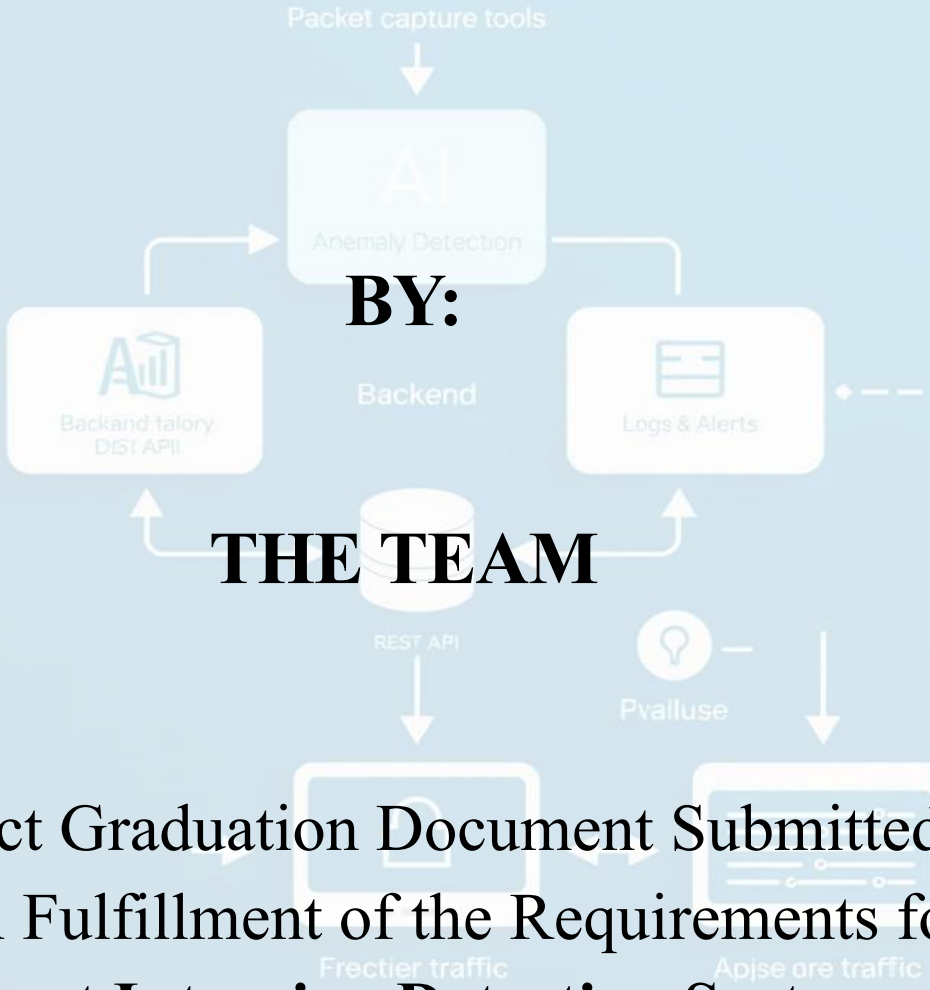
وزارة التعليم العالـــى
معهد الدلتا العالـــى
لنظم المعلومات الإدارية والمحـاسبية
بالمنصـــــــــورة

DELTA HIGHER INSTITUTE FOR MANAGEMENT ACCOUNTING INFORMATION SYSTEMS



BY:

THE TEAM

A Project Graduation Document Submitted in Partial Fulfillment of the Requirements for

Smart Intrusion Detection System

Faculty of BIS, Delta university
Mansoura, Egypt
2026

Introduction:

This project, titled "Smart Intrusion Detection System," has been submitted as part of the graduation requirements at Delta Higher Institute for Science & Technology. This milestone is the culmination of years of study, hands-on experience, and a deep commitment to technical excellence, innovation, and teamwork, The objective of this project is to design and implement an intelligent security solution capable of detecting and responding to unauthorized access attempts within modern digital infrastructures. The system's integration of state-of-the-art technologies is designed to facilitate real-time monitoring, the identification of anomalies, and the mitigation of threats with high precision and efficiency.

This project encompasses a variety of technical disciplines, including:

- **The field of Network Engineering encompasses the construction and fortification of infrastructural frameworks, with a focus on ensuring their security and resilience.**
- **The field of cybersecurity encompasses the application of threat analysis, incident response, and security protocols.**
- **The field of Artificial Intelligence (AI) and Machine Learning (ML) aims to facilitate intelligent behavior through the identification of anomalies and the implementation of automated decision-making processes.**
- **The system administrator's primary responsibility is the management of the core servers, with the objective of ensuring operational continuity.**
- **The objective of the Software Development initiative is to develop the system interface and central control dashboard.**

The team's interdisciplinary approach has facilitated the transformation of theoretical knowledge into a practical, real-world application. This endeavor has not only augmented our technical expertise but also fortified our problem-solving, collaboration, and perseverance skills—essential qualities for any aspiring professional navigating the rapidly evolving tech landscape.

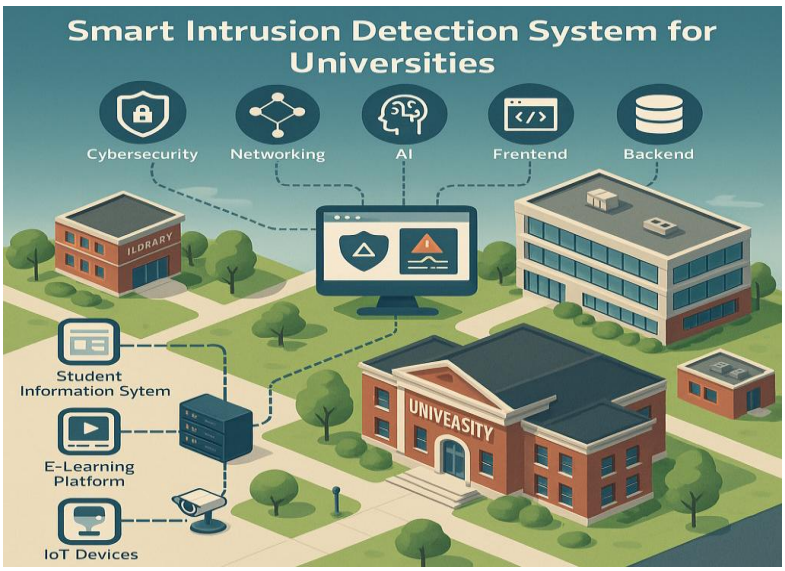
We would like to express our profound gratitude to our supervisor, **** is owed to our profound gratitude for his constant guidance and support, and the project's success would not have been possible without the contributions of all those who worked directly or indirectly on it. It is our hope that the publication of this book will fulfill two objectives: first, that it will serve as a comprehensive documentation of our work, and second, that it will function as a valuable source of inspiration for future learners and innovators.**

Smart Intrusion Detection System (SIDS)

Project Overview:

The Smart Intrusion Detection System (SIDS) is a sophisticated cybersecurity solution that is designed to detect, analyze, and respond to network intrusions in real-time. The integration of Cybersecurity, Networking, Artificial Intelligence (AI), Frontend, and Backend technologies enables SIDS to provide a robust, scalable, and user-friendly platform to safeguard networks from unauthorized access, malware, and other cyber threats. The documentation under review here meticulously delineates the conceptual framework of the project, the implementation approach, and the interplay of the involved domains to achieve a cohesive system.

نظام الكشف عن التطفل الذكي (SIDS) هو حل متطور للأمن السيبراني مصمم لاكتشاف عمليات اختراق الشبكة وتحليلها والاستجابة لها في الوقت الفعلي. يتيح التكامل بين تقنيات الأمن السيبراني والشبكات والذكاء الاصطناعي والواجهة الأمامية والخلفية لنظام SIDS توفير منصة قوية وقابلة للتطوير وسهلة الاستخدام لحماية الشبكات من الوصول غير المصرح به والبرمجيات الخبيثة والتهديدات السيبرانية الأخرى. تحدد الوثائق قيد المراجعة هنا بدقة الإطار المفاهيمي للمشروع، ونهج التنفيذ، والتفاعل بين المجالات المعنية لتحقيق نظام متماسك.



The following illustration is a simplification of the original concept

الرسم التوضيحي التالي هو تبسيط للمفهوم الأصلي

Project Idea:

SIDS aims to create a **proactive intrusion detection system** that leverages **AI** to identify anomalous network behavior, supported by a **secure backend** for data processing and a **user-friendly frontend** for real-time monitoring and interaction.

The system combines:

- **Cybersecurity**: To ensure secure data handling and threat mitigation.
- **Networking**: To monitor and analyze network traffic in real-time.
- **AI**: To detect anomalies and predict potential threats using machine learning.
- **Frontend**: To provide an intuitive interface for users to visualize threats and manage alerts.
- **Backend**: To process network data, store logs, and integrate AI models with the front end.

The goal is to build a system that is accessible to **network administrators**, **cybersecurity professionals**, and **organizations**, offering **real-time insights** and **automated responses** to cyber threats.

يهدف نظام SIDS إلى إنشاء نظام استباقي للكشف عن التسلل يستفيد من الذكاء الاصطناعي لتحديد السلوكيات الشاذة في الشبكة، مدعومًا بواجهة خلفية آمنة لمعالجة البيانات وواجهة أمامية سهلة الاستخدام للمراقبة والتفاعل في الوقت الفعلي.

يجمع النظام بين:

الأمن السيبراني: لضمان التعامل الآمن مع البيانات والتخفيف من التهديدات.

الشبكات: لمراقبة حركة مرور الشبكة وتحليلها في الوقت الفعلي.

الذكاء الاصطناعي: للكشف عن الحالات الشاذة والتنبؤ بالتهديدات المحتملة باستخدام التعلم الآلي.

الواجهة الأمامية: لتوفير واجهة سهلة الاستخدام للمستخدمين لتصور التهديدات وإدارة التنبيهات.

الواجهة الخلفية: لمعالجة بيانات الشبكة وتخزين السجلات ودمج نماذج الذكاء الاصطناعي مع الواجهة الأمامية.

الهدف هو بناء نظام يمكن لمسؤولي الشبكات ومحترفي الأمن السيبراني والمؤسسات الوصول إليه، وتقديم رؤى في الوقت الفعلي واستجابات آلية للتهديدات السيبرانية.

Objectives:

1. Real-Time Threat Detection: The ability to swiftly identify intrusions and anomalies in network traffic is paramount.

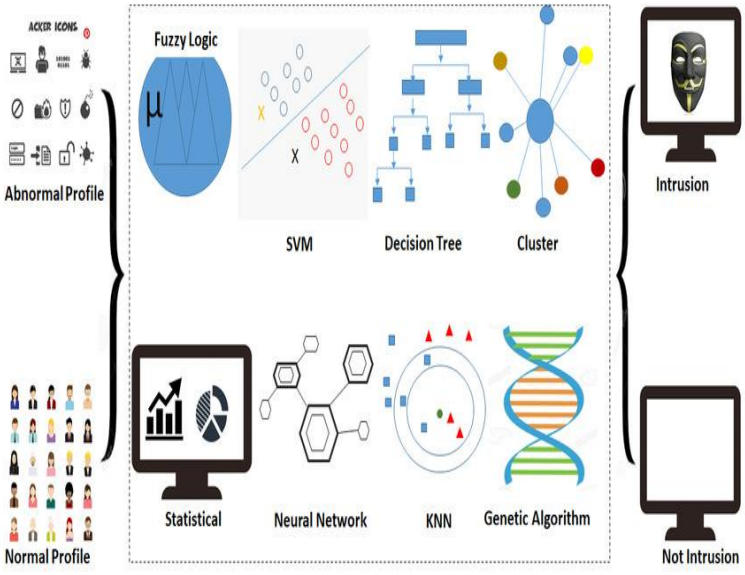
2. Scalability: The objective is to provide support for networks ranging from small to large scale, with minimal latency.

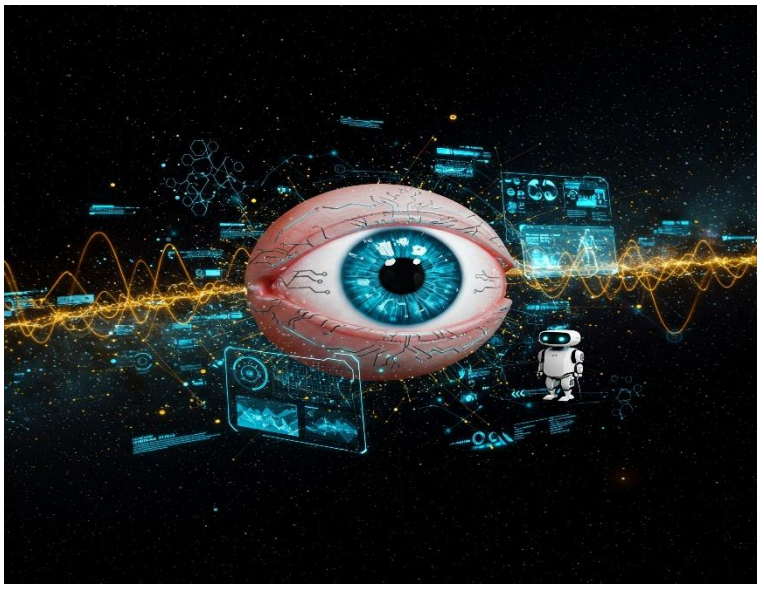
3. User Accessibility: It is imperative to furnish an accessible interface for the purpose of monitoring and managing threats.

4. Automation: The utilization of artificial intelligence (AI) has emerged as a pivotal strategy for the automation of threat detection and response processes.

5. The capacity for seamless interaction and integration among different systems and components is paramount in the field of medical informatics. The integration of cybersecurity, networking, artificial intelligence, frontend, and backend components must be seamless.

1- الكشف عن التهديدات في الوقت الحقيقي: القدرة على تحديد الاختراقات والحالات الشاذة في حركة مرور الشبكة بسرعة أمر بالغ الأهمية.
2- قابلية التوسع: الهدف هو توفير الدعم للشبكات التي تتراوح بين الصغيرة والكبيرة الحجم، مع الحد الأدنى من الوقت المستغرق.
3- إمكانية وصول المستخدم: من الضروري توفير واجهة يسهل الوصول إليها لغرض مراقبة التهديدات وإدارتها.
4- الأتمتة: برز استخدام الذكاء الاصطناعي كاستراتيجية محورية لأتمتة عمليات الكشف عن التهديدات والاستجابة لها.
5- القدرة على التفاعل السلس والتكامل بين الأنظمة والمكونات المختلفة أمر بالغ الأهمية في مجال المعلوماتية الطبية. يجب أن يكون التكامل بين مكونات الأمن السيبراني والربط الشبكي والذكاء الاصطناعي والواجهة الأمامية والخلفية سلسًا.





Domain Breakdown and Implementation:

1. Cybersecurity:

Role:

- Ensures the system is secure, protects sensitive data, and mitigates detected threats.

Implementation:

- Use encryption (e.g., AES-256) for data in transit and at rest.
- Implement secure authentication mechanisms (e.g., OAuth 2.0, JWT) for user access.
- Deploy firewalls and intrusion prevention rules to block malicious traffic.
- Regularly update the system to patch vulnerabilities

Impact:

- Cybersecurity ensures the integrity and confidentiality of the system, making it trustworthy for users and resistant to attacks.

الدور:

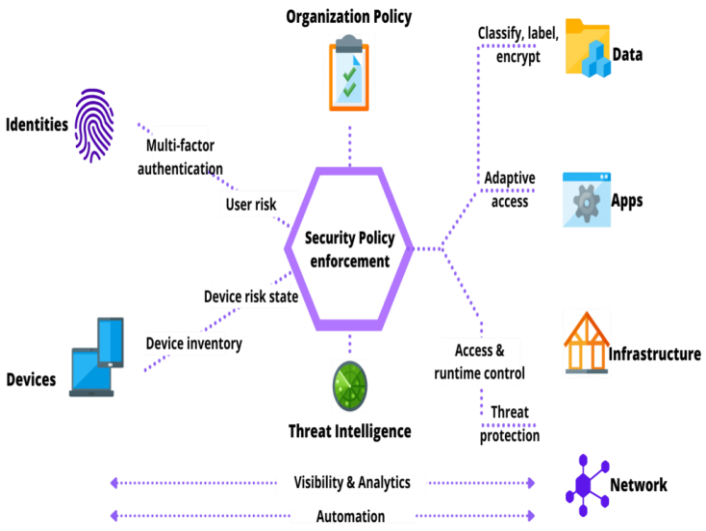
- **ضمان أمن النظام وحماية البيانات الحساسة والتخفيف من التهديدات المكتشفة.**

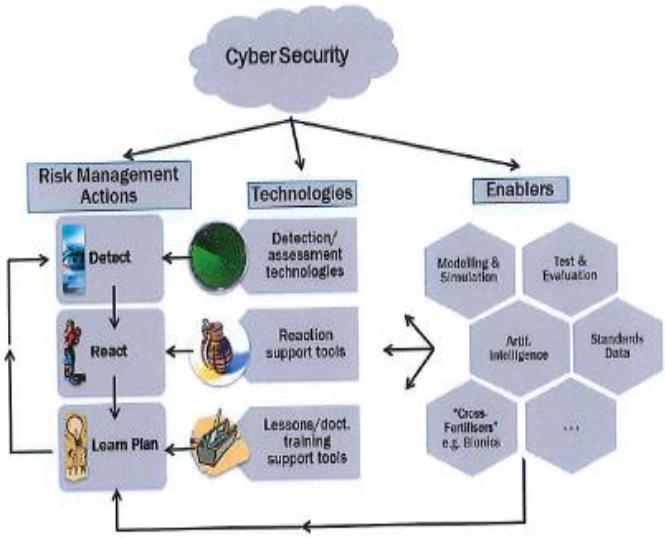
التنفيذ:

- **استخدام التشفير (على سبيل المثال، AES-256) للبيانات أثناء النقل وفي حالة السكون.**
- **تنفيذ آليات مصادقة آمنة (على سبيل المثال، OAuth 2.0، JWT) لوصول المستخدم.**
- **نشر جدران الحماية وقواعد منع التطفل لمنع حركة المرور الضارة.**
- **تحديث النظام بانتظام لتصحيح الثغرات الأمنية.**

التأثير:

- **يضمن الأمن السيبراني سلامة النظام وسريته، مما يجعله جديراً بالثقة للمستخدمين ومقاوماً للهجمات.**





2. Networking:

Role:

- Monitors and analyze network traffic to detect suspicious activities.

Implementation:

- Capture network packets using packet sniffing tools.
- Analyze traffic for patterns (e.g., unusual port activity, high data transfer rates).
- Support both wired and wireless networks with protocols like TCP/IP, UDP, and ICMP.
- Implement Quality of Service (QoS) to prioritize critical traffic during attacks.

Impact:

- Networking provides the raw data (traffic) that AI and cybersecurity components analyze, forming the foundation of intrusion detection.

الدور:

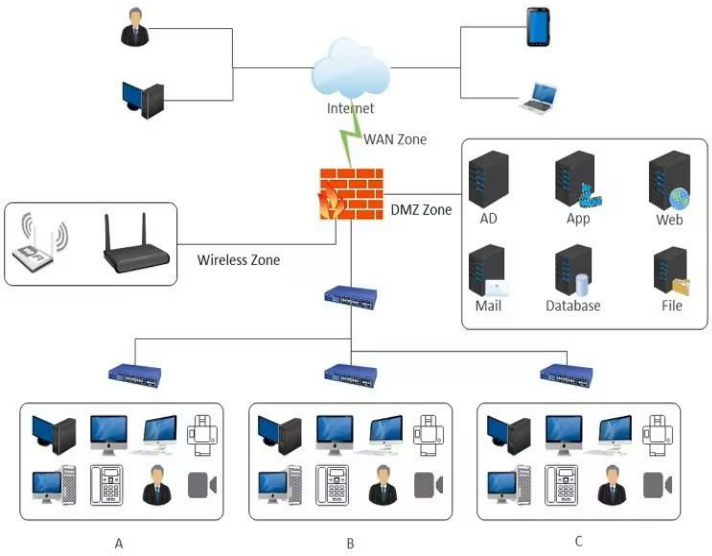
- **مراقبة وتحليل حركة مرور الشبكة للكشف عن الأنشطة المشبوهة.**

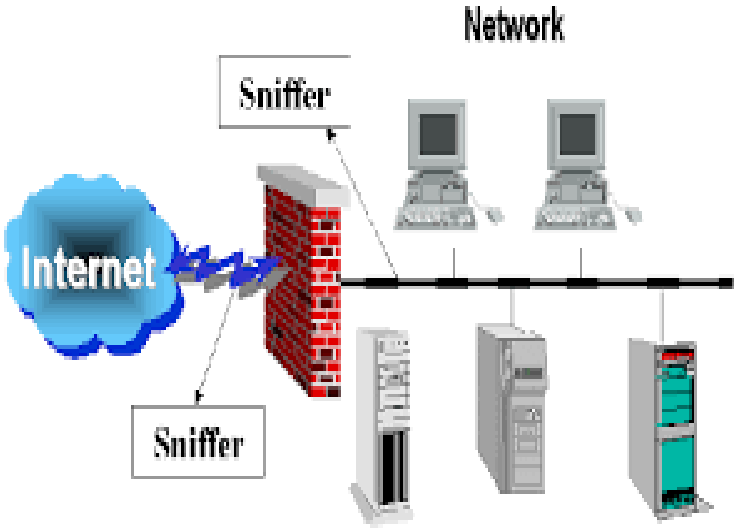
التنفيذ:

- **التقاط حزم الشبكة باستخدام أدوات استنشاق الحزم.**
- **تحليل حركة المرور بحثًا عن الأنماط (على سبيل المثال، نشاط المنفذ غير المعتاد، ومعدلات نقل البيانات العالية).**
- **دعم كل من الشبكات السلكية واللاسلكية باستخدام بروتوكولات مثل TCP/IP و UDP و ICMP.**
- **تنفيذ جودة الخدمة (QoS) لتحديد أولويات حركة المرور الحرجة أثناء الهجمات.**

التأثير:

- **توفر الشبكات البيانات الأولية (حركة المرور) التي تقوم مكونات الذكاء الاصطناعي والأمن السيبراني بتحليلها، مما يشكل أساس اكتشاف الاختراق.**





3. Artificial Intelligence (AI):

Role:

- Detects anomalies and predicts threats by analyzing network traffic patterns.

Implementation:

- Train machine learning models (e.g., Random Forest, LSTM) to identify normal vs. anomalous traffic.
- Use unsupervised learning (e.g., Autoencoders) for zero-day attack detection.
- Implement real-time inference to flag threats instantly.
- Continuously update models with new data to improve accuracy.

Impact:

- AI enhances detection accuracy and reduces false positives, enabling proactive threat mitigation.

الدور:

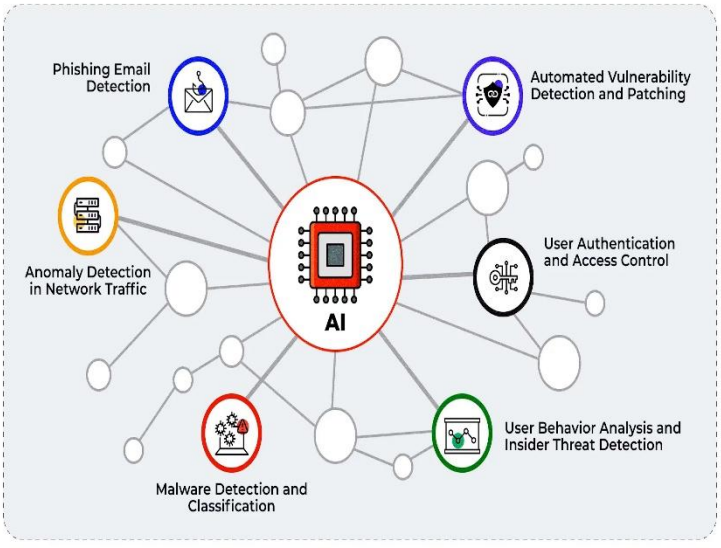
- يكتشف الحالات الشاذة ويتنبأ بالتهديدات من خلال تحليل أنماط حركة مرور الشبكة.

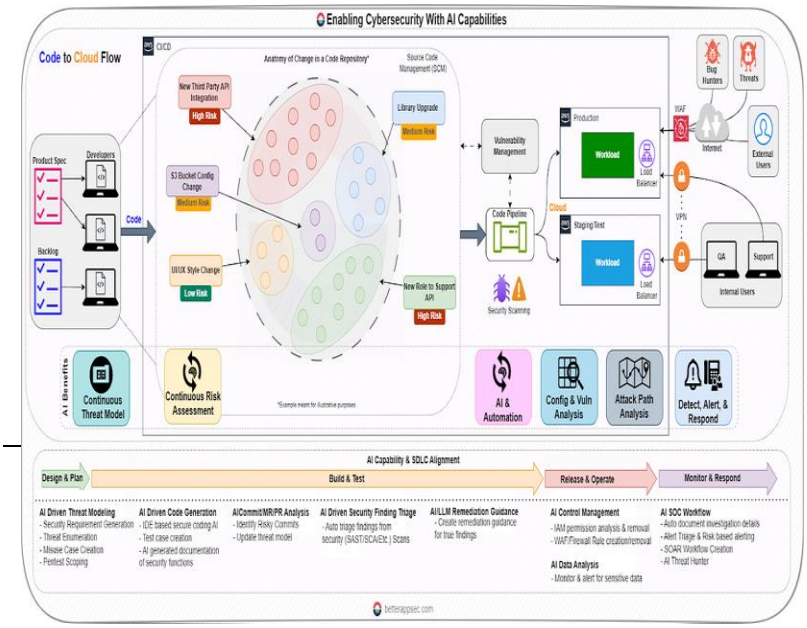
التنفيذ:

- تدريب نماذج التعلّم الآلي (على سبيل المثال: Random Forest وLSTM) لتحديد حركة المرور العادية مقابل حركة المرور الشاذة.
- استخدام التعلّم غير الخاضع للإشراف (على سبيل المثال، التشفير التلقائي) للكشف عن هجمات يوم الصفر.
- تنفيذ الاستدلال في الوقت الحقيقي للإبلاغ عن التهديدات على الفور.
- تحديث النماذج باستمرار ببيانات جديدة لتحسين الدقة.

التأثير:

- يحسّن الذكاء الاصطناعي دقة الكشف ويقلل من النتائج الإيجابية الخاطئة، مما يتيح التخفيف الاستباقي للتهديدات.





4. Front-End:

Role:

- Provides a user-friendly interface for monitoring threats and managing the system.

Implementation:

- Develop a web-based dashboard to visualize network traffic, alerts, and system status.
- Display real-time charts (e.g., traffic volume, threat frequency) using data visualization libraries.
- Allow users to configure detection rules, view logs, and respond to alerts (e.g., block IP addresses).
- Ensure responsiveness for desktop and mobile devices.

Impact:

- The frontend makes the system accessible and actionable, bridging technical data with user interaction.

الدور:

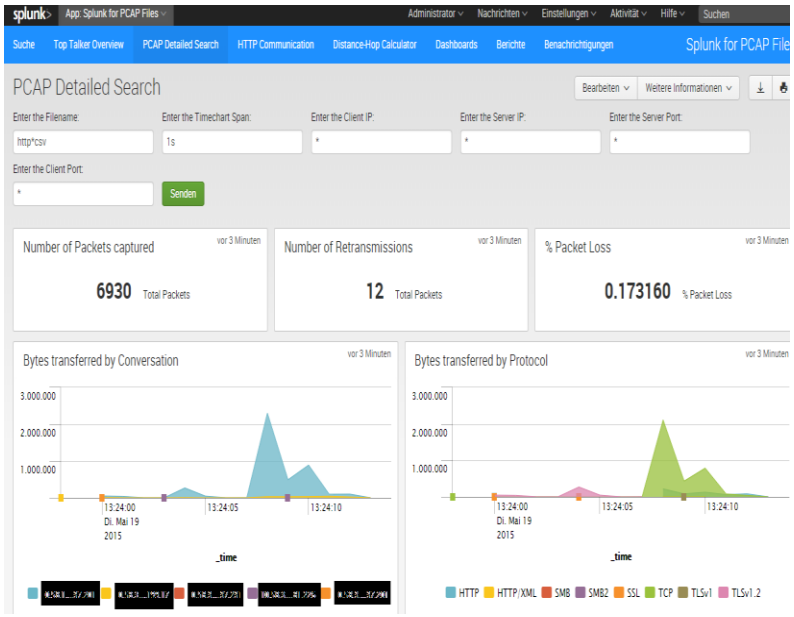
- **يوفر واجهة سهلة الاستخدام لمراقبة التهديدات وإدارة النظام.**

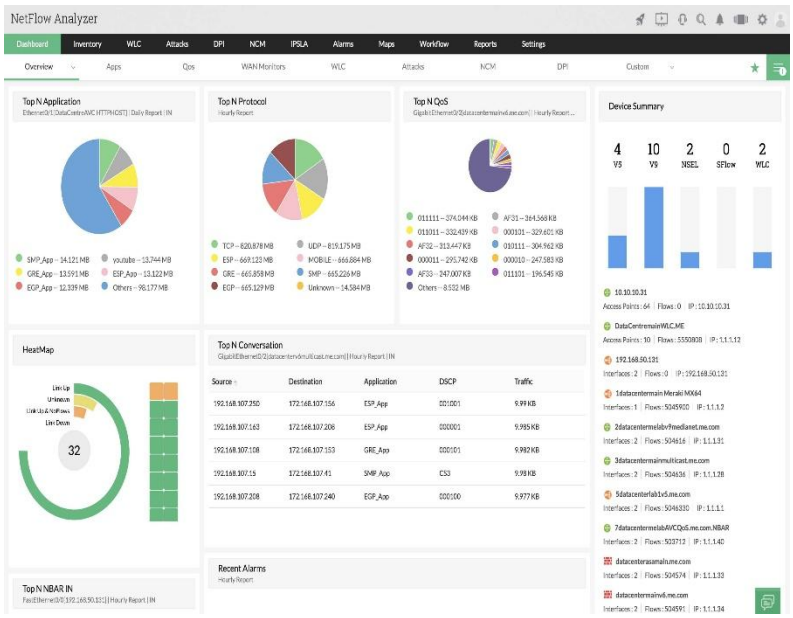
التنفيذ:

- **تطوير لوحة معلومات على شبكة الإنترنت لتصور حركة مرور الشبكة والتنبيهات وحالة النظام.**
- **عرض الرسوم البيانية في الوقت الحقيقي (على سبيل المثال، حجم حركة المرور، وتكرار التهديدات) باستخدام مكتبات تصور البيانات.**
- **السماح للمستخدمين بتكوين قواعد الكشف وعرض السجلات والاستجابة للتنبيهات (على سبيل المثال، حظر عناوين IP).**
- **ضمان الاستجابة لأجهزة سطح المكتب والأجهزة المحمولة.**

التأثير:

- **تتيح الواجهة الأمامية إمكانية الوصول إلى النظام وقابليته للتنفيذ، وتربط البيانات التقنية بتفاعل المستخدم.**





5. Back-End:

Role:

- Processes network data, integrates AI models, and serves data to the frontend.

Implementation:

- Build a RESTful API to handle requests from the frontend (e.g., fetching alerts, updating rules).
- Store network logs and threat data in a database for analysis and auditing.
- Integrate AI models to process incoming network data and generate alerts.
- Ensure high availability and scalability using microservices architecture.

Impact:

- The backend ensures seamless communication between components, enabling real-time processing and storage.

الدور:

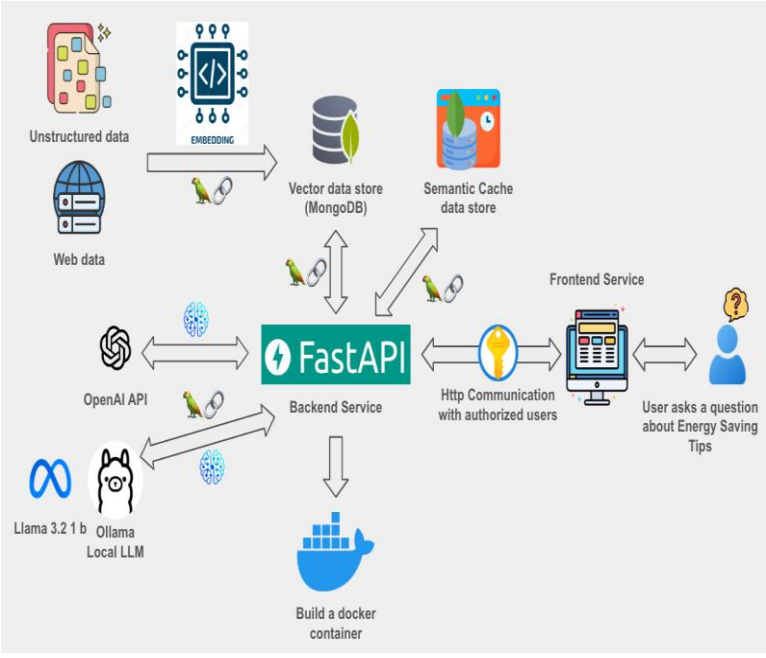
- معالجة بيانات الشبكة ودمج نماذج الذكاء الاصطناعي وتقديم البيانات إلى الواجهة الأمامية.

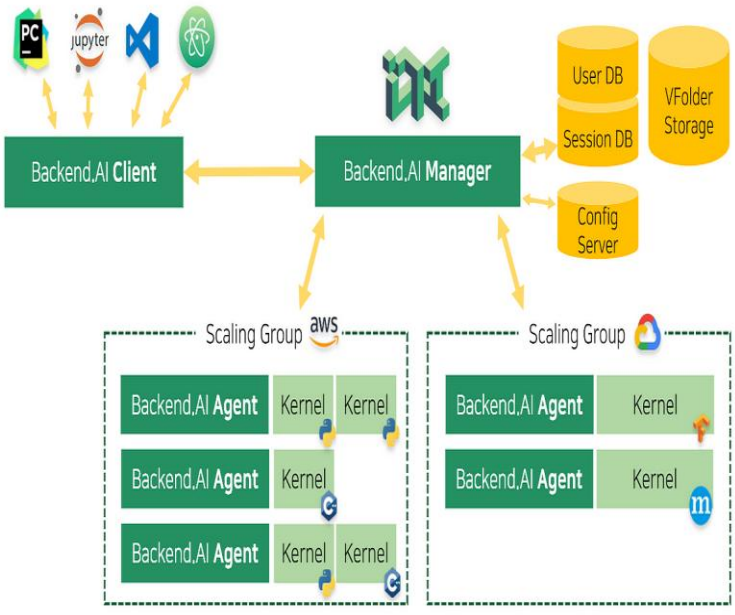
التنفيذ:

- إنشاء واجهة برمجة تطبيقات RESTful API للتعامل مع الطلبات من الواجهة الأمامية (على سبيل المثال، جلب التنبيهات وتحديث القواعد).
- تخزين سجلات الشبكة وبيانات التهديدات في قاعدة بيانات للتحليل والتدقيق.
- دمج نماذج الذكاء الاصطناعي لمعالجة بيانات الشبكة الواردة وإنشاء التنبيهات.
- ضمان التوافر العالي وقابلية التوسع باستخدام بنية الخدمات المصغرة.

التأثير:

- تضمن الواجهة الخلفية التواصل السلس بين المكونات، مما يتيح المعالجة والتخزين في الوقت الفعلي.





The domains work together to create a cohesive system:

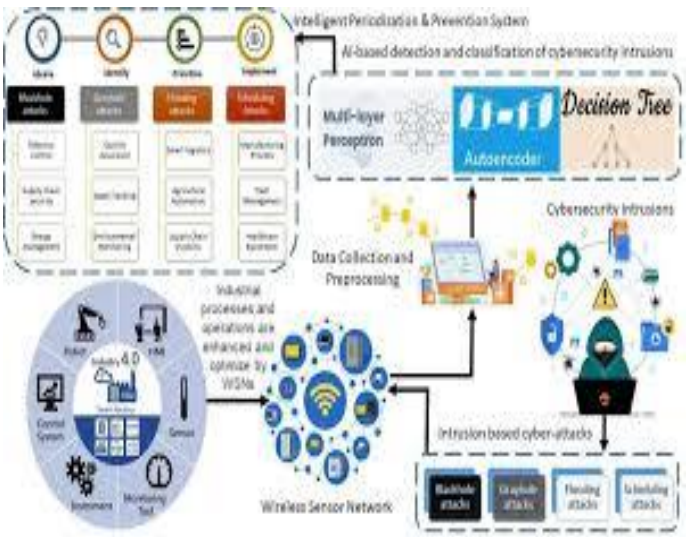
- **Cybersecurity + Networking: Cybersecurity secures the network infrastructure, while networking provides the data needed to detect intrusions.**
- **Networking + AI: Networking supplies raw traffic data, which AI analyzes to identify anomalies and predict threats.**
- **AI + Backend: The backend integrates AI models, feeding them data and storing their output (e.g., alerts, predictions).**
- **Backend + Frontend: The backend processes data and serves it to the front end, which visualizes it for users.**
- **Frontend + Cybersecurity: The frontend incorporates secure authentication and displays cybersecurity alerts, ensuring user trust.**
- **AI + Frontend: AI-generated insights (e.g., threat scores) are visualized on the frontend, making complex data understandable.**

This synergy ensures that SIDS is secure, efficient, and user-centric, with each domain enhancing the others' capabilities.

تعمل النطاقات معًا لإنشاء نظام متماسك:

- **الأمن السيبراني + الشبكات: يؤمن الأمن السيبراني البنية التحتية للشبكة، بينما توفر الشبكات البيانات اللازمة لاكتشاف الاختراقات.**
- **الشبكات + الذكاء الاصطناعي: توفر الشبكات بيانات حركة المرور الأولية، والتي يقوم الذكاء الاصطناعي بتحليلها لتحديد الحالات الشاذة والتنبؤ بالتهديدات.**
- **الذكاء الاصطناعي + الواجهة الخلفية: تقوم الواجهة الخلفية بدمج نماذج الذكاء الاصطناعي وتغذيتها بالبيانات وتخزين مخرجاتها (مثل التنبيهات والتنبؤات).**
- **الواجهة الخلفية + الواجهة الأمامية: تعالج الواجهة الخلفية البيانات وتقدمها إلى الواجهة الأمامية التي تعرضها للمستخدمين.**
- **الواجهة الأمامية + الأمن السيبراني: تتضمن الواجهة الأمامية مصادقة آمنة وتعرض تنبيهات الأمن السيبراني، مما يضمن ثقة المستخدم.**
- **الذكاء الاصطناعي + الواجهة الأمامية: يتم عرض الرؤى الناتجة عن الذكاء الاصطناعي (مثل نتائج التهديدات) على الواجهة الأمامية، مما يجعل البيانات المعقدة مفهومة.**

ويضمن هذا التآزر أن تكون SIDS آمنة وفعالة ومتمحورة حول المستخدم، حيث يعمل كل مجال على تعزيز قدرات المجالات الأخرى.



Useful Resources & Recommended Links:

1. Cybersecurity & IDS Concepts:

- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
- **Network-based Intrusion Prevention System for Android**
- **Network-based Intrusion Detection System for Android**
- **Using Sysmon to monitor and detect the malicious processes behavior**
- **Detecting malicious scripts using AMSI**
- **Anti Ransomware**
- **MITRE ATT&CK Framework**

LINKS:

- **LINK:** Click here
- **LINK:** Click here
- **LINK:** Click here
- **LINK:** Click here
- **LINK:** Click here
- **LINK:** Click here
- **LINK:** Click here
- **LINK:** Click here
- **LINK:** Click here
- **LINK:** Click here
- **LINK:** Click here
- **LINK:** Click here
- **LINK:** Click here

2. AI & Machine Learning for Security:

- **How ai/ml techniques help to solve network**
- **AI/ML Methods to Diagnose Network Issues Using Telemetry Data**
  - **LINK:** Click here
  - **LINK:** Click here
  - **LINK:** Click here

3. Networking & System Administration:

- **AI-Assisted Network Monitoring: Real or Hype?**
  - **LINK:** Click here
- **Designing AI for Network Troubleshooting**
  - **LINK:** Click here
- **Network Traffic Anomaly Detection Using Machine Learning**
  - **LINK:** Click here
  - **LINK:** Click here
- **Predicting Network Behavior Using Machine Learning AI**
  - **LINK:** Click here
- **Cisco AI and ML Overview**
  - **LINK:** Click here
  - **LINK:** Click here
- **Network Watcher Flow Logs**
  - **LINK:** Click here
- **AI/ML for networks | Codi Lime**
  - **LINK:** Click here
  - **LINK:** Click here
  - **LINK:** Click here
- **ManageEngine: LINK:** Click here

Conclusion:

The Smart Intrusion Detection System (SIDS) integrates a suite of technologies, including cybersecurity, networking, artificial intelligence, frontend, and backend components, to formulate a robust, user-friendly, and scalable solution for network security. By leveraging the strengths of each domain and ensuring their seamless integration, SIDS provides real-time threat detection, automated responses, and an intuitive interface for users. This documentation serves as a foundational framework for the construction and exposition of the project, thereby elucidating its conceptual underpinnings and inherent value to any audience.

يدمج نظام الكشف عن التطفل الذكي (SIDS) مجموعة من التقنيات، بما في ذلك الأمن السيبراني والشبكات والذكاء الاصطناعي والواجهة الأمامية ومكونات الواجهة الخلفية، لصياغة حل قوي وسهل الاستخدام وقابل للتطوير لأمن الشبكات. من خلال الاستفادة من نقاط القوة في كل مجال وضمان تكاملها بسلاسة، توفر SIDS الكشف عن التهديدات في الوقت الحقيقي، والاستجابات الآلية، وواجهة سهلة الاستخدام للمستخدمين. تُعد هذه الوثائق بمثابة إطار عمل تأسيسي لبناء المشروع وعرضه، وبالتالي توضيح أسسه المفاهيمية وقيمته الكامنة لأي جمهور.