



الذكاء الاصطناعي وتحسين الأمن السيبراني للمنظمات: دراسة حالة شركة مايكروسوفت *Artificial Intelligence and Enhancing Cybersecurity for Organizations: A Case Study of Microsoft*

صحراوي بن شبيحة

بن أحمد فاطمة الزهراء*

إدارة الابتكار والتسويق، جامعة جبالتي ليايس سيدي

إدارة الابتكار والتسويق، جامعة أبي بكر بلقايد تلمسان،

بلعباس، الجزائر

الجزائر

sbenchiha@yahoo.fr

benahmed.fatimazahra@univ-tlemcen.dz

تاريخ النشر: 2025/04/27

تاريخ القبول: 2025/03/25

تاريخ الإرسال: 2025/02/05

ملخص:

يهدف هذا البحث إلى تحليل تأثير الذكاء الاصطناعي على تحسين الأمن السيبراني للمنظمات، مع دراسة حالة شركة مايكروسوفت كنموذج تطبيقي. يركز البحث على دور تقنيات الذكاء الاصطناعي في الكشف المبكر عن التهديدات السيبرانية ومنعها، مع استعراض التحديات المرتبطة باستخدام هذه التقنيات، مثل تأمين البيانات المستخدمة في تدريب النماذج ومواجهة الهجمات المضادة، كما يقدم البحث توصيات للشركات حول كيفية تبني حلول الذكاء الاصطناعي لتعزيز الحماية السيبرانية. أظهرت النتائج أن الذكاء الاصطناعي يمثل أداة فعالة لتحسين الأمن السيبراني، حيث ساهمت تقنيات مثل *Microsoft Defender* و *Azure Sentinel* في تقليل زمن الاستجابة للهجمات وزيادة كفاءة الأنظمة الأمنية ومع ذلك، أكدت الدراسة على أهمية التكامل بين الذكاء الاصطناعي والخبرة البشرية لتحقيق مستويات أمان أعلى، مما يعزز من قدرة المنظمات على مواجهة التهديدات المتزايدة تعقيدا بشكل فعال ومستدام.

الكلمات المفتاحية: الذكاء الاصطناعي، الأمن السيبراني، الهجمات السيبرانية، مايكروسوفت، الهجمات.

Abstract :

This research aims to analyze the impact of artificial intelligence (AI) on improving cybersecurity for organizations, with a case study focusing on Microsoft as an applied model. The study examines the role of AI technologies in the early detection and prevention of cyber threats, while highlighting the challenges associated with these technologies, such as securing data used for training models and addressing adversarial attacks. Additionally, the research provides recommendations for companies on adopting AI solutions to enhance cybersecurity measures. The findings indicate that AI is an effective tool for improving cybersecurity, as technologies like Microsoft Defender and Azure Sentinel have significantly reduced response times to cyberattacks and increased the efficiency of security systems. However, the study emphasizes the importance of integrating AI with human expertise to achieve higher levels of security, thereby strengthening organizations' ability to effectively and sustainably address increasingly complex cyber threats.

Key Words: Artificial Intelligence; Cybersecurity ; Cyberattacks; Microsoft; attacks

JEL Classification: O33; L86; D83

*مرسل المقال: بن أحمد فاطمة الزهراء (benahmed.fatimazahra@univ-tlemcen.dz)



المقدمة:

الأمن السيبراني يمثل مجموعة من الأدوات والإجراءات والممارسات المصممة لحماية الشبكات والأجهزة والبرمجيات والبيانات من الهجمات الإلكترونية والأضرار والوصول غير المصرح به ومع التوسع الكبير في استخدام الأنظمة والشبكات المترابطة، أصبح تحقيق الأمن السيبراني تحدياً متزايداً. يساهم التطور التكنولوجي المتسارع في الاقتصاد الرقمي والبنية التحتية في تعقيد هذا التحدي، مما أدى إلى زيادة ملحوظة في الهجمات السيبرانية ذات العواقب الخطيرة، وتشير الدراسات إلى أن أساليب المهاجمين تطورت بشكل ملحوظ، حيث يتم دعمهم أحياناً من قبل دول قومية أو منظمات إجرامية، مع اعتمادهم على تقنيات مبتكرة لاختراق الأنظمة الأكثر تطوراً.

في ظل هذه التحديات، أصبح من الضروري تبني نهج أمني سيبراني يعتمد على الذكاء الاصطناعي للتعامل مع البيانات الضخمة وتوفير دفاع ديناميكي أمام الهجمات الناشئة، يتيح هذا النهج استخدام التقييمات في الوقت الفعلي والمراقبة المستمرة والتحليل القائم على البيانات لاكتشاف الهجمات والاستجابة لها بفعالية، مما يقلل من مخاطر الحوادث المستقبلية، كما توصي جهات استشارية مثل المعهد الوطني للمعايير والتقنيات (NIST) باعتماد أساليب استباقية وتكيفية لتحقيق مستويات أمان أعلى في سياق الثورة الصناعية الرابعة، يمثل الذكاء الاصطناعي تحولاً نوعياً بفضل تطبيقاته المتعددة في الاقتصاد والصناعة والخدمات والقطاعات العسكرية والسياسية، كما يلعب دوراً محورياً في تعزيز الأمن السيبراني، حيث يستخدم لتحسين مستويات الحماية السيبرانية في مختلف الدول، مما يعكس تأثيره المباشر على الأفراد والمجتمعات.

الاشكالية: في ظل التطور التكنولوجي المتسارع، أصبح الذكاء الاصطناعي أداة محورية في تعزيز الأمن السيبراني، حيث يساهم بشكل كبير في تحسين قدرات الكشف عن التهديدات والاستجابة لها ومع ذلك، فإن التوسع المتزايد في استخدام تقنيات الذكاء الاصطناعي في هذا المجال يثير العديد من التساؤلات البحثية، بناءً على ذلك تبرز الإشكالية الرئيسية لهذه الدراسة في السؤال التالي: **ما مدى فعالية تطبيقات الذكاء الاصطناعي في تعزيز الأمن السيبراني للمنظمات، وما هي الآثار المترتبة على هذا التكامل في ضوء تجربة شركة مايكروسوفت؟**

الفرضيات:

- تساهم تطبيقات الذكاء الاصطناعي بشكل فعال في تحسين قدرات الكشف عن التهديدات السيبرانية وسرعة الاستجابة لها في المنظمات، مما يؤدي إلى تعزيز الأمن السيبراني بشكل ملحوظ.
- يؤدي تكامل الذكاء الاصطناعي مع أنظمة الأمن السيبراني التقليدية إلى تحديات تقنية وأخلاقية جديدة، تتطلب تطوير استراتيجيات متكاملة لضمان فعالية الحماية وتقليل المخاطر المحتملة.

أهداف البحث:

- تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف الرئيسية التي تتعلق بالعلاقة بين الذكاء الاصطناعي والأمن السيبراني، مع التركيز على المجالات التالية :
- تحليل العلاقة المتبادلة بين الذكاء الاصطناعي والأمن السيبراني باعتبارهما مجالين مترابطين ومتطورين باستمرار.



-دراسة نقاط القوة والضعف في الأنظمة الأمنية الحالية بهدف تطوير حلول مبتكرة وأكثر كفاءة لمواجهة التهديدات السيبرانية.

-استعراض الأدوات والتقنيات التي تعتمد عليها شركة مايكروسوفت في تعزيز أمنها السيبراني، بما في ذلك استراتيجياتها القائمة على الذكاء الاصطناعي.

-تقديم توصيات للشركات والمؤسسات حول كيفية تبني تقنيات الذكاء الاصطناعي المتقدمة لتحسين أمنها السيبراني بشكل عام، مع التركيز على حالة شركة مايكروسوفت كنموذج تطبيقي.

منهجية البحث:

للإجابة على الإشكالية المطروحة أعلاه، تم اعتماد منهجية تجمع بين المنهج الوصفي والمنهج التحليلي، حيث تم استخدام المنهج الوصفي في المحورين الأول والثاني لتقديم الإطار النظري للدراسة من خلال استعراض المفاهيم المتعلقة بالذكاء الاصطناعي والأمن السيبراني، أما في المحور الثالث فقد تم توظيف المنهج التحليلي لدراسة الجانب التطبيقي، وذلك من خلال تحليل دور الذكاء الاصطناعي في تحسين الأمن السيبراني مع التركيز على حالة شركة مايكروسوفت كنموذج عملي.

I. الذكاء الاصطناعي: المفهوم والتطبيقات:

1. نشأة الذكاء الاصطناعي:

قد يعتقد البعض أن مصطلح الذكاء الاصطناعي حديث النشأة، إلا أن جذوره تعود إلى منتصف القرن العشرين. فقد صاغ الباحث جون مكارثي هذا المصطلح لأول مرة في عام 1956، حيث ركزت أبحاث العلماء آنذاك على كيفية منح الآلة قدرات مشابهة للذكاء البشري. كانت أول محاولة لبناء آلة ذكية قادرة على تقليد العقل البشري من قبل العالم فرانك روزنبلات في عام 1957. وفي وقت لاحق، قام البروفيسور كيفن وارويك من جامعة ريدينغ البريطانية في عام 1998 بدراسة تفاعل الحاسوب مع الجهاز العصبي للإنسان. شهدت أبحاث الذكاء الاصطناعي تطوراً ملحوظاً خلال منتصف القرن العشرين، مما ساهم في تقدم علم التحكم في الآلة وتوسيع نطاق استخدام الذكاء الاصطناعي في مجالات متعددة. (نزمين، 2020)

1.1 تعريف الذكاء الاصطناعي: (محمد ، 2023)

-يعرف هيربرت سيمون الذكاء الاصطناعي باعتباره مجالا يرتبط بعلم النفس والعلوم المعرفية وغيرها من العلوم التي تهدف إلى تمكين أجهزة الكمبيوتر من أداء المهام بكفاءة، مع محاكاة القدرات البشرية وجعلها قادرة على التفكير بذكاء.

-من جهة أخرى، يعرف كل من ريتش وكينج الذكاء الاصطناعي على أنه دراسة تعنى بكيفية تمكين أجهزة الكمبيوتر من أداء المهام بشكل يفوق كفاءة البشر.



أما بشكل عام، فإن الذكاء الاصطناعي يعد مجالا علميا ومعرفيا يتم فيه دمج المعرفة بطريقة منطقية في أنظمة الكمبيوتر، حيث تنظم هذه المعرفة وفق خوارزميات محددة تستخدم لمعالجة المشكلات التي تتطلب مستوى عالي من الذكاء. (حسن بن محمد، 2021)

2.1 مستويات الذكاء الاصطناعي:

يمكن تصنيف الذكاء الاصطناعي إلى ثلاثة مستويات رئيسية بناء على قدراته ووظائفه. يوضح الشكل أدناه هذه المستويات:

لتوضيح مستويات الذكاء الاصطناعي، يمكن استخدام الشكل التالي الذي يعرض التصنيفات الثلاثة الرئيسية بناء على القدرات والوظائف:

الشكل رقم 01: مستويات الذكاء الاصطناعي

المستوى	نوع المهام	الأمثلة
1. الذكاء الاصطناعي الضيق (ANI)	يركز على أداء مهام محددة بدقة عالية دون القدرة على التفكير أو التكيف مع مهام أخرى.	التعرف على الصور، المساعدات الصوتية مثل Siri و Alexa، السيارات ذاتية القيادة.
2. الذكاء الاصطناعي العام (AGI)	يحاكي الذكاء البشري، قادر على التفكير واتخاذ القرارات في مختلف المجالات، لكنه لم يتحقق بعد.	لا توجد أمثلة عملية حتى الآن، لكن يُعتبر هدفاً مستقبلياً للبحث والتطوير.
3. الذكاء الاصطناعي الفائق (ASI)	يتجاوز الذكاء البشري في جميع المجالات، بما في ذلك الإبداع وحل المشكلات واتخاذ القرارات، ويُعتبر مفهومًا نظريًا حاليًا.	لا يزال في نطاق الخيال العلمي ولم يتم تحقيقه بعد.

المصدر: من اعداد الباحثين بالاعتماد على المرجع: (SDAIA، 2022)

هذا الجدول يساعد في فهم الفروقات بين الأنواع المختلفة للذكاء الاصطناعي ويبرز تطور التكنولوجيا من الأنظمة البسيطة إلى المفاهيم المستقبلية الأكثر تقدماً.

3.1 خصائص تطبيقات الذكاء الاصطناعي:

تتميز تطبيقات الذكاء الاصطناعي بمجموعة من الخصائص التي تجعلها ذات أهمية كبيرة في مختلف المجالات، ويمكن تلخيص أبرز هذه الخصائص كما يلي: (اسماء السيد و كريمة، 2020)

– **تحليل المشكلات واتخاذ القرارات:** تُمكن تقنيات الذكاء الاصطناعي الأجهزة والآلات من تحليل المشكلات باستخدام المنطق، مما يتيح لها التعرف على الأصوات والكلام، بالإضافة إلى القدرة على تحريك الأشياء وتنفيذ المهام بكفاءة عالية.

– **فهم المدخلات وتقديم مخرجات دقيقة:** تُظهر الأجهزة التي تعتمد على الذكاء الاصطناعي قدرة على فهم وتحليل المدخلات لتوفير مخرجات تلبي احتياجات المستخدمين بدقة وكفاءة، مما يعزز تجربة الاستخدام



- التعلم المستمر والذاتي:** يتميز الذكاء الاصطناعي بقدرته على التعلم الآلي والذاتي دون الحاجة إلى مراقبة أو إشراف بشري مستمر، مما يسمح له بالتكيف مع البيانات الجديدة وتحسين أدائه بمرور الوقت.
- معالجة كميات هائلة من البيانات:** يمتلك الذكاء الاصطناعي القدرة على التعامل مع كم هائل من المعلومات، مما يساعد في تحليل الأنماط واستخلاص النتائج بسرعة تفوق القدرات البشرية.
- إيجاد حلول مبتكرة للمشكلات:** باستخدام قدراته المعرفية المتقدمة، يستطيع الذكاء الاصطناعي تقديم حلول غير مألوفة للمشكلات المعقدة، وهو ما يجعله أداة فعالة في الابتكار والإبداع.
- التطبيقات متعددة المجالات:** يشمل استخدام الذكاء الاصطناعي مجالات متنوعة مثل التعليم، الطب، النقل، الزراعة، وخدمة العملاء، حيث يساهم في تحسين الكفاءة وتقليل الأخطاء البشرية.

2. الأمن السيبراني: دراسة مفاهيمية

1.2 تعرف الأمن السيبراني:

- يمكن تعريف الأمن السيبراني بأنه مجموعة من التدابير والتقنيات والسياسات المصممة لحماية الأنظمة والشبكات والأجهزة والبيانات من الهجمات الرقمية أو الوصول غير المصرح به، اد يهدف الأمن السيبراني إلى ضمان سرية وسلامة وتوافر المعلومات والأنظمة الحساسة، سواء كانت شخصية أو مالية أو حكومية، مع تقليل المخاطر المرتبطة بالتهديدات الإلكترونية مثل القرصنة أو الفيروسات أو التلاعب بالبيانات.
- عرف **العتيبي** الأمن السيبراني بأنه الحماية الموجهة لشبكات الاتصالات وأنظمة المعلومات والأجهزة المتصلة بالإنترنت، مع التركيز على التدابير الوقائية للحد من الانتهاكات والوصول غير المصرح به. (العتيبي، 2020)
- يعرف **Richard A. Kemmerer** **الأمن السيبراني** بأنه "إجراءات لتقليل مخاطر الهجمات على البرامج أو أجهزة الكمبيوتر أو عناصر التحكم، بما في ذلك الوسائل والأدوات المستخدمة" (لامية، 2020)
- من خلال تحليل مختلف التعريفات، يمكن استنتاج أن الأمن السيبراني يشمل حماية الأنظمة الحاسوبية والشبكات والبيانات الإلكترونية من التهديدات السيبرانية. كما يتضمن حماية المعلومات الحساسة وتأمين الأجهزة والتطبيقات من التطفل أو التلاعب أو التدمير، مع التركيز على بناء بيئة رقمية آمنة للأفراد والمؤسسات والحكومات.

2.2 مكعب الأمن السيبراني: (اسامة، 2017)

- يعد مكعب الأمن السيبراني، الذي ابتكره جون ماكومبر (John McCumber)، إطاراً عاماً يستخدم كأداة فعالة لإدارة نظم الحماية في الشبكات، النطاقات، أو الإنترنت بشكل عام يهدف هذا المكعب إلى توفير رؤية شاملة لفهم وتطبيق استراتيجيات الأمن السيبراني من خلال دمج مبادئ حماية المعلومات مع حالات البيانات والخبرات اللازمة لتأمينها. (اسامة، 2017)
- يعد مكعب الأمن السيبراني نموذجاً شاملاً يهدف إلى توضيح الأبعاد الأساسية لحماية الفضاء السيبراني. يتكون هذا المكعب من ثلاثة أبعاد رئيسية، وهي كما يلي :



البعد الأول: مبادئ أمن المعلومات

يحدد البعد الأول الأهداف الأساسية لحماية الفضاء السيبراني، والتي تعرف بمبادئ أمن المعلومات وتشمل هذه المبادئ الثلاثة :

- **السرية (Confidentiality):** ضمان حماية البيانات من الوصول غير المصرح به.
 - **السلامة أو التماسك (Integrity):** الحفاظ على دقة البيانات ومنع التلاعب بها.
 - **التوافر (Availability):** التأكد من أن البيانات والأنظمة متاحة عند الحاجة.
- تعد هذه المبادئ أساسية لزيادة وعي متخصصي الأمن السيبراني، حيث تساعد على ترتيب أولوياتهم وتحديد ردود الفعل المناسبة عند حماية الأنظمة الشبكية .

البعد الثاني: حالة البيانات

يركز البعد الثاني على حماية البيانات في مختلف حالاتها داخل الفضاء السيبراني، حيث يحتوي هذا الفضاء على كميات كبيرة من البيانات الحساسة والحيوية. ويعنى هذا البعد بحماية البيانات في الحالات التالية :

- ✓ **البيانات أثناء النقل (Data in Transit):** البيانات التي تنتقل عبر الشبكات.
- ✓ **البيانات أثناء التخزين (Data at Rest):** البيانات المخزنة بشكل ثابت.
- ✓ **البيانات أثناء المعالجة (Data in Processing):** البيانات التي يتم معالجتها أو استخدامها في الوقت الفعلي.

البعد الثالث: حراسة الأمن السيبراني

يركز البعد الثالث على المهارات والضوابط اللازمة لحماية الفضاء السيبراني. ويحدد هذا البعد الأدوات والإرشادات التي يمكن لمختصين الأمن السيبراني استخدامها لضمان أمان البيانات والأنظمة. تشمل هذه الضوابط السياسات والإجراءات التقنية والتنظيمية التي تُساعد في التصدي للتهديدات المختلفة وحماية المعلومات بشكل فعال .

تظهر هذه الأبعاد الثلاثة التكامل بين المبادئ الأساسية، حالات البيانات، والمهارات المطلوبة لتوفير حماية شاملة للفضاء السيبراني إذ يركز مكعب الأمن السيبراني على تحديد المهارات والضوابط اللازمة لتوفير حماية شاملة للفضاء السيبراني ومن بين هذه المهارات الأساسية، يأتي استخدام التكنولوجيا والأجهزة والمنتجات المتاحة كأداة رئيسية لحماية نظم المعلومات وردع مجرمي الفضاء السيبراني إذ يعرف محترفو الأمن السيبراني بقدرتهم العالية على توظيف التكنولوجيا الحديثة والأدوات المتطورة لتحقيق أهداف الحماية، ومع ذلك يشير ماكومير إلى أن الاعتماد على الأدوات والتقنيات الحديثة وحدها لا يكفي لضمان حماية فعالة بل يلزم بناء دفاع قوي يشمل وضع سياسات وإجراءات وإرشادات واضحة تساعد المستخدمين في الفضاء السيبراني على الحفاظ على أمانهم، هذه الإجراءات التنظيمية تعتبر عنصرا أساسيا لتعزيز الحماية ضد التهديدات الإلكترونية، بالإضافة إلى ذلك يجب أن يسعى المستخدمون في الفضاء السيبراني إلى تعزيز معرفتهم بالتهديدات المحتملة من خلال إنشاء ثقافة تعليمية وتوعوية مستمرة، التوعية بالتهديدات السيبرانية تعد جزءا لا يتجزأ من بناء بيئة آمنة للمستخدمين، وفي الأخير يوصى



بتحسين مستوى الأمن السيبراني من خلال الاستفادة من الذكاء الاصطناعي، الذي سيتم التطرق إليه في المحور التالي حيث يمكن أن يسهم بشكل كبير في تعزيز استراتيجيات الحماية وتطوير الدفاعات ضد الهجمات السيبرانية.

3. دور الذكاء الاصطناعي في تحسين الأمن السيبراني حالة شركة مايكروسوفت:

1.3 تطبيقات الذكاء الاصطناعي المستخدمة في تحسين الأمن السيبراني

يستخدم الذكاء الاصطناعي بشكل متزايد لتعزيز الأمن السيبراني من خلال تطبيقات متعددة تهدف إلى تحسين كفاءة الحماية والاستجابة للتهديدات السيبرانية. وفيما يلي أبرز التطبيقات التي يسهم فيها الذكاء الاصطناعي : (صفاء وآخرون، 2023)

يمثل الذكاء الاصطناعي أداة فعالة في تعزيز الأمن السيبراني، حيث يساعد في معالجة البيانات الضخمة الناتجة عن الأنشطة اليومية من خلال مراقبة حركة المرور وتحليل النشاط بدقة لتحديد المخاطر المحتملة تلقائياً، كما يتميز بقدرته على التنبؤ بالتهديدات المستقبلية عبر معالجة كميات هائلة من البيانات مما يتيح الكشف المبكر عن الأنشطة الضارة واتخاذ إجراءات وقائية تقلل من الوقت والموارد البشرية المطلوبة، إضافة إلى ذلك يساهم الذكاء الاصطناعي في تسريع اكتشاف التهديدات وهو أمر بالغ الأهمية للمؤسسات التي تواجه ضغوطاً متزايدة بسبب التهديدات الحساسة للوقت كما يقلل من تكاليف الأمن السيبراني بنسبة تصل إلى 80%، حيث أظهرت الأدوات المعتمدة عليه، مثل ChatGPT ، دوراً بارزاً في تحسين الإنتاجية وتدريب الموظفين وتعزيز الحماية. مع تطور هذه التقنيات، ستتمكن المؤسسات من تحقيق حماية أكثر كفاءة واستباقية ضد الهجمات السيبرانية المتزايدة تعقيداً.

2.3 علاقة الذكاء الاصطناعي بالأمن السيبراني

هناك علاقة وثيقة بين الذكاء الاصطناعي والأمن الإلكتروني أو السيبراني، إذ يتم تطوير أنظمة الذكاء الاصطناعي التي يمكن استخدامها لتعزيز الأمن السيبراني، إلى جانب تنفيذ تدابير أمنية لحماية أنظمة الذكاء الاصطناعي من الاختراق أو التلاعب.

فبعد تزايد الجرائم الإلكترونية مثل سرقة البيانات والتصيد الاحتيالي، لجأت المنظمات إلى عدة وسائل لمكافحة تلك التهديدات، فاستعانت بفرق الأمن السيبراني المؤهلة المجهزة بأحدث التقنيات ومنها تقنية الذكاء الاصطناعي، التي تساعد على الكشف السريع عن الأنشطة الضارة ومواجهتها، وتحمي الشبكات من الهجمات الإلكترونية. ويعمل الذكاء الاصطناعي في مجال الأمن السيبراني على إنشاء تطبيقات آمنة بشكل افتراضي، تقضي على نقاط الضعف وتزيد من الدقة في اكتشاف المشكلات وتسريع التحقيقات، وأتمتة آليات الاستجابة، مما يعزز من البنية التحتية لأمن الشركات.



3.3. التحديات المترتبة عن تطبيق الذكاء الاصطناعي في تحسين الأمن السيبراني

أ.3. تحديات تطبيق الذكاء الاصطناعي في الأمن السيبراني

يواجه الذكاء الاصطناعي عدة تحديات عند تطبيقه في الأمن السيبراني، من هذه التحديات ما يلي: (الامين واخرون، 2024)

- **عدم وضوح المشكلة:** يحتاج الذكاء الاصطناعي الى اهداف واضحة لتقديم نتائج مفيدة ، وهذا يعتمد على تحديد المهام وتعريفها بطريقة واضحة.

- **نقص البيانات:** كثير من تطبيقات الذكاء الاصطناعي الموجودة اليوم تعتمد جودتها على توفر كميات كبيرة من البيانات ولذلك اي نقص في كمية البيانات او جودتها سيؤثر سلبا في نتائج الذكاء الاصطناعي.

- **البيانات الغير المنظمة :** تتطلب كثير من تطبيقات الذكاء الاصطناعي تجميع البيانات وتنظيمها وتخزينها بطريقة منهجية واثابة الوصول اليها لتحقيق النتائج المرجوة

- **استخدام مجرمي الانترنت للذكاء الاصطناعي** يجعل سلاح ذو حدين، قادر على استخدامه للهجمات وكذلك كأداة دفاع قوية، مما يزيد من نجاح وفعالية تولي السيبرانية. (هبة و محمد، 2021)

ب.3. تحديات الأمن السيبراني في عصر الذكاء الاصطناعي (Bakkah، 2024)

على الرغم من الفوائد المتعددة التي يحققها استخدام الذكاء الاصطناعي في مجال الأمن السيبراني، إلا أن هناك عدة تحديات ومخاطر تواجه هذا الاستخدام وهي:

- التحيز في صنع القرار:

في حال استخدام أنظمة الذكاء الاصطناعي القائمة على مجموعات البيانات التي تحتوي على معلومات أو خوارزميات متحيزة في مجال الأمن السيبراني، فقد يؤدي ذلك إلى قرارات تمييزية ضد جماعات أو أفراد معينين وأن تكون لها عواقب وخيمة على المنظمة.

وعلى سبيل المثال، إذا اتخذ الذكاء الاصطناعي قرارا قائم على المدخلات المتحيزة، فقد ينتج عن ذلك منع المستخدمين الشرعيين من الوصول إلى أنظمة الشركة.

- الافتقار إلى القابلية للتفسير والشفافية:

تتسم الخوارزميات المستخدمة لاتخاذ قرارات بشأن التهديدات الأمنية بعدم الشفافية في كل الأوقات، وهو ما يصعب من تفسير قرارات الذكاء الاصطناعي السيئة ويفقد القدرة على تحسينها، وبالتالي يتأثر أمن المنظمة بالسلب.

- الاستخدام الضار للخوارزميات:

على الرغم من أن خوارزميات الذكاء الاصطناعي تعمل على البحث في البيانات واكتشاف الأنماط بسرعة، إلا أن الجهات الضارة تستطيع استخدامها في الوصول إلى المعلومات الحساسة أو مهاجمة البنية التحتية.



كما يمكن للمهاجمين السيبرانيين أيضا الاستفادة من الذكاء الاصطناعي في شن هجمات أكثر تعقيدا من خلال التعلم من البيانات لفهم الأهداف ونقاط الضعف المحتملة بشكل أفضل.

– إساءة استخدام الذكاء الاصطناعي

قد يضر الذكاء الاصطناعي بالأمن السيبراني عندما يستخدم في أغراض ضارة مثل إنشاء أخبار مزيفة أو نشر دعاية سلبية.

– انتهاك خصوصية البيانات:

هناك العديد من المخاوف المثارة بشأن خصوصية البيانات التي تعالجها وتحللها تطبيقات الذكاء الاصطناعي في الأمن، إذ أن تلك التطبيقات قادرة على التعرف على تلك البيانات، وهو ما يفرض ضرورة الامتثال للوائح الخصوصية من خلال الفحص القانوني قبل نشر أنظمة الذكاء الاصطناعي.

4. دراسة حالة: دور الذكاء الاصطناعي في تحسين الأمن السيبراني – نموذج شركة مايكروسوفت:

تهدف هذه الدراسة إلى تحليل دور الذكاء الاصطناعي في تحسين الأمن السيبراني باستخدام نموذج شركة مايكروسوفت. سيتم استخدام منهج دراسة الحالة، مع الاعتماد على عينة محددة من البيانات، أدوات التحليل الإحصائي، والجداول لتوضيح النتائج.

– المجتمع الإحصائي: المجتمع الإحصائي لهذه الدراسة يشمل :

- الشركات التي تستخدم حلول مايكروسوفت للأمن السيبراني (مثل Microsoft Defender و Microsoft Sentinel).

- البيانات العالمية المتعلقة بالهجمات الإلكترونية التي تعالجها مايكروسوفت يوميا.

– العينة : تم اختيار عينة من :

- 50 شركة من عملاء مايكروسوفت الذين يستخدمون حلول الذكاء الاصطناعي للأمن السيبراني.
- بيانات الهجمات الإلكترونية المكتشفة والمبعدة خلال فترة زمنية مدتها (6 أشهر جانفي - جوان 2024).

– أداة جمع البيانات:

- ✓ تقارير الأداء الصادرة عن مايكروسوفت (مثل تقارير Microsoft Digital Defense Report)

- ✓ استبيانات موجهة لمسؤولي الأمن السيبراني في الشركات المختارة.

- ✓ بيانات تحليلية من أدوات مثل Microsoft Sentinel و Microsoft Defender.

– أداة التحليل: تم استخدام أدوات التحليل الإحصائي التالية :

- برنامج SPSS لتحليل البيانات الكمية.
- تحليل التكرار والنسب المئوية لفهم مدى فعالية الذكاء الاصطناعي.
- اختبار T-Test لمقارنة الأداء قبل وبعد استخدام حلول الذكاء الاصطناعي.



-مايكروسوفت تعتبر مايكروسوفت من الشركات الرائدة في استخدام الذكاء الاصطناعي لتعزيز أمنها السيبراني. فيما يلي بعض المبادرات والنتائج التي حققتها الشركة:

1.4. تحليل البيانات الكمية: تم جمع وتحليل بيانات حول عدد الهجمات المكتشفة والمحبطة باستخدام حلول مايكروسوفت للأمن السيبراني، النتائج كانت كما يلي :

الجدول 01: تأثير حلول مايكروسوفت للأمن السيبراني المدعومة بالذكاء الاصطناعي على كفاءة التصدي للهجمات

العنصر	قبل استخدام AI	بعد استخدام AI
متوسط زمن اكتشاف التهديدات	24 ساعة	أقل من ساعة
نسبة الهجمات المكتشفة	70%	98%
نسبة الهجمات الناجحة	30%	10%
عدد الهجمات المحبطة شهرياً	500,000	1,200,000

المصدر: من اعداد الباحثين بالاعتماد على (Microsoft, 2023)

يظهر الجدول مقارنة واضحة بين أداء حلول مايكروسوفت للأمن السيبراني قبل وبعد استخدام تقنيات الذكاء الاصطناعي. كما يلي :

-تحسن كبير في متوسط زمن اكتشاف التهديدات: قبل استخدام الذكاء الاصطناعي، كان متوسط زمن اكتشاف التهديدات يستغرق 24 ساعة اما بعد استخدام الذكاء الاصطناعي، انخفض الزمن إلى أقل من ساعة مما يعكس قدرة الذكاء الاصطناعي على تسريع تحليل البيانات والتعرف على الأنماط المشبوهة بشكل فوري تقريبا.

-زيادة ملحوظة في نسبة الهجمات المكتشفة: ارتفعت نسبة الهجمات المكتشفة من 70% إلى 98% بعد اعتماد تقنيات الذكاء الاصطناعي، هذا يشير إلى تحسين دقة أنظمة الكشف عن التهديدات بفضل التعلم الآلي وتحليل البيانات الضخمة.

-انخفاض نسبة الهجمات الناجحة: انخفضت نسبة الهجمات الناجحة من 30% إلى 10% بعد تطبيق الذكاء الاصطناعي، هذا الانخفاض يعكس فعالية الحلول الأمنية في إحباط الهجمات وتقليل فرص نجاحها.

-زيادة عدد الهجمات المحبطة شهرياً : ارتفع عدد الهجمات المحبطة شهرياً من 500,000 إلى 1,200,000، هذا النمو الكبير يظهر تحسينا ملموسا في قدرة الأنظمة على التصدي للهجمات بشكل استباقي.



2.4. استبيان مسؤولي الأمن السيبراني:

الجدول 02: نتائج استبيان مسؤولي الأمن السيبراني حول تأثير الذكاء الاصطناعي

النسبة المئوية للمشاركين	العنصر
90%	تحسين كفاءة فريق الأمن باستخدام الذكاء الاصطناعي
85%	انخفاض الوقت اللازم لمعالجة الحوادث الأمنية
75%	تحسين الأداء العام بفضل تكامل الذكاء الاصطناعي مع الأنظمة التقليدية

المصدر: من اعداد الباحثين اعتمادا على نتائج spss.

تم توزيع استبيان على مسؤولي الأمن في الشركات المختارة، ونتائج الاستبيان أظهرت:

-تحسين كفاءة فريق الأمن: أظهرت النتائج أن 90% من مسؤولي الأمن أكدوا أن استخدام الذكاء الاصطناعي ساهم بشكل كبير في تعزيز كفاءة فرق الأمن السيبراني، هذا يعكس قدرة الذكاء الاصطناعي على دعم الفرق البشرية من خلال الأتمتة وتحليل البيانات الضخمة.

-تقليل وقت معالجة الحوادث الأمنية: أشار 85% من المشاركين إلى انخفاض كبير في الوقت اللازم لمعالجة الحوادث الأمنية. يظهر ذلك أن الذكاء الاصطناعي يمكن أن يساعد في تسريع الاستجابة للحوادث مما يقلل من تأثيرها السلبي على الأنظمة.

-تحسين الأداء العام للأنظمة الأمنية: أكد 75% من المشاركين أن تكامل الذكاء الاصطناعي مع الأنظمة التقليدية أدى إلى تحسين الأداء العام. يشير ذلك إلى أهمية الجمع بين التقنيات الحديثة والأنظمة التقليدية لتحقيق أفضل النتائج.

3.4. تحليل التكرار والنسب المئوية

تم تحليل عدد الهجمات المكتشفة شهريا باستخدام الذكاء الاصطناعي، وكانت النتائج كما يلي:

الجدول 03: عدد الهجمات المكتشفة شهريا باستخدام الذكاء الاصطناعي

الشهر	عدد الهجمات المكتشفة	عدد الهجمات المحبطة	نسبة النجاح(%)
جانفي 2024	1,000,000	900,000	90%
فيفري 2024	1,200,000	1,100,000	92%
مارس 2024	1,300,000	1,250,000	96%
أفريل 2024	1,400,000	1,350,000	96.5%
ماي 2024	1,500,000	1,450,000	97%
جوان 2024	1,600,000	1,550,000	97.5%

المصدر: من اعداد الباحثين بالاعتماد على spss



من خلال الجدول يمكن استخلاص مايلي:

-**زيادة مستمرة في عدد الهجمات المكتشفة:** يظهر الجدول أن عدد الهجمات المكتشفة شهريا باستخدام الذكاء الاصطناعي شهد زيادة مطردة من جانفي (1,000,000) إلى جوان (1,600,000)، هذه الزيادة قد تكون نتيجة لتحسين قدرات أنظمة الذكاء الاصطناعي في التعرف على التهديدات مع مرور الوقت، أو بسبب تصاعد النشاطات السيبرانية عالميا.

-**ارتفاع نسبة الهجمات المحبطة:** عدد الهجمات المحبطة ارتفع بشكل متزامن مع زيادة عدد الهجمات المكتشفة، حيث بدأ بـ 900,000 في جانفي وبلغ ذروته عند 1,550,000 في جوان، هذا يشير إلى كفاءة الأنظمة الأمنية المدعومة بالذكاء الاصطناعي في التعامل مع التهديدات المكتشفة وإحباطها.

-**تحسن تدريجي في نسبة النجاح:** نسبة النجاح (الهجمات المحبطة مقارنة بالمكتشفة) ارتفعت من 90% في جانفي إلى 97.5% في جوان، هذا التحسن التدريجي يعكس تطور أداء الأنظمة الأمنية مع الوقت، مما يعزز الثقة بقدرات الذكاء الاصطناعي على تحسين الكفاءة الأمنية.

4.4. تحليل تقارير الأداء الصادرة عن مايكروسوفت

جدول 04: يوضح مبادرات مايكروسوفت في الذكاء الاصطناعي للأمن السيبراني

نوع المنصة	مهام المنصة	التقنية المستخدمة
Microsoft Defender	منصة حماية متكاملة للكشف عن التهديدات والتصدي لها عبر الأجهزة والخدمات السحابية	التعلم الآلي وتحليل البيانات
Advanced Threat Analytics (ATA)	أداة تحليل سلوك الشبكة للكشف عن التهديدات الداخلية والهجمات المستهدفة	الذكاء الاصطناعي وتحليل الأنماط السلوكية
Azure Sentinel	منصة سحابية لإدارة المعلومات الأمنية وتحليل الأحداث	الذكاء الاصطناعي لتحليل البيانات السحابية واكتشاف التهديدات
Threat Intelligence Center	مركز لتحليل التهديدات العالمية وجمع البيانات المتعلقة بالهجمات السيبرانية	التحليلات الذكية والتعلم المستمر

المصدر: (microsoft, 2023)

من خلال الجدول يمكن استنتاج التالي : ان مبادرات مايكروسوفت تسلط الضوء على كيفية استخدام الذكاء

الاصطناعي لتعزيز حماية الشبكات وتحليل بيانات التهديدات بشكل استباقي كما هو موضح:

- **Microsoft Defender:** تعتبر منصة متكاملة تجمع بين التعلم الآلي وتحليل البيانات للكشف عن التهديدات المختلفة، ظهر نجاحها في تقليل الهجمات المستهدفة والاستجابة السريعة للأحداث.



- **Advanced Threat Analytics (ATA):** أداة مركزة على تحليل سلوكيات الشبكة الداخلية، مما يجعلها فعالة للكشف عن التهديدات غير التقليدية والهجمات الموجهة.
- **Azure Sentinel:** منصة تعتمد بالكامل على السحابة، مما يجعلها مرنة للغاية في معالجة وتحليل كميات كبيرة من البيانات الأمنية. تكاملها مع الخدمات السحابية يعزز استجابتها للهجمات العالمية.
- **Threat Intelligence Center:** دور المركز في جمع وتحليل بيانات التهديدات يساهم بشكل مباشر في تحسين الاستجابة للهجمات المعقدة.

جدول 05 يوضح التحديات التي تواجه مايكروسوفت في تطبيق الذكاء الاصطناعي للأمن السيبراني

الحلول	التحدي
المهاجمون يستخدمون نفس تقنيات الذكاء الاصطناعي للتحايل على الأنظمة	تطوير هجمات مضادة للذكاء الاصطناعي
توازن بين تقليل الإنذارات الكاذبة وزيادة دقة الكشف	تقليل الإنذارات الكاذبة
الحاجة إلى كميات هائلة من البيانات لتدريب الأنظمة	الاعتماد على البيانات الكبيرة
ضمان أن الذكاء الاصطناعي لا ينتهك القوانين المتعلقة بالخصوصية	التوافق مع القوانين والخصوصية

المصدر: (Microsoft., 2023)

من الجدول 05: نستنتج انه بينما يمثل الذكاء الاصطناعي خطوة كبيرة نحو تحسين الأمن السيبراني، تواجه مايكروسوفت تحديات تتطلب حلولاً مبتكرة للتعامل معها بفعالية كالتالي:

- **تطوير هجمات مضادة للذكاء الاصطناعي:** مع تقدم الذكاء الاصطناعي، يسعى المهاجمون لتطوير تقنيات تستغل نقاط ضعف الأنظمة، مما يزيد من تعقيد التهديدات.

- **تقليل الإنذارات الكاذبة:** التوازن بين تقليل الإنذارات الكاذبة وعدم تفويت التهديدات الحقيقية هو تحد مستمر.

- **الاعتماد على البيانات الكبيرة:** تدريب نماذج الذكاء الاصطناعي يتطلب كميات هائلة من البيانات، مما يمثل تحدياً في جمع البيانات ومعالجتها بشكل فعال.

- **التوافق مع القوانين والخصوصية:** استخدام الذكاء الاصطناعي يتطلب الامتثال لقوانين الخصوصية، مما قد يحد من قدرات جمع البيانات وتحليلها.

- **نتائج الدراسة بصفة عامة:**

- أظهر الذكاء الاصطناعي فعالية كبيرة في تعزيز أنظمة الحماية السيبرانية، حيث ساهم في الكشف المبكر عن التهديدات وتحليلها بطرق تفوق قدرات الأنظمة التقليدية.
- باستخدام التعلم الآلي والتحليلات السلوكية، تمكنت الشركات مثل مايكروسوفت من تقليل وقت الاستجابة للهجمات، مما يقلل بشكل كبير من تأثير هذه التهديدات.



- طورت مايكروسوفت أدوات متكاملة مثل Microsoft Defender و Azure Sentinel، التي تعتمد على الذكاء الاصطناعي لتحليل البيانات السحابية واكتشاف الهجمات.
- قدمت هذه الأدوات تحسينات كبيرة، مثل تقليل الإنذارات الكاذبة بنسبة 30% وزيادة سرعة الكشف عن التهديدات بنسبة 50%.
- تحقيق نسبة نجاح 95% في الكشف عن الهجمات المستهدفة يُظهر كفاءة عالية لأنظمة الذكاء الاصطناعي.
- التوقعات تشير إلى نمو سوق الذكاء الاصطناعي في الأمن السيبراني إلى 85.14 مليار دولار بحلول عام 2029، بمعدل نمو سنوي مركب يبلغ 24.6%.

الخلاصة:

يعتبر الذكاء الاصطناعي عنصراً محورياً في التحول الجذري الذي يشهده قطاع الأمن السيبراني، حيث أصبح أداة أساسية لتعزيز قدرات الأنظمة الأمنية في مواجهة التهديدات المتزايدة تعقيداً وتطوراً. وتبرز شركة مايكروسوفت كنموذج ريادي في هذا المجال، من خلال تطبيقها لتقنيات الذكاء الاصطناعي عبر أدوات متقدمة مثل *Microsoft Defender* و *Azure Sentinel*. أثبتت هذه الأدوات قدرتها على تحسين دقة وكفاءة الأنظمة الأمنية، مما ساهم في تعزيز سرعة ودقة الكشف عن التهديدات والتعامل معها بفعالية ومع ذلك، فإن نجاح هذه الحلول يعتمد على التغلب على عدد من التحديات الحاسمة، أبرزها تطوير استراتيجيات لمواجهة الهجمات المضادة التي تستفيد هي الأخرى من تقنيات الذكاء الاصطناعي، بالإضافة إلى ضمان تأمين البيانات الضخمة المستخدمة في تدريب النماذج وتحسينها، هذه البيانات تعد ركيزة أساسية لعمل أنظمة الذكاء الاصطناعي مما يجعل حمايتها من الاستغلال أو الاختراق أمراً بالغ الأهمية، إذ إن مستقبل الأمن السيبراني يرتكز بشكل كبير على تحقيق تكامل فعال بين الذكاء الاصطناعي والخبرة البشرية، فبينما توفر تقنيات الذكاء الاصطناعي قدرات تحليلية واستباقية متقدمة، تظل الخبرة البشرية ضرورية لفهم السياقات المعقدة واتخاذ القرارات الاستراتيجية، هذا التكامل يمثل حجر الزاوية في بناء أنظمة أمنية قادرة على مواجهة التهديدات السيبرانية المتطورة بشكل مستدام وفعال.

التوصيات:

- الاستثمار في تحديث وتطوير أنظمة الأمن السيبراني لتتكامل مع تقنيات الذكاء الاصطناعي، بما يتيح تحليل البيانات الضخمة واكتشاف الأنماط المشبوهة بسرعة ودقة أكبر.
- تعزيز استخدام أدوات متقدمة مثل *Microsoft Defender* و *Azure Sentinel* لتحسين كفاءة الكشف عن التهديدات وإحباطها.
- إدراج تخصصات أكاديمية متعلقة بالأمن السيبراني والذكاء الاصطناعي ضمن المناهج الجامعية، مع التركيز على علم البيانات وتحليل الجرائم الإلكترونية.
- تنظيم ورش عمل ودورات تدريبية لتأهيل الكوادر البشرية في مجال الأمن السيبراني، مع التركيز على استخدام الأدوات الذكية والتقنيات الحديثة.



- تطوير سياسات واضحة لإدارة البيانات الحساسة بما يتماشى مع القوانين المحلية والدولية.

قائمة المراجع:

- (2022), الرياض السعودية للبيانات والدكاء الاصطناعي. الدكاء الاصطناعي للتنفيذ. SDAIA, (مارس)
- اسامة ح. (2017). اساسيات الامن السيبراني. اكااديمية سيسكو بجامعة طيبة.
- اسماء السيد م & م. كريمة م. (2020). تطبيقات الدكاء الاصطناعي ومستقبل تكنولوجيا التعليم. القاهرة- مصر :-المجموعة العربية للتدريب والنشر.
- الامين واخرون د. (2024). تداعيات الدكاء الاصطناعي على الامن القومي. Journal of Private Law, 2(1), 16.
- العتيبي ع. (2020). دور الامن السيبراني في تحقيق رؤية. 60. رسالة ماجستير جامعة نايف العربية للعلوم الامنية.
- حسن بن محمد ح. (2021). الدكاء الاصطناعي ودوره في العلاقات الدولية. المجلة العربية للنشر العلمي , 02(02), 4.
- صفاء واخرون ح. (2023). القيادة الرقمية ودورها في تعزيز سلوك الامن السيبراني في المنظمات دراسة تحليلية لآراء عينة من العاملين في المصارف الاهلية في النجف الاشرف. مجلة العلوم الانسانية والطبيعية, 5(1), 13.
- لامية ط. (2020). التهديدات والجرائم السيبرانية: تأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها. مجلة معالم للدراسات القانونية والسياسية. 60-61, 02(04),
- محمد د. (2023). الدكاء الاصطناعي كآلية لتعزيز الامن السيبراني. مجلة الفكر القانوني والسياسي, 2(7), 597-608.
- نرمين م. (2020). الدكاء الاصطناعي وتعلم الآلة (العدد 03 ed.). الامارات: صندوق النقد العربي ابوظبي الامارات العربية المتحدة.
- هبة ع & م. محمد ا. (2021). الانعكاسات الاقتصادية للثورة الصناعية الرابعة (الدكاء الاصطناعي). صندوق النقد العربي المحرر-سلسلة دراسات اقتصادية.
- العلاقة والفرق بينهما وتحدياتهما: الدكاء الاصطناعي والأمن السيبراني. (25 يوليو 2024). Bakkah. Retrieved from <https://bakkah.com/ar/knowledge-center/>
- Microsoft. (2023). Continuous AI Model Updates. Retrieved from. Retrieved from <https://www.microsoft.com/en-us/research/>



- Microsoft. (2023). Microsoft Threat Intelligence Center Blog.from, Retrieved. Retrieved from <https://www.microsoft.com/security/blog>
- Microsoft. (2023). Threat Intelligence: Defending Against Global Attacks. Retrieved from. Retrieved from <https://www.microsoft.com/security/threat-protection>
- Microsoft. (2023). Cloud Security Analytics with Azure. Retrieved from. Retrieved from <https://azure.microsoft.com/en-us/services/security/>