارنة نتائج حركة المرور في التطبيق بحركة التي يتم رصدها عن طريق واير شارك.

رسم توضيحي 15-5 منطقة مراقبة حركة مرور البيانات

حركة المرور في التطبيق مع مقارنة IP للمصدر والوجهة مع IP للمصدر والوجهة في حركة مرور في الواير شارك يتضح انه الحركة حقيقية وليست مجرد مصادر او وجهات او حركة مزيفة.



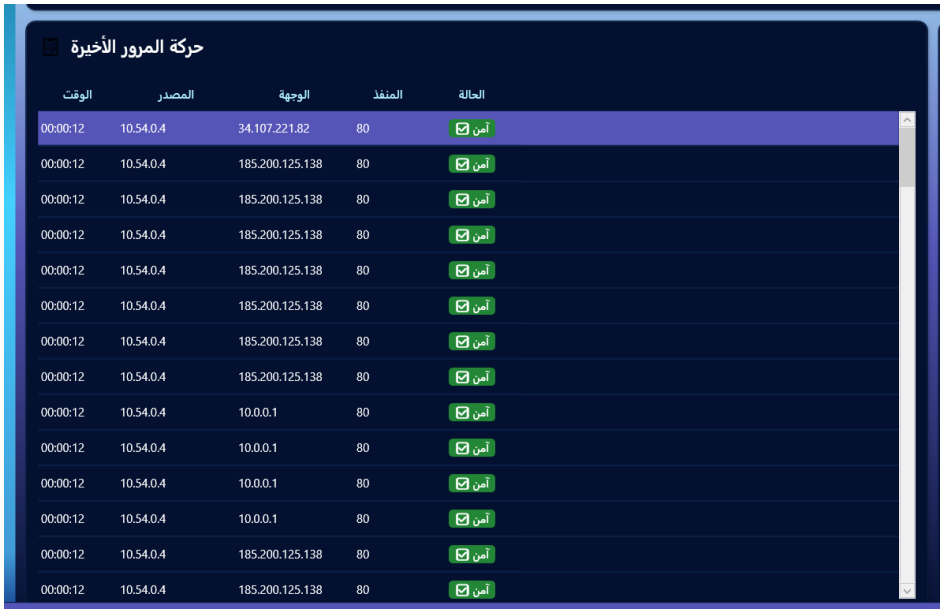
رسم توضيحي 16-5 حركة البيانات في WireShark



No.	Time	Source	Destination	Protocol	Length	Info
61	2026-04-10 23:59:20.558496	10.54.0.4	10.0.0.1	DNS	73	Standard query
62	2026-04-10 23:59:20.559001	10.54.0.4	10.0.0.1	DNS	71	Standard query
63	2026-04-10 23:59:20.560494	10.0.0.1	10.54.0.4	DNS	105	Standard query
64	2026-04-10 23:59:20.599902	10.54.0.4	34.107.243.93	TCP	62	[TCP Retransmi
65	2026-04-10 23:59:20.600875	10.54.0.4	239.255.102.18	UDP	191	62657 → 50001
66	2026-04-10 23:59:20.601764	10.54.0.4	239.255.102.18	UDP	191	62658 → 50002
67	2026-04-10 23:59:20.602526	10.54.0.4	239.255.102.18	UDP	191	62659 → 50003
70	2026-04-10 23:59:20.746871	10.54.0.4	10.0.0.1	DNS	73	Standard query
71	2026-04-10 23:59:20.762809	10.0.0.1	10.54.0.4	DNS	178	Standard query
72	2026-04-10 23:59:20.767145	10.54.0.4	185.200.125.163	TCP	62	54920 → 80 [SY
74	2026-04-10 23:59:20.788117	10.54.0.4	224.0.0.22	IGMPv3	54	Membership Rep
79	2026-04-10 23:59:20.805208	10.54.0.4	224.0.0.252	LLMNR	64	Standard query
81	2026-04-10 23:59:20.817222	10.54.0.4	224.0.0.22	IGMPv3	54	Membership Rep
82	2026-04-10 23:59:20.833569	10.54.0.4	10.0.0.1	DNS	79	Standard query
83	2026-04-10 23:59:20.841925	10.54.0.4	10.0.0.1	DNS	78	Standard query
85	2026-04-10 23:59:20.854673	10.54.0.4	224.0.0.22	IGMPv3	54	Membership Rep
86	2026-04-10 23:59:20.864719	10.54.0.4	34.107.243.93	TCP	62	[TCP Retransmi
87	2026-04-10 23:59:20.953656	185.200.125.163	10.54.0.4	TCP	66	80 → 54920 [SY
88	2026-04-10 23:59:20.953852	10.54.0.4	185.200.125.163	TCP	54	54920 → 80 [AC
89	2026-04-10 23:59:20.954001	10.54.0.4	185.200.125.163	HTTP	136	GET /ncc.txt H
90	2026-04-10 23:59:20.977270	10.0.0.1	10.54.0.4	DNS	219	Standard query
91	2026-04-10 23:59:20.980468	10.54.0.4	20.47.110.73	TCP	62	54921 → 443 [S
92	2026-04-10 23:59:21.011732	10.0.0.1	10.54.0.4	DNS	163	Standard query

رسم توضيحي 17-5 حركة البيانات في WireShark

وهذه حركة المرور التي تم التقاطها في الواير شارك .



رسم توضيحي 18-5 توضيح قلة الإيجابيات السلبية

واختبار الإيجابيات السلبية حيث انها اقل ما يمكن مع مراقبة مستمرة للحركة المرور .

لاختبار اكتشاف التطبيق للهجمات عن طريق الذكاء الاصطناعي وتصنيفها سنقوم ببعض الهجمات من خلال نظام كالي لينكس.

هجوم Udp-Flood :

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --udp --flood -p 1900 10.54.0.4 --data 1400 -c 10000 --fast
HPING 10.54.0.4 (eth0 10.54.0.4): udp mode set, 28 headers + 1400 data bytes
hping in flood mode, no replies will be shown
^C
--- 10.54.0.4 hping statistic ---
65357 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

رسم توضيحي 19-5 هجوم UDP-Flood

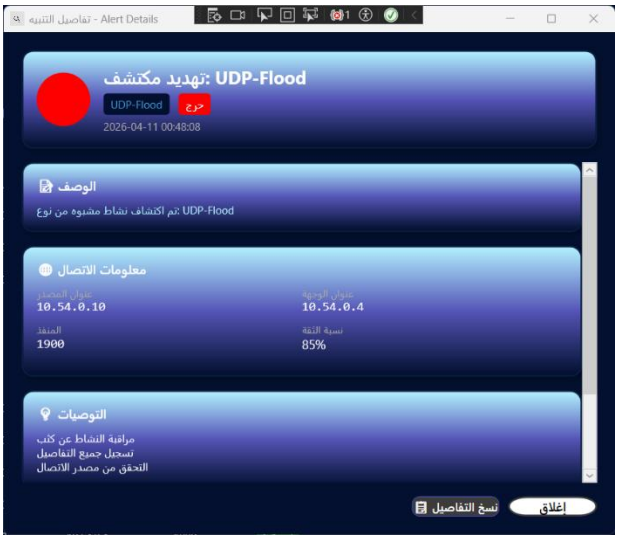
عن طريق تنفيذ هجمة UDP-FLOOD من خلال الشبكة على النظام المثبت لتطبيق cybersim سيتم اكتشاف هجمة قوية كهذه منفذه من خلال أداة Hping3 على port مفتوح 1900

وهكذا كانت النتائج

رسم توضيحي 20-5 رد فعل التطبيق لهجمة UDP

هذا ناتج حدوث الهجمة فعلا تم تصنيفها في منطقة التنبيهات الأخيرة على انها هجمة من نوع UDP-FLOOD وفي منطقة مستشار الامن تم إعطاء النصائح والإجراءات التي يجب اتخاذها .

وعند الضغط على الهجوم من منطقة التنبيهات الأخيرة تظهر النافذة الاتيه لتعرض تفاصيل اكثر عن الهجمة مثل المصدر والوجهة



رسم توضيحي 21-5 واجهة المعلومات الإضافية عن الهجمة

هجوم DDos and WenAttack :

عن طريق نفس الأداة في نظام الكالي لينكس Hping3 تم تنفيذ هجمتين في نفس الوقت هجوم DdoS عن طريق استخدام اكثر من IP للهجوم وليس مجرد واحد عن طريق rand-source– وهجمة Wepattack بسبب استخدام PORT 80 او حتى لو استخدمنا 443 .

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 -S --flood --rand-source -p 80 10.54.0.4 -d 1400
HPING 10.54.0.4 (eth0 10.54.0.4): S set, 40 headers + 1400 data bytes
hping in flood mode, no replies will be shown
^C
── 10.54.0.4 hping statistic ──
223236 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

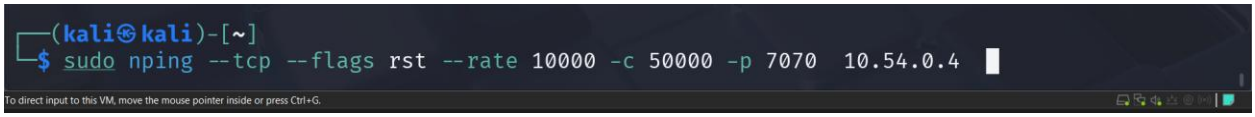
رسم توضيحي 22-5 هجومي WebAttack and DDoS

والنتيجة في تطبيق Cybersim :

رسم توضيحي 23-5 رد فعل التطبيق على هجوم DDoS

رسم توضيحي 24-5 رد فعل التطبيق على هجوم Webattack

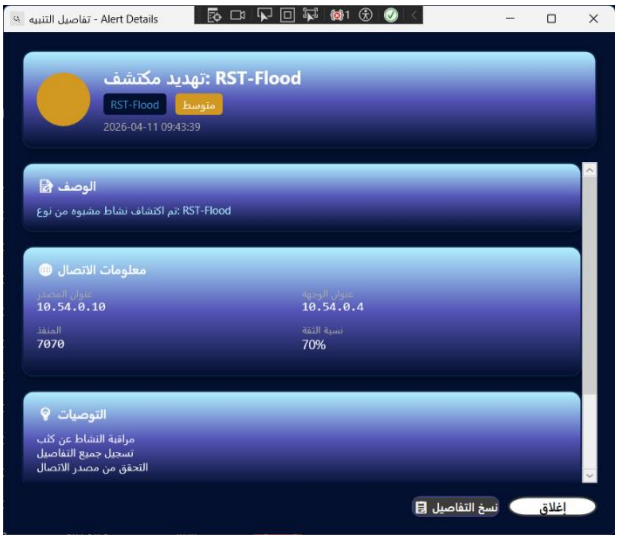
هجوم RST-Flood and Syn-Flood :



رسم توضيحي 25-5 هجوم RST-Flood

عن طريق استخدام أداة Nping لعمل هجمتي RST , SYN Flood في الكالي لينكس أولا تم تنفيذ هجوم ال RST ثم هجمة SYN كانت النتائج كالتالي في تطبيق cybersim

رسم توضيحي 26-5 رد فعل التطبيق على هجوم RST-Flood



رسم توضيحي 27-5 واجهة المعلومات الإضافية عن RST-Flood

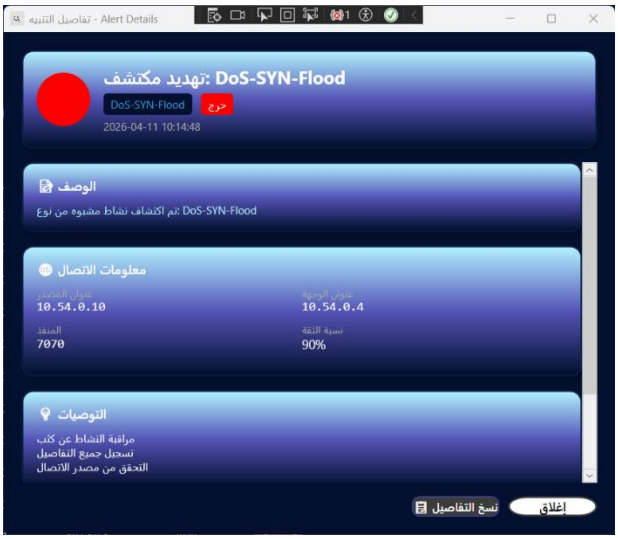
كود هجوم SYN :

```
┌──(kali㉿kali)-[~]
└─$ sudo nping --tcp --flags syn --rate 2000000 -c 50000 -p 7070 10.54.0.4
```

رسم توضيحي 28-5 هجوم SYN-Flood

النتائج في cybersim :

رسم توضيحي 29-5 رد فعل التطبيق على هجوم SYN

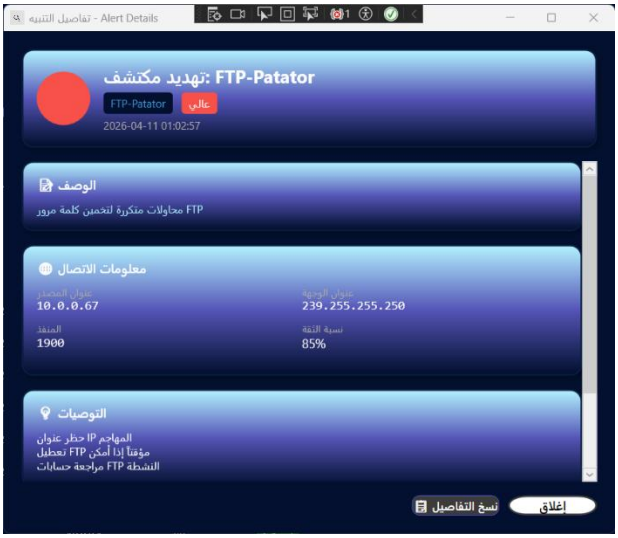


رسم توضيحي 30-5 واجهة المعلومات الإضافية عن هجمة SYN-Flood

هجمتي SSH and FTP :

تم ادراج بيانات اختبار الى التطبيق بسبب إمكانيات الأجهزة لانها Home Edition ولا يمكن فتح 22 و 21 هذه المنافذ فلا يمكن تجريب الهجوم واقعيا لذا تم اختبار منطق العمل وكانت النتيجة على هجوم FTP:

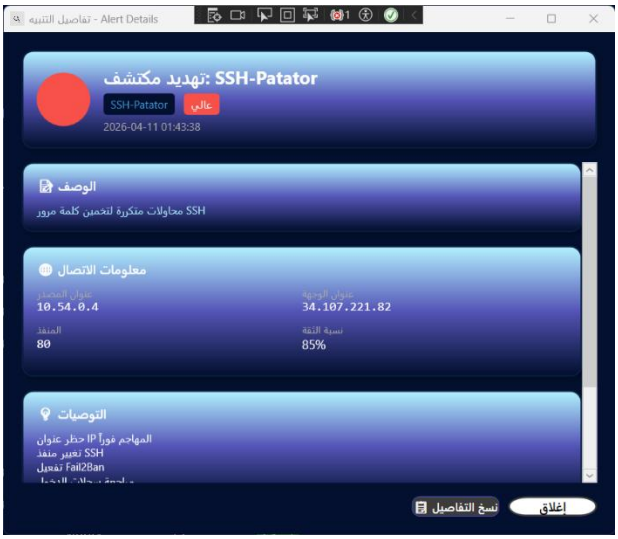
رسم توضيحي 31-5 هجوم Brute Force FTP



رسم توضيحي 32-5 واجهة المعلومات الإضافية لهجمة Brute Force FTP

هجوم SSH :

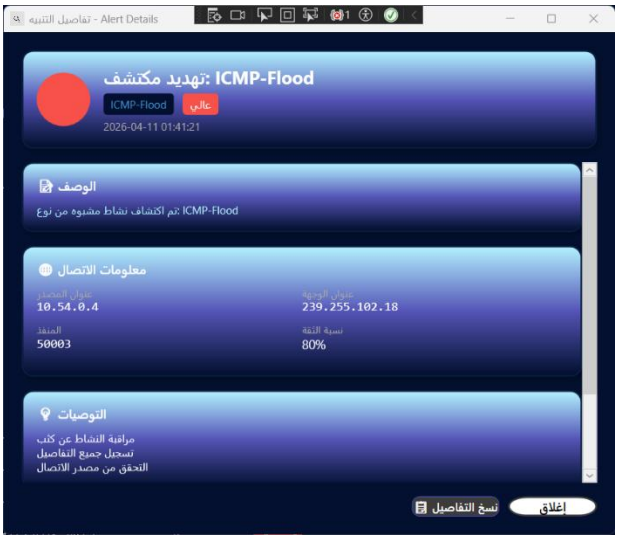
رسم توضيحي 33-5 هجوم Brute Force SSH



رسم توضيحي 34-5 واجهة المعلومات الإضافية لهجمة Brute Force SSH

هجوم ICMP :

رسم توضيحي 35-i5 هجوم ICMP-Flood



رسم توضيحي 36-5 واجهة المعلومات الإضافية عن هجمة ICMP-Flood

وهذه هي الهجمات الشبكية التي يمكن تطبيق cybersim ان يكشفها ويعطي نصائح وإجراءات للقيام بها مع نسبة عالية من الدقة واقل من الإيجابيات السلبية .

حتى لو لم يستطيع المستخدم من ان يراقب الشبكة تماما يتم حفظ سجل التهديدات التي ظهرت في منطقة التنبيهات الأخيرة .

الفصل 6
الاستنتاجات والتوصيات المستقبلية
(Conclusions and Future Recommendations)

المقدمة

يتناول هذا الفصل أهم النتائج التي تم التوصل إليها من خلال تنفيذ مشروع CyberSim Defender، بالإضافة إلى التوصيات المقترحة لتطوير المشروع مستقبلاً بما يعزز فعاليته وقابلية استخدامه في البيئات التعليمية والمهنية.

1.6 الاستنتاجات:

من خلال تنفيذ مشروع CyberSim Defender وتحليل نتائجه، يمكن القول إن الجمع بين محاكاة الهجمات السيبرانية والمراقبة الأمنية الحقيقية داخل بيئة ويندوز يمثل خطوة مهمة لفهم طبيعة التهديدات الحديثة دون تعريض الأنظمة الحقيقية للمخاطر. فقد أظهر المشروع إمكانية إنشاء نظام متكامل يعتمد على تقنيات حديثة مثل WPF لبناء الواجهات التفاعلية، و SharpPcap لالتقاط وتحليل حزم الشبكة، وONNX Runtime لتشغيل نماذج الذكاء الاصطناعي، مما أتاح مراقبة وتحليل حركة الشبكة والملفات الحساسة محاكاة 10 أنواع مختلفة من الهجمات (SQL Injection ، DDoS، Port Scan، Ransomware، وغيرها) بطريقة عملية ومنهجية.

كما بيّن المشروع أن دمج الذكاء الاصطناعي في مجال الأمن السيبراني يسهم في تحسين عملية تصنيف الهجمات وفهم سلوكها، حيث تم تدريب نموذج Random Forest على مجموعة بيانات CIC-IDS2017(التي تحتوي على 79 ميزة وأكثر من 2.5 مليون سجل) وتصديره إلى تنسيق ONNX لتشغيله داخل التطبيق. ساعد هذا النموذج في تحليل البيانات المستخلصة من الحزم الشبكية وتقديم استجابات أكثر دقة من مستشار الأمان (Advisor Service) الذي يوفر إجراءات فورية ونصائح وقائية حسب نوع الهجوم، مقارنة بالتحليل اليدوي التقليدي. وهذا يعكس أهمية تبني التقنيات الذكية في أنظمة الحماية المستقبلية.

من ناحية أخرى، أثبتت الواجهات التفاعلية الثلاث للمشروع فعاليتها في توضيح مسار الهجوم بصرياً، مما يجعل النظام أداة تعليمية مناسبة للطلاب والمتدربين في مجال الأمن السيبراني. فقد مكنت واجهة محاكاة الهجمات المستخدم من تتبع مراحل الهجوم خطوة بخطوة مع رسوم متحركة وتفاصيل تقنية، بينما أتاحت واجهة مراقبة الملفات اكتشاف التغييرات غير المصرح بها على المسارات الحرجة (مثلSystem32 ، Startup، Temp)عبر حساب قيم التجزئة MD5، وأظهرت واجهة مراقبة الشبكة التنبيهات الأمنية والإحصائيات الفورية، مما يعزز الوعي الأمني ويطور مهارات التحليل والاستجابة للحوادث.

كما أظهر تصميم النظام وفق هيكلية واضحة تعتمد على نمط MVVM و Service Locator أنه قابل للتوسع والتطوير مستقبلاً، حيث يمكن إضافة أنواع جديدة من الهجمات إلى محاكي الهجمات، أو إضافة قواعد كشف جديدة إلى نظام مراقبة الشبكة، أو إضافة مسارات جديدة للمراقبة في نظام مراقبة الملفات، دون الحاجة إلى إعادة بناء النظام بالكامل. إضافة إلى ذلك، أوضح المشروع إمكانية تحديث قاعدة المعرفة بالتهديدات الجديدة من خلال إضافة`AttackStep` جديدة أو تعديل قواعد الكشف، مما يضمن بقاء النظام مواكباً للتطورات المستمرة في مجال الهجمات السيبرانية.

وبشكل عام، يمكن اعتبار CyberSim Defender خطوة أولية ناجحة نحو بناء نظام متكامل يجمع بين المحاكاة التعليمية، الكشف الاستباقي، و المراقبة الأمنية، ويشكل أساساً يمكن البناء عليه لتطوير حلول أكثر تقدماً في المستقبل.

2.6 التوصيات المستقبلية:

على الرغم من تحقيق مشروع CyberSim Defender لأهدافه الأساسية، إلا أن هناك عدة جوانب يمكن تطويرها مستقبلاً لتعزيز كفاءته وفعاليته. فمن المستحسن العمل على تحسين نماذج الذكاء الاصطناعي المستخدمة في التصنيف، من خلال تبني نماذج أكثر تطوراً مثل XGBoost أو LightGBM أو Neural Networks، بالإضافة إلى توسيع بيانات التدريب لتشمل أنواعاً أوسع من الهجمات الواقعية، وإعادة تدريب النموذج على مجموعة بيانات محدثة (مثل CIC-IDS2018 أو CSE-CIC-IDS2019) لزيادة دقة الكشف.

كما يُوصى بتوسيع نطاق نظام مراقبة الشبكة ليشمل كشف أنواع أكثر تعقيداً من الهجمات مثل الهجمات المتقدمة المستمرة (APT)، هجمات سلسلة التوريد، هجمات اليوم الصفري (Zero-Day)، Infiltration، و Heartbleed، إلى جانب تحسين آليات الكشف والاستجابة لها. كذلك يمكن تطوير النظام ليعمل على أنظمة تشغيل أخرى مثل Linux و macOS، أو تحويله إلى تطبيق ويب يسهل الوصول إليه واستخدامه دون الحاجة إلى تثبيت محلي

وأيضا تمكين المراقبة على مستوى كل الواجهات وليس فقط الوايفاي..

بالإضافة إلى ذلك، يمكن تعزيز قدرات مراقبة الملفات من خلال إضافة المزيد من المسارات الحرجة (مثل مجلدات التطبيقات الحساسة)، واستخدام خوارزميات تجزئة أكثر أماناً مثل SHA-256 بدلاً من MD5، وإضافة آلية للتمييز بين التحديثات الشرعية والتهديدات الحقيقية بشكل أكثر دقة. كما يمكن دمج النظام مع أدوات مثل Wireshark لتحليل الحزم بشكل أعمق، و Volatility لتحليل الذاكرة، مما يوفر رؤية أشمل للحوادث الأمنية

وفيما يتعلق بواجهة المستخدم، يُقترح تطوير لوحات معلومات تفاعلية تعرض نتائج التحليل بشكل بصري باستخدام الرسوم البيانية (مثل مخططات الزمن لتطور الهجمات، وتوزيع أنواع التهديدات)، مع توفير وضعين للاستخدام: وضع تعليمي مبسط للمبتدئين يعرض شرحاً تفصيلياً لكل هجوم، ووضع احترافي متقدم لمحللي الأمن يعرض التفاصيل التقنية والإحصائيات المتقدمة. كما يمكن إضافة سيناريوهات تدريب جاهزة بمستويات صعوبة مختلفة مع نظام تقييم تلقائي لأداء المستخدم بعد كل تجربة محاكاة.

وأخيراً، يُوصى بإمكانية دمج النظام مع أدوات أمنية مؤسسية مثل أنظمة SIEM (مثال: Splunk، ELK) و EDR (مثال: CrowdStrike، Carbon Black)، مما يسمح باستخدامه داخل بيئات العمل الحقيقية كأداة اختبار وتقييم جاهزية أمنية، وليس فقط كأداة تعليمية. كما يمكن إضافة ميزة تصدير التقارير بصيغ متعددة (PDF، JSON، CSV) لتوثيق التنبيهات والتهديدات المكتشفة.

قائمة المراجع(References) :

1. Kaspersky. (2024). Cyberthreats in the Middle East: Regional Malware Trends and Targeted Attacks Report 2023–2024. Retrieved from https://www.kaspersky.com

2. Digital Watch Observatory. (2024). Cybersecurity Readiness in Yemen: Institutional Gaps and Threat Exposure. Retrieved from https://digitalwatch.giplatform.org

3. Manurung, J., Mardamsyah, A., & Sianipar, B. (2025). Enhancing Security in Smart Robot Digital Twins Through Intrusion Detection Systems. *Applied Sciences*, 15(9), 4596. doi: 10.3390/app15094596 Available at: https://www.mdpi.com/2076-3417/15/9/4596

4. Obahor, V., & Oluwagbenga, A. (2025). Design of an Open-Source Cyber Range for Educators and Security Professionals. *AAIRJ*, 2(1), pp. 0-0. doi: 10.23246/AAIRJ.2025.02.01.03 Available at: https://public.thinkonweb.com/journals/aairj/digital-library/101969

5. Muppavaram, K., Aruna Sri, T., Krishna, T. M., Tripathi, J., Das, M. N., Mani, S., Prasad, G. L. V., & Manyam, T. (2026). An Adaptive AI-Driven Cyber Threat Detection Framework for Securing Heterogeneous IoT Networks. *MTMT*. Available at: https://m2.mtmt.hu/api/publication/36840842

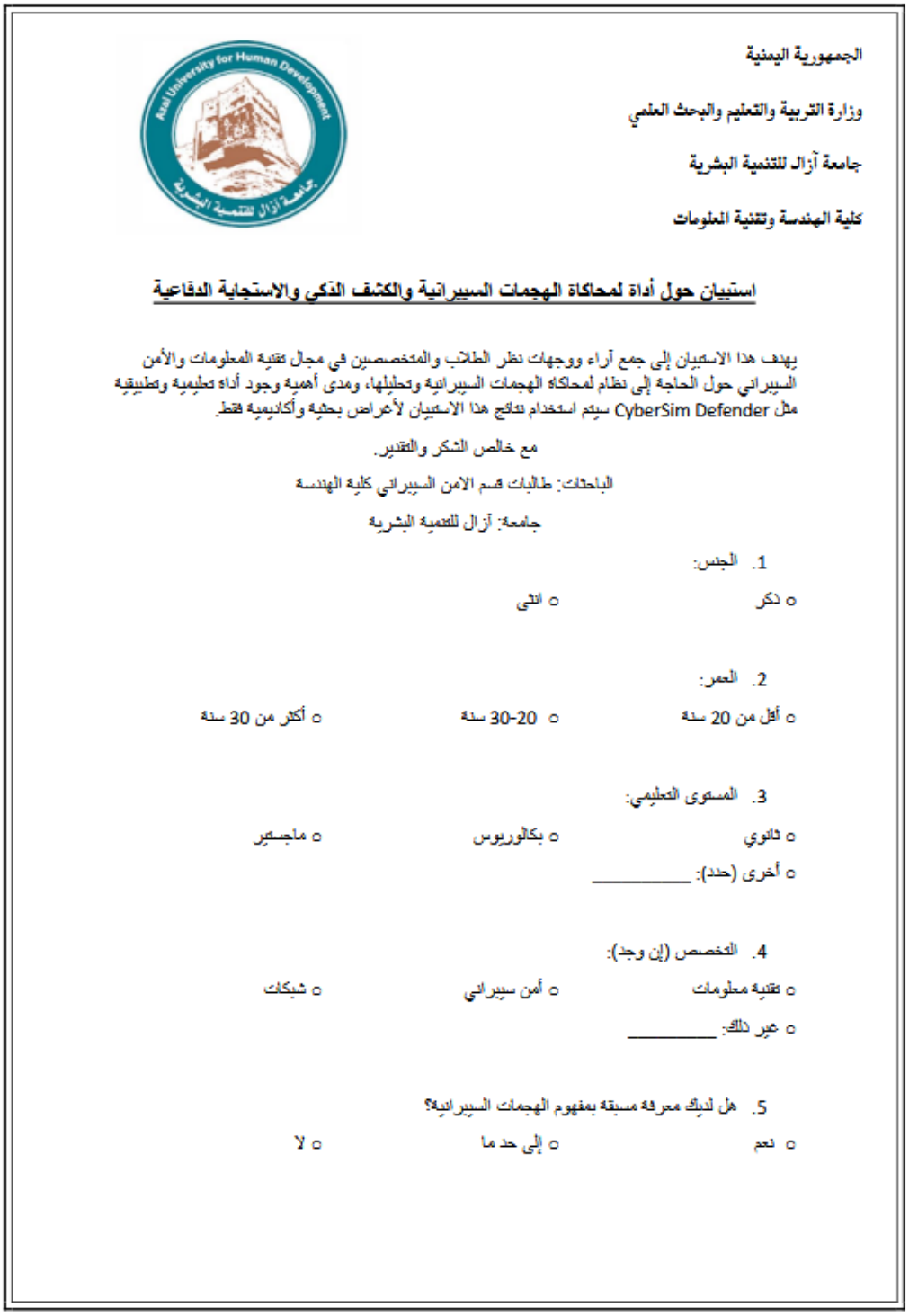
6. **Uddin, K. M. M., & Chishti, M. A. (2022).** Network Anomaly Uncovering on CICIDS-2017 Dataset: A Supervised Artificial Intelligence Approach. *IEEE EIT*. doi: 10.1109/EIT53891.2022.9814045 Available at : https://ieeexplore.ieee.org/document/9814045

.7 **University of New Brunswick (UNB). (2017).** *CIC-IDS2017: Intrusion Detection Evaluation Dataset*. Canadian Institute for Cybersecurity. Retrieved from https://www.unb.ca/cic/datasets/ids-2017.html

.8 **Alavala, R. (2024).** Investigating the Effectiveness of Hash Line Baseline for File Integrity Monitoring. *2024 5th International Conference on Image Processing and Capsule Networks (ICIPCN)*, IEEE. doi: 10.1109/ICIPCN61550.2024.10660915 From https://ieeexplore.ieee.org/document/10660915

الملاحق (Appendices) :

1 ملحق (أ): نموذج استبيان الطلاب والتخصصين في مجال تقنية المعلومات والامن السيبراني



الجمهورية اليمنية

وزارة التربية والتعليم والبحث العلمي

جامعة آزال للتنمية البشرية

كلية الهندسة وتقنية المعلومات

استبيان حول أداة لمحاكاة الهجمات السيبرانية والكشف الذكي والاستجابة الدفاعية

يهدف هذا الاستبيان إلى جمع آراء ووجهات نظر الطلاب والمتخصصين في مجال تقنية المعلومات والأمن السيبراني حول الحاجة إلى نظام لمحاكاة الهجمات السيبرانية وتحليلها، ومدى أهمية وجود أداة تعليمية وتطبيقية مثل CyberSim Defender سيتم استخدام نتائج هذا الاستبيان لأغراض بحثية وأكاديمية فقط.

مع خالص الشكر والتقدير.

الباحثات: طالبات قسم الامن السيبراني كلية الهندسة

جامعة: آزال للتنمية البشرية

1. الجنس:

○ ذكر ○ انثى

2. العمر:

○ أقل من 20 سنة ○ 20-30 سنة ○ أكثر من 30 سنة

3. المستوى التعليمي:

○ ثانوي ○ بكالوريوس ○ ماجستير

○ أخرى (حدد): _____

4. التخصص (إن وجد):

○ تقنية معلومات ○ أمن سيبراني ○ شبكات

○ غير ذلك: _____

5. هل لديك معرفة مسبقة بمفهوم الهجمات السيبرانية؟

○ نعم ○ إلى حد ما ○ لا

رسم توضيحي 1-6 نموذج استبيان الطلاب

الجمهورية اليمنية

وزارة التربية والتعليم والبحث العلمي

جامعة آزال للتنمية البشرية

كلية الهندسة وتقنية المعلومات

6. هل سبق أن درست أو تدربت على الأمن السيبراني؟

○ نعم ○ لا

7. هل تعتقد أن الهجمات السيبرانية أصبحت تهديدًا حقيقيًا للمؤسسات والأفراد؟

○ أوافق ○ إلى حد ما ○ لا أوافق

8. هل تعتقد أن التعلم النظري وحده كافٍ لفهم الهجمات السيبرانية؟

○ نعم ○ إلى حد ما ○ لا

9. هل ترى أن التدريب العملي على محاكاة الهجمات يساعد في فهمها بشكل أفضل؟

○ نعم ○ إلى حد ما ○ لا

10. هل صادف أن احتجت إلى بيئة عملية لتجربة أو دراسة الهجمات السيبرانية ولم تجدها؟

○ نعم ○ أحيانًا ○ لا

11. هل تعتقد أن وجود نظام مثل **CyberSim Defender** سيكون مفيدًا للتعلم والتدريب؟

○ مفيد ○ نوعا ما ○ غير مفيد

12. هل تعتقد أن عرض مسار الهجوم بشكل بصري (خريطة تفاعلية) سيساعد في الفهم؟

○ نعم ○ إلى حد ما ○ لا

13. هل ترى أن دمج الذكاء الاصطناعي في تحليل الهجمات أمر ضروري؟

○ ضروري ○ غير ضروري

رسم توضيحي2-6 نموذج استبيان الطلاب

الجمهورية اليمنية

وزارة التربية والتعليم والبحث العلمي

جامعة آزال للتنمية البشرية

كلية الهندسة وتقنية المعلومات

14. برأيك، من الفئات التي ستستفيد أكثر من هذا النظام؟ (يمكن اختيار أكثر من خيار)

- ○ طلاب الأمن السيبراني
- ○ مدراء الأنظمة والشبكات
- ○ باحثون في مجال الأمن
- ○ شركات البرمجيات الأمنية
- ○ المؤسسات الحكومية
- ○ المدربون في مجال الأمن السيبراني

15. هل تعتقد أن هذا النظام يمكن أن يساعد المؤسسات على تحسين جاهزيتها الأمنية؟

○ نعم ○ إلى حد ما ○ لا

16. هل ترى أن هذا المشروع يمكن أن يكون إضافة علمية وتقنية مهمة في مجال الأمن السيبراني؟

○ نعم ○ إلى حد ما ○ لا

17. ما الميزات التي تتمنى وجودها في نظام مثل CyberSim Defender ؟

.....

.....

.....

18. هل لديك أي ملاحظات أو اقتراحات أخرى؟

.....

.....

.....

رسم توضيحي 3-6 نموذج استبيان الطلاب

2 ملحق (ب): نموذج استبيان آراء المؤسسات والشركات التقنية والمدربين والمتخصصين :

الجمهورية اليمنية

وزارة التربية والتعليم والبحث العلمي

جامعة آزال للتنمية البشرية

كلية الهندسة وتقنية المعلومات

استبيان حول أداة لمحاكاة الهجمات السيبرانية والكشف الذكي والاستجابة الدفاعية

يهدف هذا الاستبيان إلى جمع آراء المؤسسات والشركات التقنية والمدربين والمتخصصين في مجال تقنية المعلومات والشبكات والأمن السيبراني حول الحاجة إلى نظام لمحاكاة الهجمات السيبرانية وتحليلها، ومدى فائدة وجود أداة مثل CyberSim Defender في البيئات التعليمية والمهنية سيتم استخدام النتائج لأغراض أكاديمية وبحثية فقط.

مع خالص الشكر والتقدير.

الباحثات: طالبات قسم الامن السيبراني كلية الهندسة

جامعة: آزال للتنمية البشرية

1. جهة العمل/المؤسسة:

.....

2. طبيعة الجهة:

- ○ شركة تقنية
- ○ مؤسسة حكومية
- ○ مؤسسة تعليمية/تدريبية
- ○ شركة أمن سيبراني
- ○ أخرى: _____

3. المسمى الوظيفي:

- ○ مهندس شبكات
- ○ مسؤول أنظمة(SysAdmin)
- ○ محلل أمن سيبراني
- ○ مدرب/محاضر
- ○ مطور برمجيات
- ○ أخرى: _____

4. سنوات الخبرة في المجال التقني:

- ○ أقل من سنتين
- ○ 2-5 سنوات
- ○ 6-10 سنوات
- ○ أكثر من 10 سنوات

رسم توضيحي 4-6 استبيان الشركات والمؤسسات

الجمهورية اليمنية

وزارة التربية والتعليم والبحث العلمي

جامعة آزال للتنمية البشرية

كلية الهندسة وتقنية المعلومات

5. هل تتعرض مؤسستك لمحاولات هجمات سيبرانية؟

○ نعم بشكل متكرر ○ أحيانًا

○ نادرًا ○ لا أعلم

6. هل تمتلك مؤسستك أدوات لاختبار الأمن أو محاكاة الهجمات؟

○ نعم ○ لا ○ قيد التخطيط

7. ما أكثر أنواع التهديدات التي تواجهها مؤسستك؟ (يمكن اختيار أكثر من خيار)

○ هجمات حجب الخدمة(DDoS) ○ اختراقات الشبكة

○ برمجيات خبيثة(Malware) ○ تصيد احتيالي(Phishing)

○ اختراق حسابات ○أخرى: _____

8. هل ترى أن تدريب الفرق التقنية عمليًا على سيناريوهات هجوم مفيد للمؤسسة؟

○ مفيد ○ غير مفيد

9. هل تعتقد أن وجود بيئة محاكاة آمنة لتجربة الهجمات ضروري للمؤسسات؟

○ ضروري ○ إلى حد ما ○ غير ضروري

10. هل ترى أن الاعتماد على أدوات محاكاة الهجمات يساعد في اكتشاف الثغرات قبل استغلالها؟

○ نعم ○ إلى حد ما ○ لا

11. هل سبق أن احتجتم في مؤسستكم إلى بيئة لاختبار الدفاعات الأمنية ولم تكن متاحة؟

○ نعم ○ أحيانًا ○ لا

رسم توضيحي 5-6 استبيان الشركات والمؤسسات

الجمهورية اليمنية

وزارة التربية والتعليم والبحث العلمي

جامعة آزال للتنمية البشرية

كلية الهندسة وتقنية المعلومات

12. إلى أي مدى ترى فائدة نظام **CyberSim Defender** لمؤسستك؟

○ عالية ○ متوسطة ○ منخفضة

13. ما أهمية الجمع بين (المحاكاة + الكشف الذكي + الاستجابة الدفاعية) في نظام واحد؟

○ عالية ○ متوسطة ○ منخفضة

14. هل ترى أن عرض مسار الهجوم بشكل بصري (خريطة تفاعلية) سيساعد فريق الأمن؟

○ نعم ○ إلى حد ما ○ لا

15. ما مدى أهمية دمج الذكاء الاصطناعي في تحليل الهجمات من وجهة نظرك؟

○ ضروري ○ محايد ○ غير ضروري

16. كيف يمكن أن تستفيد مؤسستك من CyberSim Defender ؟ (يمكن اختيار أكثر من خيار)

○ تدريب فريق الأمن ○ اختبار جاهزية الأنظمة ○ اكتشاف الثغرات

○ تقييم فعالية أدوات الحماية ○ البحث والتطوير ○ أخرى: _____

17. هل تعتقد أن هذا النظام يمكن أن يحسن مستوى الأمن في المؤسسات المحلية؟

○ نعم ○ إلى حد ما ○ لا

18. ما الميزات التي تفضل وجودها في نظام مثل CyberSim Defender ؟

.....

.....

19. هل لديك أي ملاحظات أو اقتراحات لتطوير المشروع؟

.....

.....

رسم توضيحي 6-6 استبيان الشركات والمؤسسات