منشآت
monsha'at
الهيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority

مركز ذكاء

كتيّب

# تطوير تطبيقات الأمن السيبراني باستخدام الذكاء الاصطناعي التحديات والحلول

## سياسة الاستخدام

إن المعلومات الواردة في هذا التقرير جُمِعَت ونُسِّقت بجهود موظفي مركز ذكاء التابع لـ الهيئة العامة للمنشآت الصغيرة والمتوسطة "منشآت"، ولا ينبغي لقارئها أن يعمل بها دون مشورة مناسبة من المتخصصين.

للمزيد من المعلومات، نرجو التواصل معنا عبر على البريد الإلكتروني: **support@thakaa.sa**

## عن كتيب الخطة والاستراتيجيات التسويقية

تم جمع وبناء محتوى هذا الكتيب كملخص لمعسكر ذكاء التدريبي:
**تطبيقات تعلم الآلة في الأمن السيبراني.**

والذي استعرض فيه أفكار لتطوير منتجات في الأمن السيبراني باستخدام تقنيات الذكاء الاصطناعي، أحد المجالات التي تشهد نمواً كبيراً في الاحتياج وتصنع جيلاً جديداً من حلول الأمن السيبراني الدفاعي المؤتمت.

## ماذا يقدم لك هذا الكتيب

يستعرض الكتيب أهم التحديات الفنية في التطبيقات الأمنية للذكاء الاصطناعي، أثر تلك التحديات على الطرق التقليدية لبناء نماذج تعلم الآلة، وقياس دقة اداءها، كما يقترح حلول عملية للتغلب والحد من آثار تلك التحديات.

# مقدمة

## تطبيقات الذكاء الاصطناعي في صناعة الأمن السيبراني:

تشهد صناعة الأمن السيبراني تطورًا لم يُسبق في السنوات الأخيرة، وذلك بفضل التقدم التقني المتسارع الذي نشهده، حيث أصبحت اليوم تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني أداة قوية للتصدي للتهديدات السيبرانية المتزايدة وحماية الأنظمة والبيانات الحساسة، كما أسهمت تلك التقنيات في كثير من حالات الاستخدام في المنتجات السيبرانية التقليدية لزيادة كفاءتها الدفاعية.

نرى اليوم زيادة كبيرةً جداً في نماذج الأعمال وفي الشركات الناشئة التي استهدفت هذا القطاع، حيث تشير بعض التقارير إلى أن حجم السوق العالمي في هذا القطاع يزيد عن 16 مليار دولار في عام 2022، بمعدل نمو سنوي مركب يقدر بما يزيد عن 20%. وبإجراء بحث سريع عن قائمة الشركات التي تستخدم تقنيات الذكاء الاصطناعي في تطوير حلول الامن السيبراني منصة بحث وتحليل للشركات الناشئة Tracxn، نجد أن عدد النتائج يتجاوز 2200 شركة، منها ما وصل بالفعل لأن يكون شركة مليارية.

من هنا تأتي أهمية تسليط الضوء على هذا القطاع وذكر نماذج من التحديات التقنية والحلول لتلك التحديات.

## أمثلة لمنتجات عالمية في الأمن السيبراني استفادت من تطبيق تقنيات الذكاء الاصطناعي:

**ومن الأمثلة اليوم علىمنتجات ساهمت بتعزيزها تقنيات الذكاء الاصطناعي:**

### 1. الكشف عن التهديدات في الشبكة:

اعتمدت كثير من الحلول التقليدية في حماية الشبكات، مثل أنظمة الكشف عن التسلل "Intrusion Detection Systems" على "قواعد" يقوم بإدخالها محللوا الأمن السيبراني لرصد الأنشطة الضارة في الشبكة وإيقافها.

أسهمت تقنيات الذكاء الاصطناعي ضمن منتجات "Next-Generation IDS" في اكتشاف أنماط جديدة لايمكن اكتشافها باستخدام القواعد المعرفّة بالشكل التقليدي. ومن الأمثلة لمنتجات في هذا المجال Cisco Firepower Next-Generation Intrusion Prevention System (NGIPS) و McAfee Network Security Platform.

**2. التنبؤ بالتهديدات المستقبلية:**

يساهم الذكاء الاصطناعي في التنبؤ بالتهديدات المستقبلية وتحليل الاتجاهات السيبرانية من خلال معالجة كميات ضخمة من البيانات من مصادر متنوعة (مثلاً: موائمة بيانات السجلات الأمنية الداخلية في المنشآة مع بيانات التهديدات السيبرانية من مصادر خارجية لاكتشاف التهديدات بشكل استباقي)، مما يساعد المنشآت على اتخاذ إجراءات وقائية مبكرة وتعزيز استراتيجيات الأمن السيبراني الدفاعي. ومن الأمثلة لمنتجات في هذا المجال CrowdStrike Falcon Intelligence و FireEye Threat Intelligence

## نظرة شمولية على المشهد السيبراني

**قبل الخوض في فرص وتحديات توظيف تقنيات الذكاء الاصطناعي في منتجات الأمن السيبراني، يمكن أن نقسم المشهد السيبراني إلى ثلاث بيئات:**

**أولاً: بيئة المنشأة، وفيها تحاول المنشأة تأمين بياناتها وأصولها السيبرانية، ومن الأنشطة التي تقوم بها المنشآت في هذا المجال:**

- التوعية والتدريب
- تحليل المخاطر
- الحوكمة والالتزام
- اختبارات الاختراقات
- إدارة الثغرات
- وغيرها من الأنشطة السيبرانية

**ثانياً: بيئة المهاجم، وفيها يحاول المهاجم الوصول إلى بيئة المنشأة المستهدفة لتحقيق واحد أو أكثر من الأهداف الهجومية، ومن الأنشطة التي يقوم بها المهاجم:**

- تقصي الضحية
- البحث عن ثغرات، بشرية أو اجرائية أو تقنية
- تطوير وسائل الهجوم المناسبة
- إجراء الهجمات
- وغيرها من الأنشطة السيبرانية الهجومية

**ثالثاً:** بيئة الاستخبارات السيبرانية، ونقصد بها جميع المصادر التي تستفيد منها إدارات الأمن السيبراني في المنظمات لتعزيز صمودها السيبراني، ومن تلك المصادر ما يكون أقرب للبيئة المنشأة (دفاعية) ومنها ما يكون أقرب لبيئة المهاجم (هجومية)، وهنا نذكر بعض تلك المصادر:

- التحذيرات الأمنية من الجهات المعنية، مثل المركز الوطني الإرشادي للأمن السيبراني، وهي أقرب لبيئة المنشآت (دفاعية).

- مستودعات البرمجيات الخبيثة، ومنها مايحوي برمجيات خبيثة جاهزة للاستخدام (Weaponized)، وتكون متاحة في بعض المتاجر في الويب العميق، ومنها ما يكون مستودع لبرمجيات خبيثة غير معدة للهجوم (Proof of Concept Exploits)، ومن مصادرها موقع Exploit-DB. وتجدر الإشارة إلى أن هذه الفئة من المصادر تكون متوسطة بين بيئة المهاجم والبيئة الدفاعية للمنشآت.

- مجتمعات الهاكرز، وهي منتديات ومنصات تجمع الهاكرز، ويجري فيها تبادل الخبرات، وبيع البرمجيات الخبيثة وخدمات الاختراق، وغيرها من الأنشطة الهجومية. وتوجد العديد من تلك المصادر في منصات التواصل الاجتماعي وبعض المنتديات في الويب المفتوح والويب المظلم. وهذه الفئة من المصادر هي الأقرب لبيئة المهاجم.

**يمكن توظيف تقنيات الذكاء الاصطناعي في تطبيقات الأمن السيبراني لتساعد بالقيام بعدة فئات من المهام، وهنا بعض تلك الفئات:**

**أولاً:** فهم التوجهات للمهاجمين والمخاطر للهجمات الجديدة، من خلال الاستفادة من البيانات التي يتم جمعها من المصادر الأقرب لبيئة المهاجم.

**ثانياً:** التنبؤ الاستباقي للهجمات والتصدي لها قبل وصولها لبيئة المنشأة، وعادة ما يتم ذلك من خلال تطبيقات الذكاء الاصطناعي على البيانات من المصادر الأقرب لبيئة الهاجم.

**ثالثاً:** اكتشاف الهجمات وتعطيلها بعد وصولها لبيئة المنشأة، وعادة ما يتم ذلك من خلال موائمة البيانات السجلات الداخلية للمنشأة مع البيانات الاستخباراتية الأقرب لبيئة المنشأة.

**وهناك الكثير من الأمثلة من تطبيقات تستهدف كل واحدة من الفئات المذكورة.**

## أمثلة لتطبيقات الذكاء الاصطناعي في الأمن السيبراني

### أولاً: فهم التوجهات للمهاجمين والمخاطر للهجمات الجديدة:

**سوق الأمن السيبراني يتجدد بشكل سريع جداً.**
هناك الكثير من المنتجات التي استفادت من تقنيات الذكاء الاصطناعي لفهم المهاجمين واستيعاب المخاطر المستجدة. يساعد هذا النوع من المنتجات متخذي القرار في تحسين الخطط الاستراتيجية والتشغيلية السيبرانية لتتواءم مع المستجدات في القطاع، ومن الأمثلة على الوظائف التي تقوم بها تلك المنتجات:

- تصنيف المنتجات والخدمات الهجومية الرائجة في السوق السوداء للأمن السيبراني، مثل خدمات (HaaS) Hacking as a Service، وبرمجيات استغلال الثغرات الجديدة. يمكن استخدام نماذج تعلم الآلة من نوع "Unsupervised learning" مثل خوارزميات التجميع (Clustering) على بيانات يتم تجميعها من المصادر الاستخباراتية الأقرب لبيئة المهاجمين.

- تمييز المصادر الاستخباراتية السيبرانية التي تساهم بمعلومات ذات موثوقية عالية وتتعلق بشكل كبير بالتقنيات والسياسات وقطاع الأعمال لكل منشأة مستفيدة من تلك المنتجات، وهذا يساعد محللي الأمن السيبراني على التركيز وعدم التشتت أمام الكم الهائل من المصادر التي يصعب متابعتها. يمكن استخدام تقنيات التصنيف والانحدار وموائمتها مع ملف المنشأة وبنيتها التقنية لتمييز المصادر الاستخباراتية السيبرانية التي ستضيف قيمة تعزز صمود المنشأة وتزيد فهمها للمخاطر المحتملة.

## ثانياً: التنبؤ الاستباقي للهجمات والتصدي لها قبل وصولها لبيئة المنشأة:

**في ظل الزيادة الضخمة والتنوع الكبير للمخاطر السيبرانية وشح الموارد البشرية التي بإمكانها معالجة جميع الثغرات والمخاطر، أصبح التنبؤ الاستباقي Predicting للأحداث السيبرانية اليوم جزءاً مهماً من استراتيجيات الأمن السيبراني الحديثة. توفر تقنيات الذكاء الاصطناعي وتعلم الآلة فرصًا للمنشآت للتركيز على التصدي لأنواع الهجمات التي بدأت تروج ولكنها لم تصل بعد لبيئة المنشأة، ومن الأمثلة على الوظائف التي تقوم بها تلك المنتجات:**

- التحديد الدقيق والآني لمدى خطورة وحجم الأثر المتوقع لكل ثغرة أمنية في أنظمة المنشأة. تساعد هذه التقنيات فرق إدارة الثغرات على ترتيب أولويات المعالجة وتحديد الطريقة المناسبة لمعالجة الثغرات (مثل تقليل المخاطر، إغلاق الثغرة، إهمال الثغرة)، بحسب ما توصي به نماذج الذكاء الاصطناعي من خلال التحليل الآني لمصادر الاستخبارات السيبرانية القريبة من مجتمع المهاجمين.

- التعرف على الأنماط الجديدة للتهديدات بشكل تلقائي ليتم نشرها على الأجهزة المكافحة للهجوم مثل أجهزة كشف التسلل وأجهزة الكشف والاستجابة للتهديدات، حتى تتصدى لتلك الأنماط قبل وصول الهجوم للشبكة. يتم هذا عادة من خلال تحليل البيانات من المصادر الاستخباراتية المفتوحة والمدفوعة.

## ثالثاً: اكتشاف الهجمات وتعطيلها بعد وصولها لبيئة المنشأة:

وهذه من أكثر حالات الاستخدام شيوعاً وتنوعاً، حيث شكلت الجيل القادم (Next-Generation Appliances) لتقنيات الحماية السيبرانية الجديدة، والتي لم تعد تعتمد بشكل أساسي على التعرف على بصمات التهديدات (Signatures) بالصورة التقليدية فحسب، بل إنه بإمكانها التعرف على أنماط التحرك في الشبكة غير الطبيعية وايقافها أو اتخاذ قرارات تحد من آثارها السلبية، وتنبيه محللي الأمن السيبراني في مراكز العمليات السيبرانية.

**من الأمثلة على تلك التطبيقات:**

- جدران الحماية النارية من الجيل القادم NGFW، والتي تستخدم فيها تقنيات الذكاء الاصطناعي للفحص العميق لحزم البيانات التي تنتقل داخل الشبكة، والكشف عن الأنماط للتحركات غير المعتادة والتي قد تشير إلى تهديدات محتملة.

- يتم استخدام تقنيات الذكاء الاصطناعي للتعرف على الرسائل البريدية التصيدية من خلال تحليل النصوص باستخدام تقنيات معالجة اللغات الطبيعية، وكذلك تحليل المرفقات البريدية والروابط المدمجة للصفحات الخارجية. حققت نماذج تعلم الآلة في هذه المهمة نتائج مبهرة عالية الدقة.

## التحديات التي تواجه تطبيقات الذكاء الاصطناعي في الأمن السيبراني

**هناك الكثير من التحديات التي يحسن أن تؤخذ بعين الاعتبار خلال مرحلة تحليل متطلبات المنتجات البرمجية التي تستخدم تطبيقات الذكاء الاصطناعي في الأمن السيبراني. نسلط الضوء في هذا الكتيب على أهم ثلاثة تحديات، ونقترح بعض الحلول لتقيل آثار التحديات.**

### التحدي الأول: اختيار نماذج تعلم الآلة المناسبة لطبيعة التطبيق:

في كثير من تطبيقات الذكاء الاصطناعي في الأمن السيبراني المعتمدة على نماذج تعلم الآلة لاتستدعي الحاجة أن تكون القرارات التي تتوصل لها النماذج المستخدمة قابلة للتفسير، وخصوصاً في التطبيقات التي تستعدي طبيعتها لأن يتخذ النموذج قراراً بشكل آني مثل قرارات الجدر الناريةFirewall بشأن حزم البيانات، سواء في قبول Pass أو رفض Drop دخولها للشبكة. تلك القرارات لا تحتمل التاخير، كما أنه من النادر أن يحتاج محللوا الشبكة لفهم المنطق والأسباب الرئيسية التي توصل بها النموذج المستخدم في الجداري الناري إلى قرار معين. إلا أن هناك فئة أخرى من التطبيقات في المجال نفسه غالباً ما تستدعي فيها الحاجة إلى فهم المنطق والأسباب التي توصل بها النموذج لقرار معين، وخصوصاً تلك التطبيقات التي لا تحتاج لاتخاذ قرارات عاجلة، أو التطبيقات التي تدعم قرارات أخرى يتخذها البشر، مثل نماذج تحديد مستوى خطورة الثغرات البرمجية المبنية على بيانات يتم جمعها من مصادر تكون قريبة لمجتمع الهاكرز، والتي يستند عليها محللوا المخاطر لاتخاذ قرارات تتعلق بترتيب أوليات معالجة الثغرات البرمجية.

### الطرق المثلى للتعامل مع تحدي اختيار نماذج تعلم الآلة المناسبة لطبيعة التطبيق

**فهم عوامل الاحتياج للنماذج القابلة للتفسير، أو ما يعرف بـ(XAI) Explainable Artificial Intelligence ومنها:**

- أهمية المشاركة البشرية في عملية اتخاذ القرار: العرض الأول لنماذج XAI هو تمكين محللي الأمن السيبراني من فهم الاستدلال والعوامل المنطقية التي أدت بالنموذج إلى أن يتوصل إلى قرار معين أكثر من نماذج الذكاء الاصطناعي الغير قابلة للتفسير. هذه الميزة تساعد المحلل السيبراني إلى الوصول إلى فهم أفضل للعوامل التقنية المرتبطة بالمخاطر، ليتم بعدها مؤائمتها مع العوامل غير التقنية (مثلاً، جدولة الكوادر، تحليل الأثر في حال حصل الخطر). هناك الكثير من التطبيقات من هذا النوع. في تلك التطبيقات يكون مخرجات النماذج داعمة لقرارات التي يتخذها البشر.
- الأداء والدقة: غالباً ما تحقق نماذج الذكاء الاصطناعي وخصوصاً نماذج التعلم العميق أداءًا عاليًا ودقةً ممتازة في مختلف المهام في مجال الأمن السيبراني، وهي اليوم تستخدم على نطاق واسع في اكتشاف وتصنيف التهديدات بشكل فعال بناءً على الأنماط والسلوكيات التي يتم تدريبها على مجموعات كبيرة من البيانات. إذا كان الأداء والدقة العالية هما الهدفان الأهم، فقد يكون من الأفضل اختيار نماذج الذكاء الاصطناعي الأعلى دقة، وغالباً لا تكون من ضمن نماذج XAI.

## ثانياً: التعامل مع فئات من البيانات غير المتزنة

(فئة الأحداث النادرة مثل الهجمات، وفئة الأحداث الطبيعية الدارجة):

**التوازن الفئوي:** هو تحدي شائع في تطبيقات الذكاء الاصطناعي للمشكلات الأمنية عموماً والتي من ضمنها مشكلات الأمن السيبراني، فعندما نستخدم الذكاء الاصطناعي لحماية أنظمتنا من الهجمات السيبرانية، غالباً ما يكون هناك فرق كبير بين عدد الهجمات وعدد الأحداث الطبيعية العادية، حيث أن الأحداث السيبرانية تكون أقل شيوعًا بكثير من الأحداث العادية التي تحدث يوميًا، وهذا يؤدي إلى توزيع غير متوازن للفئات في بيانات التدريب، حيث تغلب الفئة الأكثرية (الأحداث العادية) على الفئة الأقلية (الهجمات).

هذا الفرق في التوازن يمكن أن يسبب تحديات، فقد يصعب على نماذج تعلم الآلة التعرف على الهجمات السيبرانية النادرة أو التنبؤ بها بشكل دقيق، لأنها غير مألوفة أبداً بالنسبة لها عندما تم تدريبها على البيانات غير المتزنة، ففي نماذج التصنيف مثلاً، كثيراً ما نجد النموذج منحازاً لتصنيف الأحداث على أنها أحداث عادية إذا لم يتم التعامل مع تحدي عدم التوازن الفئوي في الحسبان. قد يؤدي ذلك إلى زيادة عدد الأخطاء في تطبيقاتنا.

### الطرق المثلى للتعامل مع تحدي فئات من البيانات غير المتزنة:

**يمكننا تقليل أثر عدم التوازن الفئوي التي تحدثنا عنها من خلال استخدام العديد من التقنيات قبل وبعد تدريب النموذج الذي وقع الاختيار عليه. ومن تلك التقنيات:**

- **تقنيات إعادة توزيع عينة التدريب (Resampling techniques):** تمكننا هذه التقنيات من التلاعب في توزيع الفئات في بيانات التدريب بطرق مختلفة بحسب نوع الاحتياج وطبيعة البيانات التي يتم التعامل معها، ويحدث ذلك من خلال زيادة عدد نقاط البيانات من الأحداث النادرة (الهجمات) أو تقليل عدد نقاط البيانات من الأحداث الدارجة (الأحداث الطبيعية). من الناحية التطبيقة، التقليل من عدد نقاط البيانات للأحداث الدارجة يبدو أمراً أسهل، حيث يمكن استخدام تقنيات جمع العينات لأخذ عينة من فئة البيانات الدارجة ثم استخدام تلك العينة في تدريب النموذج، كثيراً ما يقلل ذلك من أثر مشكلة عدم التوازن الفئوي. في أحيان أخرى يتم زيادة نقاط البيانات من الفئة الأقل (الهجمات) إما بزيادة عشوائية من خلال تكرار بعض نقاط البيانات، أو تتم الزيادة باستخدام تقنيات توليدية لنقاط البيانات من نوع الهجمات، ومن الأمثلة الدارجة لتلك التقنيات SMOTE (Synthetic Minority Over-sampling Technique). يمكن التعامل مع محددات كثيرة تقنيات إعادة توزيع العينة من خلال مكتبة imbalanced-learn بلغة البايثون.

- **تعديل وزن الفئات أثناء تدريب النماذج:** يمكننا تعديل وزن الفئات بإعطاء الفئة الأقلية وزنًا أعلى لتعزيز أهميتها وتحسين الكشف عن الهجمات.

## ثالثاً: التعامل مع تحدي تغيير مفهوم البيانات مع تقدم الوقت:

تغير المفهوم"، أو ما يسمى (Concept Drift)، هو عبارة عن ظاهرة في البيانات تتمثل في تغير الخصائص الاحصائية للمتغيرات في البيانات مع مرور الوقت، سواء المتغير المراد تصنيفه في نماذج التصنيف، أو علاقة المتغيرات ببعضها في نماذج تعلم الآلة بشكل عام. كما ذكرنا، التقنيات في الأمن السيبراني بشقيه الدفاعي والهجومي تتجدد بشكل سريع جداً، فبرمجيات استغلال الثغرات التي تستخدم في وقت ما قد لا تكون قابلة للاستخدام بعد سنة فقط من تطويرها بسبب أن الثغرات قد تم سدها في تحديثات برمجية. كذلك الوسائل الهجومية والدفاعية وطرق حماية الأنظمة والأصول تتغير بشكل سريع.

وللتوضيح أكثر، دعونا نفترض أن لدينا نموذج تعلم الآلة يهدف إلى تحليل بيانات مختلفة حول الأمان السيبراني لمنشأة ما وترتيب المخاطر بناءً على البنية التقنية لتلك المنشأة. يعتمد النموذج على مجموعة من المؤشرات (Features) مثل عدد الهجمات السابقة، وتصنيف ثغرات الأمان، وتكلفة الحوادث السيبرانية السابقة، وغيرها. مع مرور الوقت، يحدث تغير في المفهوم للمخاطر السيبرانية وعلاقتها بالبنية التقنية للمنشأة. قد يظهر تهديد سيبراني جديد يستغل ثغرة في موجودة في البنية التقنية الحالية أو يستخدم تقنيات هجومية متطورة لم تكن موجودة في السابق. هذا التغير يمكن أن يؤدي إلى تعديل العلاقات والترتيبات بين المؤشرات التي يعتمد عليها النموذج.

## الطرق المثلى للتعامل مع تحدي تغيير مفهوم البيانات مع تقدم الوقت:

**هناك العديد من الطرق للتعامل مع التطبيقات التي يكون فيها تغير المفهوم حاضراً، ومن تلك الطرق:**

- **تحليل وقياس تغير المفهوم:** تعتمد تقنيات تحليل وقياس تغير المفهوم على أساليب إحصائية لحساب الفرق بين توزيعين احصائيين لاكتشاف التغير في المفهوم، فكلما زاد الفرق خلال مدة قصيرة دل ذلك على أن وجود تغير أقوى بالمفهوم. فمثلاً لا نتوقع ابداً أن يكون هناك تغير في توزيع البيانات في عينة كبيرة من الصور لقطط تم التقاطها قبل مدة طويلة (عشر سنوات مثلاً) بالمقارنة بعينة كبيرة من الصور التي تم التقاطها لقطط مؤخراً، وذلك ببساطة لأن حيوان القط لم يطرأ عليه تغيير خلال المدة وإن طالت. يمكننا قياس تغير المفهوم باستخدام مؤشرات كثيرة، ومنها KL Divergence، و JS Divergence، أو ببساطة يمكن تدريب نموذج على بيانات تاريخية تتوقف قبل تاريخ محدد وقياس دقته على بيانات موزعة زمنياً بعد تاريخ التوقف عن التدريب ورصد تناقص دقة النموذج مع مرور الوقت، ثم التدخل لمعالجة الأمر في حال نقصت الدقة عن مستوى معين.

- **إعادة تدريب النماذج بشكل دوري:** من الطرق الدارجة كذلك إعادة تدريب النماذج بشكل دوري باستخدام بيانات جديدة لالتقاط التغير في المفهوم. عند اكتشاف تغير كبير في المفهوم، يمكننا جمع بيانات جديدة تمثل المفهوم الحالي واستخدامها لإعادة تدريب النموذج. يسمح ذلك للنموذج بالتكيف مع التغيرات في التوزيع الإحصائي، إلا أنه من المهم الإشارة إلى أن إعادة تدريب النماذج ليست عملية سهلة في كثير من الأحيان، وقد تتطلب جهد بشري كبير في تصنيف نقاط كثيرة من البيانات حتى يتم تدريب النماذج عليها.

## خاتمة:

**في ختام هذا الكتيب**، ندرك أن صناعة الأمن السيبراني تعيش حقبة من التطور غير المسبوق بفضل التقدم التقني السريع الذي نشهده. تطبيقات الذكاء الاصطناعي في مجال الأمن السيبراني أصبحت أدوات قوية في مكافحة التهديدات المتزايدة وحماية الأنظمة والبيانات الحساسة. هذه التقنيات لعبت دورًا حاسمًا في تعزيز كفاءة منتجات الأمن السيبراني التقليدية. شهد القطاع نموًا كبيرًا في عدد الشركات الناشئة ونماذج الأعمال المتعلقة بهذا المجال، إلا أنه من الواضح أن هذا القطاع يواجه تحديات تقنية مهمة، ومن بينها تحديات اختيار نماذج تعلم الآلة المناسبة لطبيعة التطبيق، والتعامل مع فئات بيانات غير متزنة، وتحدي تغير مفهوم البيانات مع مرور الوقت.

استعرضنا في هذا الكتيب عدد من الطرق التي يمكننا الاعتماد عليها للتغلب على تلك التحديات وتعزيز قدرتنا على اكتشاف التهديدات السيبرانية باستخدام تقنيات الذكاء الاصطناعي لتأمين الأنظمة والبيانات بشكل فعال.

## حدود المسئولية:

تُقدِّم "منشآت" المصادر التعليميَّة، وهي خدمة من خدمات مكتبة مركز ذكاء، التي تُقدِّمها "منشآت"، والتي تساهم وتساعد في إثراء المحتوى العربي لمصادر التعلم عبر الإنترنت، لتوفير المعرفة لفئات مختلفة في مجالات التقنية وريادة الأعمال، ولا تقدم "منشآت" أو من يمثلها أي قرارات أو ضمانات، سواءً بشكل صريح أو ضمني حول اكتمال أو دقة أو موثوقية أو ملاءمة أو توافر هذه البيانات أو المعلومات أو المواد ذات الصلة الواردة لأي غرض كان، ولا يجوز استخدامها لغرض آخر غير الاستخدام العام، ولا تتحمّل "منشآت" أو من يُمثِّلها، أنَّها -بأي حال من الأحوال- أي أضرار مادية أو معنوية، مباشرة أو غير مباشرة قد تحصل، وتؤكد "منشآت" أو من يمثلها أنها غير مسؤولة عن أي فرصة ضائعة أو خسارة أو ضرر من أي نوع، ومنها على سبيل المثال لا الحصر، أي ضرر أو فيروس قد يتعرض له الحاسوب الشخصي، ذلك نتيجة الدخول إلى هذه الصفحة، وأن "منشآت" أو من يُمثِّلها، تبذل الجهد للتأكد من أن المعلومات المتوفرة من خلال المصادر التعليميَّة، شاملة ودقيقة قدر المستطاع.

وكما تؤكد "منشآت" على الالتزام بحقوق النشر وحقوق الملكية الفكرية لمحتويات المصادر التعليميَّة، بما في ذلك شعار "منشآت"، ولا يحق نشر أي معلومات أو رأي يتم التعبير عنه هنا، دون الحصول على إذن خطي مسبق للقيام بذلك من قِبَل "منشآت".

منشآت
monsha'at
الهيئة العامة للمنشآت الصغيرة والمتوسطة
Small & Medium Enterprises General Authority

مركز ذكاء

# شكرًا