

تأثير الذكاء الاصطناعي على غرف التحكم الأمنية – دراسة تطبيقية على

البنك الوطني العربي

**The Impact of Artificial Intelligence on Security Control Rooms –  
An Applied Study on the Arab National Bank**

اعداد الطالب:

محمد عبده عجبي

اشراف:

الدكتورة/ آلاء احمد

الدكتورة/ سارة فريد

العام الدراسي: 2026م – 1447هـ



## الإهداء

إلى والديّ الغاليين، دعاؤهما سر نجاحي، ورضاهما غاية سعبي، فمهما  
شكرت لا أوفي جميلهما.

إلى زوجتي الحبيبة، رفيقة دربي، سندي وصبري، وشريكة همومي  
وأفراحي.

إلى أبنائي الأعزاء، أرجو أن يكون هذا العمل فخراً لكم، وأن تدركوا قيمة  
العلم.

إلى مشرفي الفاضل، الدكتور / .....، بنصحه وتوجيهه ووقته الثمين،  
فله جزيل الشكر.

إلى القادة الأمنيين ومحلي **SOC** وخبراء البنك الوطني العربي، الذين  
أثروا الدراسة بآرائهم.

إلى وطني المملكة العربية السعودية، قيادةً وشعباً، بدعمه للتحول  
الرقمي والأمن السيبراني تحقيقاً لرؤية 2030.

وإلى كل من ساهم في هذا العمل، أهدي ثمرة جهدي، راجياً الله أن  
ينفع به.

## الشكر والتقدير

الحمد لله رب العالمين، الذي بنعمته تتم الصالحات.

أتقدم بخالص الشكر والتقدير إلى مشرفي الفاضل، الدكتور / .....،  
على توجيهاته القيمة ونقده البناء وصبره الجميل، فله مني جزيل  
الامتنان.

كما أشكر لجنة المناقشة وأساتذة كلية الإدارة بجامعة ميدأوشن على ما  
قدموه من علم وعون.

جزيل الشكر للبنك الوطني العربي (anb) على تعاونه الكبير، ولجميع  
أفراد عينة الدراسة من القادة الأمنيين ومحليي SOC والخبراء، الذين  
كانوا روح هذا البحث.

أشكر كل باحث سابق في مجال الذكاء الاصطناعي والأمن السيبراني،  
وأخص بالشكر أسرتي الكريمة على دعمهم وصبرهم.

وأخيراً، أسأل الله أن يجعل هذا العمل خالصاً لوجهه، نافعاً لعباده، وأن  
يوفقنا جميعاً لما يحبه ويرضاه.

الباحث / محمد عبده عجيبى - 2026م

## الملخص

هدفت هذه الدراسة إلى قياس تأثير تقنيات الذكاء الاصطناعي (الرؤية الحاسوبية، تعلم الآلة والتحليلات التنبؤية، ومعالجة اللغات الطبيعية) على كفاءة أداء غرف التحكم الأمنية في البنك الوطني العربي، من حيث ثلاثة أبعاد رئيسية: سرعة الاستجابة (المقاسة بمؤشري MTTR و MTDD)، ودقة التحليل (الحد من الإنذارات الكاذبة وإجهاد التنبيهات)، ومستوى الامتثال التنظيمي لأطر البنك المركزي السعودي (SAMA) والهيئة الوطنية للأمن السيبراني (NCA). اتبعت الدراسة المنهج الكمي الوصفي التحليلي، مستخدمة استبانة إلكترونية صممت خصيصاً لهذا الغرض، تم توزيعها على عينة قصدية بلغ قوامها (190) مشاركاً من القادة الأمنيين، ومحلي مراكز العمليات الأمنية (SOC)، ومهندسي الذكاء الاصطناعي، وخبراء تقنية المعلومات في البنك الوطني العربي. تم تحليل البيانات باستخدام برنامج SPSS، واختبار الفرضيات عبر تحليل الانحدار المتعدد والخطي البسيط، واختبارات تحليل التباين (ANOVA) واختبار "ت". أظهرت النتائج وجود تأثير إيجابي ذي دلالة إحصائية لتقنيات الذكاء الاصطناعي مجتمعة على أداء غرف التحكم الأمنية، حيث فسرت ما نسبته 82.1% من التباين الحاصل في الأداء الأمني. كما تبين أن تعلم الآلة والتحليلات التنبؤية هو الأكثر تأثيراً ( $\beta = 0.371$ ) يليه الرؤية الحاسوبية ( $\beta = 0.328$ ) ثم معالجة اللغات الطبيعية ( $\beta = 0.301$ ). وسجلت جميع أبعاد الأداء الأمني مستويات مرتفعة (متوسط عام 4.08 من 5). كما كشفت النتائج عن وجود فروق ذات دلالة إحصائية في التقديرات تعزى إلى المسعى الوظيفي وسنوات الخبرة، بينما لم تظهر فروق حسب المؤهل العلمي. وأبرز التحديات التي تواجه البنك كانت: نقص الكوادر البشرية المؤهلة (متوسط 3.99)، وارتفاع التكاليف التشغيلية (4.02)، وتحديات الخصوصية والأخلاقيات (3.94). أوصت الدراسة بتعميم استخدام تقنيات الذكاء الاصطناعي في جميع مراكز العمليات الأمنية، وتطوير برامج تدريبية مستمرة للمحللين، وإنشاء وحدة حوكمة داخلية للإشراف على أخلاقيات الذكاء الاصطناعي، ودمج حلول SOAR لأتمتة الاستجابة، وإجراء تقييمات دورية لمؤشرات الأداء. كما أوصت الجهات التنظيمية بإصدار دلائل إرشادية موحدة لتبني الذكاء الاصطناعي في القطاع المصرفي، وإنشاء منصة وطنية لتبادل التهديدات الذكية.

الكلمات المفتاحية: الذكاء الاصطناعي، غرف التحكم الأمنية، مراكز العمليات الأمنية (SOC)، تعلم الآلة، الرؤية الحاسوبية، معالجة اللغات الطبيعية، الامتثال التنظيمي، البنك الوطني العربي، رؤية المملكة 2030.

## **Abstract**

**This study aimed to measure the impact of artificial intelligence technologies (computer vision, machine learning and predictive analytics, and natural language processing) on the efficiency of security control room performance at the Arab National Bank, in terms of three main dimensions: response speed (measured by MTTD and MTTR indicators), analysis accuracy (reducing false alarms and alert fatigue), and the level of regulatory compliance with the frameworks of the Saudi Central Bank (SAMA) and the National Cybersecurity Authority (NCA). The study adopted a quantitative descriptive-analytical approach, using a specifically designed electronic questionnaire distributed to a purposive sample of (190) participants, including security leaders, Security Operations Center (SOC) analysts, AI engineers, and information technology experts at the Arab National Bank. Data were analyzed using SPSS software, and hypotheses were tested using multiple and simple linear regression analysis, ANOVA, and T-tests. The results showed a statistically significant positive impact of AI technologies collectively on security control room performance, explaining 82.1% of the variance in security performance. Machine learning and predictive analytics were found to have the greatest impact ( $\beta = 0.371$ ), followed by computer vision ( $\beta = 0.328$ ), and then natural language processing ( $\beta = 0.301$ ). All security performance dimensions recorded high levels (overall mean of 4.08 out of 5). The results also revealed statistically significant differences in estimates attributed to job title and years of experience, while no differences were found based on educational qualification. The most prominent challenges facing the bank were: shortage of qualified human cadres (mean 3.99), high operational costs (4.02), and privacy and ethical challenges (3.94). The study recommended the widespread adoption of AI technologies across all security operations centers, the development of continuous training programs for analysts, the establishment of an internal governance unit to oversee AI ethics, the integration of SOAR solutions for response automation, and the periodic evaluation of performance indicators. It also recommended that regulatory bodies issue unified guidelines for AI adoption in the banking sector and establish a national platform for intelligent threat intelligence sharing.**

**Keywords:** Artificial Intelligence, Security Control Rooms, Security Operations Centers (SOC), Machine Learning, Computer Vision, Natural Language Processing, Regulatory Compliance, Arab National Bank, Saudi Vision 2030.

## فهرس المحتويات

| الصفحة | العنوان                                                        |
|--------|----------------------------------------------------------------|
| ب      | البسمة                                                         |
| ج      | الإهداء                                                        |
| د      | الشكر والتقدير                                                 |
| هـ     | الملخص                                                         |
| و      | Abstract                                                       |
| ز      | فهرس المحتويات                                                 |
| ط      | فهرس الجداول                                                   |
|        | الفصل الأول: الإطار العام للدراسة                              |
| 2      | 1.1. مقدمة البحث                                               |
| 3      | 1.2. مشكلة الدراسة                                             |
| 4      | 1.3. أهمية الدراسة                                             |
| 5      | 1.4. أسئلة الدراسة                                             |
| 6      | 1.5. أهداف الدراسة                                             |
| 7      | 1.6. فرضيات الدراسة                                            |
| 8      | 1.7. نموذج الدراسة                                             |
| 8      | 1.8. الدراسة الميدانية (نطاق الدراسة)                          |
| 9      | 1.9. مصطلحات الدراسة                                           |
| 12     | 1.10. هيكل الدراسة                                             |
|        | الفصل الثاني: الإطار النظري للدراسة                            |
| 14     | تمهيد                                                          |
| 14     | المبحث الأول: الدراسات السابقة                                 |
| 14     | 2.1.1 الدراسات العربية                                         |
| 17     | 2.1.2 الدراسات الأجنبية                                        |
| 18     | 2.1.3 التعقيب على الدراسات السابقة                             |
| 19     | المبحث الثاني: الإطار النظري                                   |
| 19     | 2.2.1 الأسس النظرية والتقنية للذكاء الاصطناعي في المجال الأمني |
| 22     | 2.2.2. غرف التحكم الأمنية ومراكز العمليات الأمنية ((SOC        |
| 25     | 2.2.3. تكامل الذكاء الاصطناعي في غرف التحكم الأمنية            |

|    |                                                                           |
|----|---------------------------------------------------------------------------|
| 28 | 2.2.4 الأبعاد التنظيمية والبشرية لتوظيف الذكاء الاصطناعي في الأمن المصرفي |
| 30 | 2.2.5 الذكاء الاصطناعي في القطاع المصرفي السعودي                          |
| 33 | خلاصة الفصل                                                               |
| 34 | الفصل الثالث: منهجية الدراسة                                              |
| 35 | تمهيد                                                                     |
| 35 | 3.1 التعريفات الإجرائية لمتغيرات البحث                                    |
| 35 | 3.2 تصميم البحث                                                           |
| 37 | 3.3 مجتمع البحث وطرق وتقنيات أخذ العينات                                  |
| 37 | 3.4 طريقة جمع البيانات                                                    |
| 37 | 3.5 أنواع البيانات                                                        |
| 38 | 3.6 إجراءات التحليل الإحصائي                                              |
| 38 | الخلاصة                                                                   |
| 39 | الفصل الرابع: التحليل الإحصائي ومناقشة النتائج                            |
| 40 | تمهيد                                                                     |
| 40 | 4.1 الإحصاء الوصفي للعينات (البيانات الديموغرافية والمهنية)               |
| 41 | 4.2 تحليل التكرارات والنسب المئوية لفقرات المتغير المستقل                 |
| 44 | 4.3 تحليل التكرارات والنسب المئوية لفقرات المتغير التابع                  |
| 46 | 4.4 تحليل التكرارات والنسب المئوية لقسم التحديات والمعوقات                |
| 47 | 4.5 المتوسطات الحسابية والانحرافات المعيارية لمتغيرات الدراسة             |
| 50 | 4.6 ثبات الأداة (Reliability)                                             |
| 50 | 4.7 صدق الأداة (Validity) – الاتساق الداخلي                               |
| 52 | 4.8 اختبار الفرضيات باستخدام تحليل الانحدار المتعدد                       |
| 53 | 4.9 اختبار الفروض الفرعية (تأثير كل بعد مستقل على الأبعاد التابعة)        |
| 56 | 4.10 اختبار الفروق حسب المتغيرات الديموغرافية (ANOVA و T-test)            |
| 58 | 4.11 ملخص اختبار الفرضيات                                                 |
| 59 | 4.12 مناقشة عامة للنتائج في ضوء الإطار النظري والدراسات السابقة           |
| 59 | خلاصة الفصل                                                               |
| 60 | الفصل الخامس: النتائج والتوصيات                                           |
| 61 | تمهيد                                                                     |
| 61 | 5.1 مناقشة النتائج                                                        |
| 62 | 5.2 الاستنتاجات العامة                                                    |
| 63 | 5.3 التوصيات                                                              |

|    |                                 |
|----|---------------------------------|
| 64 | 5.4 مقترحات لدراسات مستقبلية    |
| 65 | 5.5 قيود الدراسة                |
| 65 | خاتمة الدراسة                   |
| 66 | قائمة المراجع والمصادر          |
| 66 | أولاً/ المراجع والمصادر العربية |
| 67 | ثانياً/ المراجع الأجنبية        |
| 71 | الملاحق: استبانة الدراسة        |

## فهرس الجداول

| الصفحة | العنوان                                                                                   | الجدول |
|--------|-------------------------------------------------------------------------------------------|--------|
| 40     | التوزيع التكراري والنسب المئوية لعينة الدراسة حسب المتغيرات الديموغرافية (n=190)          | 4.1    |
| 42     | توزيع تكرارات ونسب فقرات بعد الرؤية الحاسوبية (Computer Vision)                           | 4.2    |
| 42     | توزيع تكرارات ونسب فقرات بعد تعلم الآلة والتحليلات التنبؤية (Machine Learning)            | 4.3    |
| 43     | توزيع تكرارات ونسب فقرات بعد معالجة اللغات الطبيعية (NLP)                                 | 4.4    |
| 44     | توزيع تكرارات ونسب فقرات بعد سرعة الاستجابة (MTTD & MTTR)                                 | 4.5    |
| 45     | توزيع تكرارات ونسب فقرات بعد دقة التحليل والحد من الإرهاق (Analysis Accuracy)             | 4.6    |
| 45     | توزيع تكرارات ونسب فقرات بعد الامتثال التنظيمي (Regulatory Compliance)                    | 4.7    |
| 46     | توزيع تكرارات ونسب فقرات قسم التحديات والمعوقات                                           | 4.8    |
| 47     | المتوسطات الحسابية والانحرافات المعيارية لأبعاد المتغير المستقل (تقنيات الذكاء الاصطناعي) | 4.9    |
| 48     | المتوسطات الحسابية والانحرافات المعيارية لأبعاد المتغير التابع (أداء غرف التحكم الأمنية)  | 4.10   |
| 49     | المتوسطات الحسابية والانحرافات المعيارية لتحديات توظيف الذكاء الاصطناعي                   | 4.11   |
| 50     | معاملات ألفا كرونباخ لثبات أداة الدراسة                                                   | 4.12   |
| 51     | معاملات ارتباط بيرسون بين كل فقرة والدرجة الكلية للبعد التابع له                          | 4.13   |
| 52     | ملخص نموذج الانحدار المتعدد (تأثير تقنيات الذكاء الاصطناعي على الأداء الأمني الكلي)       | 4.14   |
| 52     | معاملات الانحدار المتعدد (Coefficients)                                                   | 4.15   |
| 53     | تحليل التباين (ANOVA) لنموذج الانحدار                                                     | 4.16   |
| 54     | نتائج الانحدار الخطي البسيط (تأثير تعلم الآلة على سرعة الاستجابة)                         | 4.17   |
| 54     | نتائج الانحدار الخطي البسيط (تأثير الرؤية الحاسوبية على دقة التحليل)                      | 4.18   |
| 55     | نتائج الانحدار الخطي البسيط (تأثير معالجة اللغات الطبيعية على سرعة الاستجابة)             | 4.19   |
| 55     | نتائج الانحدار المتعدد (تأثير تقنيات الذكاء الاصطناعي على الامتثال التنظيمي)              | 4.20   |

|    |                                                |      |
|----|------------------------------------------------|------|
| 56 | تحليل التباين الأحادي (ANOVA) – المسمى الوظيفي | 4.21 |
| 56 | تحليل التباين الأحادي (ANOVA) – سنوات الخبرة   | 4.22 |
| 57 | تحليل التباين الأحادي (ANOVA) – المؤهل العلمي  | 4.23 |
| 57 | تحليل التباين الأحادي (ANOVA) – القسم التابع   | 4.24 |
| 58 | ملخص نتائج اختبار فرضيات الدراسة               | 4.25 |

## الفصل الأول: الإطار العام للدراسة

- 1.1. مقدمة البحث
- 1.2. مشكلة الدراسة
- 1.3. أهمية الدراسة
  - 1.3.1. على المستوى النظري
  - 1.3.2. على المستوى التطبيقي
- 1.4. أسئلة الدراسة
- 1.5. أهداف الدراسة
- 1.6. فرضيات الدراسة
- 1.7. نموذج الدراسة
- 1.8. الدراسة الميدانية (نطاق الدراسة)
- 1.9. مصطلحات الدراسة
- 1.10. مخطط المشروع

## 1.1. مقدمة البحث

يشهد القطاع المصرفي العالمي تحولاً هيكلياً متسارعاً في ظل الثورة الرقمية المعاصرة، حيث أصبح الذكاء الاصطناعي أحد المرتكزات الاستراتيجية لإعادة تشكيل البنية التشغيلية والأمنية للمؤسسات المالية. فلم تعد تطبيقات الذكاء الاصطناعي تقتصر على دعم العمليات أو تحسين الكفاءة الإجرائية، بل امتدت لتشكيل إطاراً متكاملًا لإدارة المخاطر والتنبؤ بالتهديدات وتعزيز المرونة المؤسسية في مواجهة الهجمات المركبة (Kovačević et al., 2024). وفي هذا السياق، تمثل غرف التحكم الأمنية ومراكز العمليات الأمنية (SOC) البنية العصبية للمنظومة المصرفية، إذ تضطلع بمهمة تحليل التدفقات الضخمة من البيانات المرئية والرقمية الصادرة عن أنظمة المراقبة وأجهزة الاستشعار وسجلات النشاط السيبراني.

إن التزايد المطرد في حجم البيانات وتعقيد أنماط التهديدات أدى إلى تراجع فعالية نماذج المراقبة التقليدية القائمة على التدخل البشري المكثف، لا سيما في ظل ظاهرة "إجهاد التنبيهات" (Alert Fatigue) التي تؤثر سلباً في دقة التحليل وسرعة الاستجابة (Devoteam, 2024). ومن ثم برزت الحاجة إلى توظيف خوارزميات التعلم العميق والرؤية الحاسوبية والتحليلات التنبؤية لتحويل غرف التحكم من نمط الاستجابة التفاعلية إلى نموذج استباقي قائم على التنبؤ والاحتواء المبكر للمخاطر (كامل، 2024).

وتشير الأدبيات الاقتصادية والتقنية إلى أن الذكاء الاصطناعي سيحدث أثراً اقتصادياً واسع النطاق خلال العقد الجاري، سواء من حيث تعزيز الإنتاجية أو إعادة هيكلة سلاسل القيمة في القطاعات الحساسة، وعلى رأسها القطاع المالي (Central Bank of Kuwait, 2024). كما توضح تقارير الصناعة أن تبني الأتمتة الذكية في العمليات المصرفية يسهم في خفض تكاليف الحوادث الأمنية وتقليل زمن الاكتشاف والاستجابة، وهو ما ينعكس إيجاباً على الاستقرار المالي وتقليل الخسائر الناجمة عن خروقات البيانات (IBM, 2024).

وفي المقابل، شهدت بيئة التهديدات تطوراً نوعياً تمثل في تصاعد الهجمات الهجينة التي تدمج بين الاختراق السيبراني والاستهداف المادي، إضافة إلى توظيف تقنيات التزييف العميق والهندسة الاجتماعية المدعومة بالذكاء الاصطناعي في عمليات الاحتيال المالي (Frontiers in Artificial Intelligence, 2024). ويؤكد ذلك الحاجة إلى نماذج أمنية هجينة (Human-AI Hybrid) تجمع بين الكفاءة الحسابية للأنظمة الذكية والحكم المهني البشري، بما يضمن تحقيق توازن بين الدقة التشغيلية ومتطلبات الامتثال والخصوصية (Rand Corporation, 2023).

وعلى المستوى الوطني، يتسق هذا التحول مع توجهات رؤية المملكة العربية السعودية 2030 التي تضع التحول الرقمي والأمن السيبراني ضمن أولوياتها الاستراتيجية لتعزيز تنافسية الاقتصاد الوطني. وقد أظهرت تقارير حديثة تنامياً في جاهزية المؤسسات السعودية لتبني تطبيقات الذكاء الاصطناعي، مع تفاوت في مستويات النضج التقني والبنية التحتية الداعمة (Cisco, 2025). وفي هذا الإطار، يُعد البنك الوطني العربي (anb) نموذجاً مصرفياً فاعلاً في تبني مبادرات التحول الرقمي وتعزيز قدراته التقنية والأمنية، حيث يعمل على تطوير البنية التشغيلية لمراكز العمليات الأمنية وتكاملها مع منصات تحليلية متقدمة (Arab National Bank, 2024). كما تعكس شراكاته الاستراتيجية، ومن أبرزها التعاون مع IBM لتوظيف منصات الذكاء الاصطناعي والتحليلات المتقدمة في مكافحة الاحتيال وحماية المعاملات المصرفية، التزام البنك بتبني أحدث التقنيات لتعزيز الأمن والموثوقية في خدماته (Retail Banker International, 2025). الأمر الذي يجعل البنك الوطني العربي حالة دراسية ملائمة لتحليل الأثر الفعلي لتطبيقات الذكاء الاصطناعي في بيئة مصرفية سعودية واقعية.

وانطلاقاً من ذلك، تنبع أهمية هذه الدراسة من الحاجة إلى تقييم علي ميداني لمدى تأثير تقنيات الذكاء الاصطناعي في كفاءة أداء غرف التحكم الأمنية داخل بيئة مصرفية سعودية، وقياس انعكاساتها على مؤشرات الأداء الرئيسية مثل دقة الكشف، ومتوسط زمن الاكتشاف (MTTD)، ومتوسط زمن الاستجابة (MTTR)، فضلاً عن مستوى الامتثال التنظيمي. وتسعى الدراسة إلى بناء نموذج تحليلي يفسر العلاقة بين تبني تقنيات الذكاء الاصطناعي وتحسين الأداء الأمني، بالاعتماد على استبانة كأداة رئيسية لجمع البيانات من عينة الدراسة، بما يسهم في تقديم إطار استراتيجي متكامل يدعم اتخاذ القرار في المؤسسات المالية السعودية.

## 1.2. مشكلة الدراسة

يشهد القطاع المصرفي تحولاً متسارعاً في بنيته الأمنية نتيجة التوسع في تبني الذكاء الاصطناعي، مما أعاد تعريف دور غرف التحكم الأمنية من المراقبة التقليدية إلى النماذج التنبؤية القادرة على استباق المخاطر. إلا أن هذا التحول يواجه تحديات تتعلق بمدى فعالية هذه التقنيات في تحسين مؤشرات الأداء الأمني (Kovačević et al., 2024).

وعلى الرغم من قدرة الذكاء الاصطناعي على تقليل زمن اكتشاف الحوادث وخفض التكاليف، تشير التقارير إلى استمرار فجوة بين الإمكانيات النظرية للتقنيات الذكية ومستوى الاستفادة الفعلية منها في المؤسسات المالية (IBM, 2024). ويتزامن

ذلك مع تصاعد الهجمات الهجينة واستخدام تقنيات التزييف العميق، مما يزيد الضغوط على غرف التحكم التي تعتمد على التدخل البشري في تحليل كميات هائلة من التنبهات اليومية (Frontiers in Artificial Intelligence, 2024).

وفي السياق السعودي، تتعاضد أهمية الموضوع في ظل رؤية 2030 التي تؤكد على الأمن السيبراني كركيزة لاستقرار النظام المالي، غير أن تقارير الجاهزية تشير لتفاوت في النضج المؤسسي والقدرة على استيعاب تطبيقات الذكاء الاصطناعي (Cisco, 2025). كما تفرض البيئة التنظيمية متطلبات دقيقة حول شفافية القرارات المؤتمتة ومساءلة الخوارزميات (Rand Corporation, 2023).

أما على المستوى المؤسسي، فيعد البنك الوطني العربي نموذجاً مصرفياً يتبنى التحول الرقمي وتطوير مراكز العمليات الأمنية، إلا أنه يواجه تساؤلات جوهرية حول مدى تحقيق تقنيات الذكاء الاصطناعي لأهدافها في تحسين سرعة الاستجابة ودقة التحليل والامتثال التنظيمي. وتكتسب هذه التساؤلات أهمية خاصة في ضوء الاعتماد على الاستبانة كأداة رئيسية لاستقصاء آراء القادة الأمنيين والمحللين والخبراء حول هذه القضايا.

من هنا تبرز الحاجة لدراسة تطبيقية تقيس أثر الذكاء الاصطناعي على أداء غرف التحكم الأمنية في البنك الوطني العربي باستخدام استبانة تصمم خصيصاً لهذا الغرض، لينطلق السؤال الرئيس: ما طبيعة وقوة تأثير تطبيق تقنيات الذكاء الاصطناعي على كفاءة أداء غرف التحكم الأمنية في البنك الوطني العربي من حيث سرعة الاستجابة ودقة التحليل والامتثال التنظيمي؟

**1.3. أهمية الدراسة:** تسهم الدراسة في دعم رؤية 2030 بتقديم رؤية تطبيقية لتعزيز الأمن السيبراني في القطاع المصرفي، مما يدعم هيئات التنظيم كالهيئة الوطنية للأمن السيبراني والبنك المركزي السعودي، ويعزز جاهزية المملكة بمؤشرات الأمن السيبراني العالمية للانتقال إلى أمن نحو الاقتصاد الرقمي.

**1.3.1. على المستوى النظري:** تساهم الدراسة في إثراء البناء المعرفي من خلال تأصيل مفاهيم "الأمن التنبئي" و"الأتمتة الدفاعية" في السياق المصرفي العربي (Central Bank of Kuwait, 2024). كما تسعى لتطوير إطار نظري يوضح علاقة تقنيات الذكاء الاصطناعي بمتغيرات الأداء الأمني مثل دقة الكشف وزمن الاستجابة والامتثال التنظيمي (كامل، 2024). فضلاً عن سد الفجوة البحثية المحلية بتوفير مرجع أكاديمي يركز على البيئة المصرفية السعودية (Sidra Capital, 2024).

**1.3.2. على المستوى التطبيقي:** تنعكس نتائج الدراسة مباشرة على ممارسات البنك الوطني العربي عبر تزويد صناع القرار ببيانات دقيقة تستند إلى نتائج الاستبانة حول قدرة الذكاء الاصطناعي على تحسين الأداء الأمني. كما تساعد في توجيه استراتيجيات الاستثمار التقني نحو الأدوات ذات الأثر الأمني الأعلى، وتعزيز الامتثال لضوابط البنك المركزي السعودي والهيئة الوطنية للأمن السيبراني (Arab National Bank, 2024). بالإضافة إلى تحديد المهارات الحرجة اللازمة لتطوير رأس المال البشري في غرف التحكم الأمنية (Cisco, 2025).

#### 1.4. أسئلة الدراسة

انطلاقاً من مشكلة الدراسة، تسعى هذه الدراسة إلى الإجابة عن مجموعة من التساؤلات التي تستهدف الكشف عن طبيعة العلاقة بين مستوى تبني تقنيات الذكاء الاصطناعي وكفاءة الأداء الأمني في البنك الوطني العربي، وذلك من خلال تصميم وتوزيع استبانة على المعنيين.

**أولاً: السؤال الرئيس للدراسة:** ما طبيعة وقوة تأثير تطبيق تقنيات الذكاء الاصطناعي على كفاءة أداء غرف التحكم الأمنية في البنك الوطني العربي، من حيث سرعة الاستجابة، ودقة التحليل، ومستوى الامتثال التنظيمي؟

#### ثانياً: التساؤلات الفرعية

1. ما مستوى تبني تقنيات الذكاء الاصطناعي (الرؤية الحاسوبية، تعلم الآلة والتحليلات التنبؤية، ومعالجة اللغات الطبيعية) في غرف التحكم الأمنية بالبنك الوطني العربي من وجهة نظر العينة؟
2. ما أثر تطبيق نماذج تعلم الآلة والتحليلات التنبؤية في خفض متوسط زمن الاكتشاف (MTTD) ومتوسط زمن الاستجابة (MTTR) للحوادث الأمنية؟
3. ما تأثير تقنيات الرؤية الحاسوبية في تحسين دقة اكتشاف التهديدات المادية وتقليل معدلات الإنذارات الكاذبة؟
4. ما العلاقة بين استخدام تقنيات معالجة اللغات الطبيعية وتحليل سجلات الأمن السيبراني وتعزيز سرعة الاستجابة للحوادث؟
5. ما تأثير تقنيات الذكاء الاصطناعي على مستوى الامتثال التنظيمي لمتطلبات الجهات الرقابية في غرف التحكم الأمنية؟

6. ما أبرز التحديات التقنية والبشرية والتنظيمية التي تحد من فعالية توظيف الذكاء الاصطناعي في غرف التحكم الأمنية

بالبنك؟

## 1.5. أهداف الدراسة

تسعى هذه الدراسة إلى تحقيق هدف رئيس يتمثل في قياس تأثير تطبيق تقنيات الذكاء الاصطناعي على كفاءة أداء غرف التحكم الأمنية في البنك الوطني العربي، وذلك من خلال تصميم استبانة وتوزيعها على عينة من القادة الأمنيين ومديري غرف التحكم ومحللي العمليات الأمنية وخبراء تقنية المعلومات. ويتفرع عن هذا الهدف الرئيس مجموعة من الأهداف الفرعية:

1. تشخيص واقع تبني تقنيات الذكاء الاصطناعي في غرف التحكم الأمنية بالبنك الوطني العربي، من خلال تحديد مستوى استخدام الرؤية الحاسوبية، وتعلم الآلة والتحليلات التنبؤية، ومعالجة اللغات الطبيعية في العمليات الأمنية، بالاعتماد على استجابات عينة الدراسة.

2. قياس تأثير تقنيات تعلم الآلة والتحليلات التنبؤية في تحسين متوسط زمن الاكتشاف (MTTD) ومتوسط زمن الاستجابة (MTTR) للحوادث الأمنية، وفقاً لتقديرات العينة المستجيبة.

3. تحليل دور تقنيات الرؤية الحاسوبية في تحسين دقة اكتشاف التهديدات المادية وتقليل معدلات الإنذارات الكاذبة داخل غرف التحكم.

4. اختبار العلاقة بين توظيف تقنيات معالجة اللغات الطبيعية في تحليل السجلات الأمنية وتعزيز سرعة الاستجابة للحوادث والتهديدات السيبرانية.

5. قياس تأثير تقنيات الذكاء الاصطناعي على مستوى الامتثال التنظيمي في غرف التحكم الأمنية بالبنك الوطني العربي من خلال مؤشرات الالتزام بسياسات البنك المركزي، ووضوح آلية التبعية والمسائلة، وقابلية تفسير قرارات الأنظمة الذكية.

6. تحديد أبرز التحديات التقنية والبشرية والتنظيمية التي تواجه تطبيق تقنيات الذكاء الاصطناعي في غرف التحكم الأمنية، كما تعكسها آراء المستجيبين، وذلك باستخدام الإحصاء الوصفي.

7. تقديم توصيات عملية لتعزيز فعالية توظيف الذكاء الاصطناعي في غرف التحكم الأمنية بالبنك الوطني العربي، بناءً على نتائج تحليل الاستبانة.

## 1.6. فرضيات الدراسة

استناداً إلى النموذج الهيكلي المقترح للدراسة، وفي ضوء الاعتماد على الاستبانة كأداة رئيسية لجمع البيانات واختبار هذه الفرضيات إحصائياً، تتمثل فرضيات الدراسة فيما يلي:

### الفرضية الرئيسية:

يوجد تأثير ذو دلالة إحصائية لتقنيات الذكاء الاصطناعي بأبعادها (الرؤية الحاسوبية، وتعلم الآلة والتحليلات التنبؤية، ومعالجة اللغات الطبيعية) على كفاءة أداء غرف التحكم الأمنية بأبعادها (سرعة الاستجابة، ودقة التحليل، ومستوى الامتثال التنظيمي) في البنك الوطني العربي.

### الفرضيات الفرعية:

- الفرضية الأولى: يوجد تأثير ذو دلالة إحصائية لتطبيق نماذج تعلم الآلة والتحليلات التنبؤية على خفض متوسط زمن الاكتشاف (MTTD) ومتوسط زمن الاستجابة (MTTR) في غرف التحكم الأمنية.
- الفرضية الثانية: يوجد تأثير ذو دلالة إحصائية لتقنيات الرؤية الحاسوبية في تحسين دقة اكتشاف التهديدات المادية وتقليل معدلات الإنذارات الكاذبة.
- الفرضية الثالثة: يوجد تأثير ذو دلالة إحصائية لاستخدام تقنيات معالجة اللغات الطبيعية في تحليل السجلات الأمنية على سرعة الاستجابة للحوادث السيبرانية.
- الفرضية الرابعة: يوجد تأثير ذو دلالة إحصائية لتقنيات الذكاء الاصطناعي على مستوى الامتثال التنظيمي في غرف التحكم الأمنية.
- الفرضية الخامسة: توجد فروق ذات دلالة إحصائية في تقديرات أفراد العينة لتأثير الذكاء الاصطناعي على أداء غرف التحكم تعزى إلى المتغيرات الديموغرافية (المسمى الوظيفي، سنوات الخبرة، المؤهل العلمي).

## 1.7. نموذج الدراسة

يعكس نموذج الدراسة العلاقة بين المتغير المستقل "تقنيات الذكاء الاصطناعي" (الرؤية الحاسوبية، تعلم الآلة والتحليلات التنبؤية، معالجة اللغات الطبيعية) والمتغير التابع "أداء غرف التحكم الأمنية" (سرعة الاستجابة، دقة التحليل، الامتثال التنظيمي). يفترض النموذج تأثيراً مباشراً يُختبر بالانحدار المتعدد، وتُقاس المتغيرات باستبانة وفق مقياس ليكرت الخماسي.



## 1.8. الدراسة الميدانية (نطاق الدراسة)

تحدد حدود هذه الدراسة لضمان دقة النتائج وقابليتها للتطبيق في بيئة واقعية، مع التركيز على تصميم وتوزيع استبانة تغطي النطاقات المحددة، كما يلي:

- **النطاق المكاني:** تُجرى الدراسة في البنك الوطني العربي (anb) بفروعه الرئيسية ومركز العمليات الأمنية (SOC) المركزي في مدينة الرياض، مع إمكانية توسيع العينة لتشمل عينة ممثلة من فروعها الرئيسية في جدة والمنطقة الشرقية لضمان تعميم النتائج على مستوى البنك. وسيتم توزيع الاستبانة إلكترونياً وورقياً على المستهدفين في هذه المواقع.

- **النطاق البشري:** تستهدف الدراسة القادة الأمنيين، مديري غرف التحكم، محللي العمليات الأمنية (SOC Analysts)، وخبراء تقنية المعلومات والذكاء الاصطناعي المنخرطين بشكل مباشر في إدارة المنظومات الأمنية بالبنك. وستوجه إليهم استبانة الدراسة لجمع البيانات اللازمة.
- **النطاق الموضوعي:** يقتصر البحث على دراسة تأثير تقنيات الذكاء الاصطناعي ممثلة في: تعلم الآلة والتحليلات التنبؤية، والرؤية الحاسوبية، ومعالجة اللغات الطبيعية على أداء غرف التحكم الأمنية، مع التركيز على مؤشرات سرعة الاستجابة ودقة التحليل والامتثال التنظيمي.
- **النطاق الزمني:** تغطي الدراسة التطورات التقنية والأبحاث المنشورة في الفترة ما بين (2020 – 2025)، مع تركيز خاص على أحدث الابتكارات في عامي 2024 و2025. كما سيتم توزيع الاستبانة وجمع البيانات خلال الفصل الدراسي الحالي.

## 1.10. مصطلحات الدراسة

تتضمن الدراسة مصطلحات علمية لفهم علاقة الذكاء الاصطناعي بأداء غرف التحكم الأمنية بالقطاع المصرفي، صيغت نظرياً من الأدبيات وإجرائياً وفق سياق البنك الوطني العربي:

### 2. الذكاء الاصطناعي (Artificial Intelligence – AI)

- **التعريف النظري:** هو مجموعة من الأنظمة والتقنيات البرمجية القادرة على محاكاة القدرات الذهنية البشرية، وتتميز بالقدرة على اتخاذ القرارات، وتوليد المحتوى، وتقديم التوصيات، أو القيام بالتنبؤات بناءً على مستويات متفاوتة من الاستقلالية (SDAIA, 2025).

- **التعريف الإجرائي:** هو حزمة البرمجيات والخوارزميات المستخدمة في غرف التحكم بالبنك الوطني العربي (مثل منصات IBM Watson) لتحليل البيانات الأمنية والمالية وكشف أنماط الاحتيال آلياً.

### 3. الذكاء الاصطناعي الوكيل (Agentic AI)

- **التعريف النظري:** هو جيل متطور من أنظمة الذكاء الاصطناعي يتجاوز مجرد الاستجابة للأوامر، حيث يمتلك القدرة على إدراك البيئة المحيطة، وتفسير المعلومات، وتحديد الأهداف، وتنفيذ مهام معقدة متعددة الخطوات بشكل مستقل أو بإشراف بشري محدود (SDAIA, 2025; Srinivas et al., 2025).

- **التعريف الإجرائي:** هو استخدام "وكلاء أذكاء" داخل مركز العمليات الأمنية بالبنك للقيام بعمليات التحقيق الأولية في التنبيهات وعزل التهديدات السيبرانية دون الحاجة لتدخل مباشر من المحلل في كل خطوة.

#### 4. رفة التحكم الأمنية (Security Control Room)

- **التعريف النظري:** هي منشأة مركزية مجهزة تقنياً لمراقبة وتأمين المواقع، تهدف إلى الكشف عن الأعمال غير القانونية وردع الجرائم لتعزيز السلامة العامة، وتعتمد في عملها على دمج بيانات الكاميرات وحساسات الدخول ( Baker & Benny, 2012; Reynaud & Untersinger, 2024 ).

- **التعريف الإجرائي:** هي المركز الفني المسؤول عن مراقبة الفروع المادية للبنك الوطني العربي وأجهزة الصراف الآلي عبر أنظمة الرؤية الحاسوبية والتحقق من هويات الداخلين.

#### 5. مركز العمليات الأمنية (Security Operations Center – SOC)

- **التعريف النظري:** هو مركز عمليات مركزي يعمل كعصب دفاعي للمؤسسة، يهدف إلى اكتشاف التهديدات، والاستجابة للحوادث، ومنع وقوعها من خلال تنسيق وتكامل جميع التقنيات الأمنية والعمليات والكوادر البشرية ( Khayat et al., 2025 ).

- **التعريف الإجرائي:** هو الفريق التقني في البنك الوطني العربي المسؤول عن إدارة التهديدات السيبرانية التي تستهدف البنية التحتية الرقمية والحسابات المصرفية على مدار الساعة.

#### 6. إرهاق التنبيهات (Alert Fatigue)

- **التعريف النظري:** هي حالة نفسية وتشغيلية تصيب محللي الأمن، حيث يفقدون الحساسية تجاه الإنذارات نتيجة الحجم الهائل من التنبيهات وارتفاع نسب الإنذارات الكاذبة (أكثر من 50%)، مما يؤدي إلى إغفال تهديدات حقيقية (Mandadi, 2025; CyberDefenders, 2026).

- **التعريف الإجرائي:** هو الضغط المعرفي الذي يواجهه محللو البنك الوطني العربي نتيجة التعامل مع مئات التنبيهات اليومية الناتجة عن أنظمة SIEM التقليدية.

#### 7. التحليلات التنبؤية (Predictive Analytics)

- **التعريف النظري:** هي عملية استخدام البيانات التاريخية، والخوارزميات الإحصائية، وتقنيات التعلم الآلي لتحديد أنماط السلوك والتنبؤ بالتهديدات أو النتائج المستقبلية قبل وقوعها (Group-IB, 2025; Kovačević et al., 2024).
- **التعريف الإجرائي:** هي النماذج الرياضية التي يطبقها البنك لاستباق عمليات الاختراق أو الاحتيال المالي بناءً على تحليل السلوك التاريخي للعملاء والمهاجمين.

#### 8. الرؤية الحاسوبية (Computer Vision)

- **التعريف النظري:** هي أحد فروع الذكاء الاصطناعي التي تمكن الحواسيب من استخلاص معلومات عالية المستوى وفهم محتوى الصور الرقمية ومقاطع الفيديو، لمحاكاة حاسة البصر البشرية في التعرف على الوجوه واكتشاف الأجسام (Microsoft, 2026; Reynaud & Untersinger, 2024).
- **التعريف الإجرائي:** هي التقنية المستخدمة في كاميرات المراقبة بالبنك الوطني العربي للتعرف التلقائي على الموظفين، وكشف محاولات التسلل، وتحليل تدفق العملاء داخل الفروع.

#### 9. معالجة اللغات الطبيعية (Natural Language Processing – NLP)

- **التعريف النظري:** هي تقنية تتيح للحواسيب فهم وتفسير وتوليد اللغة البشرية، وتُستخدم في الأمن لتلخيص سجلات النشاط المعقدة وتحليل تقارير الاستخبارات الأمنية غير المهيكلية (Allen et al., 2022; Srinivas et al., 2025).
- **التعريف الإجرائي:** هي الأدوات المستخدمة داخل البنك لتحويل آلاف السجلات النصية (Logs) إلى ملخصات مفهومة تساعد المحللين في اتخاذ قرارات سريعة.

#### 10. الكفاءة التشغيلية (Operational Efficiency)

- **التعريف النظري:** هي قدرة غرفة التحكم على إدارة مشهد التهديدات المتسع بأقل الموارد الممكنة، وتُقاس من خلال تقليل متوسط زمن الاكتشاف (MTTD) ومتوسط زمن الاستجابة (MTTR) وزيادة دقة الأداء (Vectra AI, 2025; Taqafi et al., 2023).
- **التعريف الإجرائي:** هي مستوى التحسن في سرعة إغلاق التذاكر الأمنية في البنك الوطني العربي وانخفاض التكاليف الناتجة عن الحوادث الأمنية بعد تبني الذكاء الاصطناعي.

## 11. الامتثال التنظيمي (Regulatory Compliance)

- **التعريف النظري:** هو الالتزام بالمتطلبات والمعايير التي تضعها الجهات الرقابية، والتي تشمل ضوابط الحوكمة، وحماية البيانات الشخصية، وإجراءات الاستجابة للحوادث لضمان استقرار النظام المالي ( SAMA, 2024; Rand Corporation, 2023).
- **التعريف الإجرائي:** هو مدى توافق أنظمة الذكاء الاصطناعي في البنك الوطني العربي مع "إطار الأمن السيبراني" الصادر عن البنك المركزي السعودي (SAMA) وسياسات الهيئة الوطنية للأمن السيبراني.

## 1.9. هيكل الدراسة

يتكون المشروع البحثي من خمسة فصول مترابطة؛ يقدم الفصل الأول الإطار العام للدراسة متضمناً المقدمة، مشكلة الدراسة، الأهمية، الأسئلة، الأهداف، الفرضيات، ونموذج الدراسة. ويعرض الفصل الثاني الدراسات السابقة والإطار النظري من خلال مراجعة أدبيات الذكاء الاصطناعي في الأمن المصرفي وغرف التحكم، بما يؤسس لبناء الاستبانة. ويتناول الفصل الثالث منهجية الدراسة موضحاً الفلسفة الوضعية، المنهج الاستنتاجي، تصميم البحث، مجتمع وعينة الدراسة، وإجراءات تصميم وتطوير الاستبانة واختبار صدقها وثباتها، مع استخدام برنامج SPSS، وقياس الامتثال التنظيمي بمقياس ليكرت، وتحليل التحديات بالإحصاء الوصفي. ويخصص الفصل الرابع للتحليل الإحصائي ومناقشة النتائج عبر عرض نتائج الاستبانة، واختبار الفرضيات بالانحدار المتعدد وتحليل التباين (ANOVA)، ومناقشتها في ضوء الأدبيات. ويختتم الفصل الخامس الدراسة بالخاتمة والتوصيات متضمناً أبرز الاستنتاجات، حدود الدراسة، وتوصيات عملية تستند إلى نتائج الاستبانة.

## الفصل الثاني: الإطار النظري للدراسة

تمهيد

المبحث الأول: الدراسات السابقة

2.1.1 الدراسات العربية

2.1.2 الدراسات الأجنبية

2.1.3 التعقيب على الدراسات السابقة

المبحث الثاني: الإطار النظري

2.2.1 الأسس النظرية والتقنية للذكاء الاصطناعي في المجال الأمني

2.2.2. غرف التحكم الأمنية ومراكز العمليات الأمنية (SOC)

2.2.3 تكامل الذكاء الاصطناعي في غرف التحكم الأمنية

2.2.4 الأبعاد التنظيمية والبشرية لتوظيف الذكاء الاصطناعي في الأمن المصرفي

2.2.5 الذكاء الاصطناعي في القطاع المصرفي السعودي

خلاصة الفصل

## تمهيد

يشكل هذا الفصل الركيزة المعرفية والمنهجية التي تستند إليها الدراسة الحالية، حيث يسعى إلى بناء فهم متكامل وعميق للعلاقة بين تقنيات الذكاء الاصطناعي وكفاءة أداء غرف التحكم الأمنية في القطاع المصرفي السعودي. وينقسم الفصل إلى مبحثين رئيسيين؛ يختص أولهما باستعراض وتحليل "الدراسات السابقة" العربية والأجنبية، بهدف استخلاص أهم النتائج والمنهجيات التي توصل إليها الباحثون في المجال، وتحديد موقع هذه الدراسة ضمن الخريطة البحثية، والفجوة المعرفية التي تسعى لسدها من خلال تطبيقها على البنك الوطني العربي (anb). أما المبحث الثاني، فيتناول "الإطار النظري" للدراسة، من خلال تأصيل المفاهيم الأساسية للذكاء الاصطناعي وتقنياته الفرعية (تعلم الآلة، الرؤية الحاسوبية، معالجة اللغات الطبيعية)، وبيان دورها في تطوير آليات العمل داخل غرف التحكم ومراكز العمليات الأمنية (SOC). كما يناقش هذا المبحث الأبعاد التنظيمية والبشرية المرتبطة بهذا التحول التقني، ويسلط الضوء على واقع تبني الذكاء الاصطناعي في البنوك السعودية بشكل عام، والبنك الوطني العربي (anb) بشكل خاص، وصولاً إلى بناء نموذج مقترح يربط بين متغيرات الدراسة المستقلة والتابعة، ليكون بمثابة الخريطة التحليلية التي توجه عملية جمع البيانات الميدانية وتحليلها في الفصول اللاحقة.

## المبحث الأول: الدراسات السابقة

تستعرض هذه الفقرة أهم الأدبيات العربية والأجنبية التي تناولت تقنيات الذكاء الاصطناعي ودورها في تطوير المنظومات الأمنية والمالية. يهدف هذا العرض إلى تحليل المنهجيات والنتائج السابقة المتعلقة بأداء غرف التحكم ومراكز العمليات الأمنية (SOC)، مما يساعد في تأصيل المتغيرات البحثية الحالية (الرؤية الحاسوبية، تعلم الآلة، ومعالجة اللغات الطبيعية) وتحديد الفجوة العلمية التي تسعى هذه الدراسة لسدها بالتطبيق على البنك الوطني العربي.

### 2.1.1 الدراسات العربية

1. دراسة (السقاط والسقاف) بتاريخ (2025) بعنوان: "تأثير الذكاء الاصطناعي على إدارة المخاطر في البنوك السعودية

دراسة استطلاعية لأراء عينة من موظفي البنوك في مدينة جدة".

هدفت الدراسة إلى تحليل تبني البنوك السعودية لتقنيات الذكاء الاصطناعي في إدارة المخاطر، وأثر ذلك على الاستراتيجيات الأمنية والتشغيلية. استخدمت المنهج الوصفي التحليلي عبر استبانة وزعت على (350) موظفاً في البنوك بمدينة جدة. توصلت النتائج إلى أن الذكاء الاصطناعي يعزز سرعة التنبؤ بالمخاطر ودقة القرارات. وأوصت الدراسة بتكثيف الاستثمارات

التقنية وتدريب الكوادر البشرية. تشابهت مع بحثنا في التركيز على القطاع المصرفي السعودي واستخدام الاستبانة، واختلفت في تناولها العام لإدارة المخاطر، بينما يركز بحثنا على غرف التحكم الأمنية وتأثير التقنيات على أدائها الميداني والرقابي.

2. دراسة (الراحله) بتاريخ (2025) بعنوان: "دور الذكاء الاصطناعي في تعزيز الامتثال لإدارة مخاطر الأمن السيبراني".

سعت الدراسة لاستكشاف كيفية مساهمة دمج الذكاء الاصطناعي في أطر الأمن السيبراني في تحسين الكشف عن التهديدات والاستجابة لها. اعتمدت على المنهج الوصفي لتحليل الأطر التنظيمية والتقنية، وخلصت إلى أن الأنظمة الذكية ترفع مستوى الامتثال للمعايير الرقابية عبر أتمتة الرقابة وتقليل الخطأ البشري. أوصت بتطوير سياسات أمنية مرنة تتماشى مع تطور الذكاء الاصطناعي التوليدي. تتفق مع بحثنا في التركيز على "الامتثال التنظيمي"، وتختلف في كونها دراسة نظرية تأصيلية، بينما يتجه بحثنا للتطبيق الميداني على البنك الوطني العربي لقياس الأثر الفعلي داخل غرف العمليات.

3. دراسة (كامل) بتاريخ (2025) بعنوان: "استخدام الذكاء الاصطناعي في مجالات الأمن والمراقبة: تحليل الممارسات الدولية واستشراف التحديات المستقبلية".

هدفت الدراسة لتحليل دور الذكاء الاصطناعي في تعزيز أنظمة الأمن والمراقبة عبر مراجعة الممارسات الدولية الرائدة (الولايات المتحدة، الصين، الإمارات). استخدمت المنهج الوصفي التحليلي لاستعراض تجارب هذه الدول في تطبيقات الرؤية الحاسوبية والتحليلات التنبؤية. توصلت إلى أن الذكاء الاصطناعي يرفع كفاءة المنظومات الأمنية عبر سرعة تحليل البيانات الضخمة من كاميرات المراقبة، ولكنه يواجه تحديات تتعلق بالخصوصية والأخلاقيات. أوصت بوضع أطر قانونية تنظم استخدام هذه التقنيات لتحقيق التوازن بين الفعالية الأمنية وحقوق الأفراد. تشابهت مع دراستنا في تناول "الرؤية الحاسوبية" وأدوات المراقبة الذكية، واختلفت في كونها دراسة مقارنة دولية، بينما يركز بحثنا على حالة تطبيقية محلية في بيئة مصرفية سعودية محددة.

4. دراسة (قاسم) بتاريخ (2024) بعنوان: "دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية دراسة مقارنة".

تناولت الدراسة دور التقنيات الذكية في الحد من الجرائم السيبرانية التي تهدد المؤسسات المالية، مع التركيز على السلطات الرقمية والتنبؤ بالجريمة. اعتمدت على المنهج المقارن بين التشريعات العربية والدولية، وتوصلت إلى أن الذكاء الاصطناعي يشكل حاجز صد منيع ضد الاختراقات بفضل قدرته على تحليل الأنماط غير الطبيعية في تدفق البيانات. أوصت بتحديث

القوانين للاعتراف بالأدلة الرقمية المستخرجة عبر الذكاء الاصطناعي. تتشابه مع بحثنا في التركيز على أمن البيانات ومكافحة التهديدات، وتختلف في بعدها القانوني والتشريعي، بينما يركز بحثنا على الجوانب التشغيلية والإدارية لغرف التحكم الأمنية وتأثير التقنية على سرعة الاستجابة.

#### 5. دراسة (البابلي) بتاريخ (2021) بعنوان: "دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة".

ركزت الدراسة على القدرات الاستباقية للذكاء الاصطناعي في غرف العمليات والتحكم، ودور الخوارزميات في توقع الحوادث الأمنية بناءً على البيانات التاريخية. استخدمت المنهج الوصفي التحليلي لاستعراض تجارب ناجحة في "الأمن التنبؤي". توصلت النتائج إلى أن التحليلات التنبؤية تقلل زمن الاستجابة وتساعد في توزيع الموارد الأمنية بشكل أكثر ذكاءً. أوصت الدراسة بدمج أنظمة الذكاء الاصطناعي في مراكز العمليات الأمنية (SOC) لتقليل الاعتماد على المراقبة البشرية التقليدية. تشابهت مع دراستنا في التركيز على "التحليلات التنبؤية" وتأثيرها على غرف التحكم، وتميزت دراستنا بتطبيق هذا المفهوم في "القطاع المصرفي" الذي يتسم بحساسية عالية تجاه المخاطر المالية.

#### 6. دراسة (الغامدي) بتاريخ (2022) بعنوان: "سلسلة الأدلة الإرشادية للهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)".

هدفت الدراسة الإرشادية إلى وضع معايير وطنية لاستخدام الذكاء الاصطناعي في المملكة لتعزيز الأمن الرقمي والوطني. استخدمت المنهج المعياري لتحديد أفضل الممارسات في حوكمة البيانات واستخدام الخوارزميات في القطاعات الحساسة. توصلت إلى أهمية وجود ضوابط صارمة لضمان موثوقية الأنظمة الذكية وقابلية تفسير قراراتها. أوصت الدراسة بإلزام الجهات الحكومية والخاصة (بما فيها البنوك) بهذه المعايير لضمان التحول الآمن نحو الاقتصاد الرقمي. تشابهت مع بحثنا في النطاق الوطني السعودي والارتباط برؤية 2030، واختلفت في كونها إطاراً تنظيمياً عاماً، بينما يمثل بحثنا دراسة حالة تطبيقية تقيس فاعلية هذه التقنيات في تحسين الأداء الأمني للبنك الوطني العربي.

## 2.1.2 الدراسات الأجنبية

1. دراسة (Khayat et al). بتاريخ (2025) بعنوان: "تمكين مراكز العمليات الأمنية (SOC) بالذكاء الاصطناعي وتعلم

الآلة: مراجعة منهجية للأدبيات".

هدفت هذه الدراسة الشاملة إلى تقييم مدى قدرة الذكاء الاصطناعي على ثورة أداء مراكز العمليات الأمنية عبر تحسين قدرات تحديد التهديدات والاستجابة الاستباقية. استخدمت الدراسة المنهج المسحي (Systematic Review) لتحليل مئات الأبحاث المنشورة مؤخراً، وتوصلت إلى أن دمج تعلم الآلة في غرف التحكم يقلل من متوسط زمن الاكتشاف (MTTD) بشكل كبير عبر أتمتة المهام الروتينية. وأوصت الدراسة بتبني نماذج "الاستقلال الموثوق" التي تمنح الأنظمة الذكية قدرة أكبر على اتخاذ قرارات دفاعية مستقلة تحت إشراف بشري. وتشابهت مع بحثنا في التركيز على مراكز العمليات الأمنية (SOC) كمتغير تابع، بينما تميزت دراستنا بكونها طبقت هذه المفاهيم في "البنك الوطني العربي" كدراسة حالة سعودية، مما يمنحها خصوصية ثقافية وتنظيمية.

2. دراسة (Srinivas et al). بتاريخ (2025) بعنوان: "مراكز العمليات الأمنية المعززة بالذكاء الاصطناعي: مسح حول

النماذج اللغوية والوكلاء للأتمتة الأمنية".

سعت هذه الدراسة إلى استكشاف تأثير "الذكاء الاصطناعي الوكيل" (Agentic AI) في أتمتة العمليات الأمنية داخل غرف التحكم. اعتمدت الدراسة على المنهج التحليلي لنماذج تطبيقية في شركات تقنية كبرى، وخلصت إلى أن الوكلاء الأذكاء يمكنهم القيام بعمليات التحقيق الأولي في التنبيهات، مما يقلل من ظاهرة "إجهاد التنبيهات" لدى المحللين بنسبة تتجاوز 40%. وأوصت الدراسة بضرورة تطوير واجهات تفاعل سلسلة بين المحلل البشري والوكيل الذكي. وتشابهت مع بحثنا في تناول متغير "معالجة اللغات الطبيعية" والوكلاء الأذكاء في الأمن، واختلفت في تركيزها على الجوانب البرمجية البحتة، في حين يركز بحثنا على الأثر الإداري والتنظيمي لهذا التحول في البنك الوطني العربي.

3. دراسة (Barrios-González et al). بتاريخ (2025) بعنوان: "إعادة تعريف استخبارات التهديدات السيبرانية (CTI)

باستخدام الذكاء الاصطناعي: من معالجة البيانات إلى الرؤى التنبؤية".

هدفت الدراسة إلى بيان الكيفية التي يعيد بها الذكاء الاصطناعي صياغة مفهوم "الاستخبارات الأمنية" من خلال تحويل كميات هائلة من البيانات غير المهيكلة إلى رؤى استراتيجية قابلة للتنفيذ. استخدمت الدراسة المنهج التجريبي لقياس سرعة

معالجة البيانات باستخدام خوارزميات الرؤية الحاسوبية ومعالجة اللغات الطبيعية، وتوصلت إلى أن هذه التقنيات تمنح غرف التحكم قدرة على التنبؤ بالهجمات قبل وقوعها بمدة كافية للاحتواء. وأوصت الدراسة بضرورة تكامل أنظمة الاستخبارات الخارجية مع أنظمة المراقبة الداخلية للمؤسسة. تتفق هذه الدراسة مع بحثنا في أبعاد المتغير المستقل (الرؤية الحاسوبية، تعلم الآلة، NLP)، بينما تنفرد دراستنا بقياس مدى التزام هذه الأنظمة بـ "الامتثال التنظيمي" الصادر عن البنك المركزي السعودي (SAMA).

### 2.1.3 التعقيب على الدراسات السابقة

من خلال الاستعراض التحليلي للدراسات السابقة، العربية منها والأجنبية، إلى وجود اهتمام بحثي متصاعد ومواكب للتحويلات الرقمية في القطاع المصرفي، حيث أجمعت تلك الأدبيات على الدور الجوهرى للذكاء الاصطناعي في إعادة صياغة مفاهيم الأمن والحماية؛ فبينما ركزت الدراسات العربية (مثل دراسة السقاط والسقاف، 2025؛ والراحله، 2025) على الأطر العامة لإدارة المخاطر والامتثال السيبراني في البنوك السعودية، اتجهت الدراسات الأجنبية (مثل دراسة Khayat et al., 2025؛ و Srinivas et al., 2025) نحو التعمق التقني في أتمتة مراكز العمليات الأمنية (SOC) وتوظيف الوكلاء الأذكياء والنماذج اللغوية الكبيرة. وبالرغم من ثراء هذه الجهود، إلا أن الباحث لاحظ وجود فجوة بحثية فيما يتعلق بالدراسات الميدانية التي تجمع بين "الأمن المادي" المتمثل في غرف التحكم و"الأمن الرقمي" في آن واحد، وقياس أثر تقنيات محددة كالرؤية الحاسوبية وتعلم الآلة على مؤشرات أداء دقيقة مثل (MTTD) و (MTTR) في سياق تنظيمي سعودي محكم. ومن هنا، تبرز قيمة الدراسة الحالية في كونها لا تكتفي بالتأصيل النظري، بل تسعى لتقديم رؤية تطبيقية شاملة من خلال نموذج هيكلي يربط بين المتغيرات المستقلة (الرؤية الحاسوبية، تعلم الآلة، NLP) وبين المتغيرات التابعة (سرعة الاستجابة، دقة التحليل، والامتثال التنظيمي)، مع إسقاط ذلك عملياً على البنك الوطني العربي (anb) كبيئة واقعية. وتستفيد الدراسة الحالية من قصور الدراسات السابقة في تناول متغير "الامتثال التنظيمي" لمتطلبات البنك المركزي السعودي (SAMA) وهيئة (سدأيا) كأثر مباشر لتطبيقات الذكاء الاصطناعي، مما يجعل هذه الدراسة محاولة جادة لسد هذه الفجوة وتقديم إطار استراتيجي يدعم اتخاذ القرار الأمني في المؤسسات المالية السعودية لمواجهة التهديدات الهجينة والسيبرانية المتطورة لعام 2026.

## المبحث الثاني: الإطار النظري

يعد القطاع المصرفي من أكثر القطاعات تأثراً بالثورة التكنولوجية، حيث أصبح التحول الرقمي ضرورة استراتيجية. وقد فرضت التحديات الأمنية المعقدة إعادة تشكيل المشهد الأمني بالاعتماد على الذكاء الاصطناعي، لتحويل غرف التحكم الأمنية من مراكز مراقبة سلبية إلى وحدات استباقية للتنبؤ بالتهديدات، تماشياً مع رؤية السعودية 2030 لاقتصاد رقمي آمن.

### 2.2.1 الأسس النظرية والتقنية للذكاء الاصطناعي في المجال الأمني

يعتمد الأمن المصرفي على أسس نظرية وتقنيات متطورة للذكاء الاصطناعي، ويستعرض هذا الجزء مفاهيمه الأساسية وركائزه التقنية الثلاث (تعلم الآلة، الرؤية الحاسوبية، ومعالجة اللغات الطبيعية) التي تشكل منظومة غرف التحكم الأمنية.

#### أولاً: الذكاء الاصطناعي: النشأة، المفهوم، والتطور

■ **الإطار المفاهيمي للذكاء الاصطناعي:** يعرف الذكاء الاصطناعي (AI) بأنه نظام آلي يعتمد على آليات برمجية وهياكل بيانية تمكنه من محاكاة القدرات الذهنية البشرية في التعلم والاستنتاج واتخاذ القرار (SDAIA, 2022). ووفقاً لتعريف منظمة التعاون الاقتصادي والتنمية، يمثل الذكاء الاصطناعي نظاماً قائماً على الآلة يمكنه، من أجل أهداف محددة، استنتاج مخرجات مثل التوقعات أو التوصيات أو القرارات التي تؤثر على البيانات الحقيقية أو الافتراضية (Bank for International Settlements, 2025). لقد انتقل المفهوم من مجرد "المحاكاة" للعمليات الروتينية إلى "الاستقلالية"، حيث تمتلك الأنظمة الحديثة القدرة على التكيف مع البيانات المتغيرة دون تدخل بشري مباشر مستمر. وفي السياق الأمني المصرفي، لم يعد الذكاء الاصطناعي مجرد أداة مساعدة، بل أصبح "فاعلاً" يمتلك وعياً سياقياً بالبيئة الأمنية المحيطة، مما يمكنه من التمييز بين السلوكيات الطبيعية والتهديدات الناشئة (Srinivas et al., 2025).

■ **تطور الذكاء الاصطناعي:** مر تطور الذكاء الاصطناعي في البيانات الأمنية بخمس أجيال أساسية تعكس القفزات النوعية في القدرة الحسابية (Vinay, 2026):

1. **جيل الأنظمة الخبيرة (Expert Systems):** اعتمدت على قواعد منطقية ثابتة، وكانت محدودة بالسيناريوهات التي يغذيها المبرمج مسبقاً (Splunk, 2024).

2. جيل تعلم الآلة (Machine Learning): بدأ في العقد الماضي بالتركيز على النماذج الإحصائية التي تكتشف الأنماط من البيانات التاريخية بشكل ديناميكي (Eskandarany, 2024).

3. جيل الذكاء الاصطناعي التوليدي (Generative AI): أتاح للأنظمة فهم وتوليد محتوى معقد، مما ساعد المحللين في تفسير التنبؤات الأمنية بلغة طبيعية مفهومة (Srinivas et al., 2025).

4. جيل الذكاء الاصطناعي الوكيل (Agentic AI): يمثل الذروة الحالية، حيث تتحول النماذج من "مساعد" إلى "وكيل" قادر على تحديد الأهداف، واستدعاء الأدوات الخارجية، وتنفيذ سلاسل من المهام المعقدة بشكل مستقل (ITI, 2025). يتميز "الذكاء الاصطناعي الوكيل" بقدرته على العمل في بيئات غير خاضعة للرقابة الكاملة، حيث يمكنه بناء فرضيات حول التهديدات وجمع الأدلة بشكل تلقائي، مما يقلل الفجوة الزمنية بين الاكتشاف والاستجابة (Sarrat & Gomez, 2023).

■ التصنيفات الرئيسية للذكاء الاصطناعي وتطبيقاتها: يمكن تصنيف تقنيات الذكاء الاصطناعي المستخدمة في الأمن المصرفي إلى فئات رئيسية (IBM, 2024):

1. التعلم الخاضع للإشراف (Supervised Learning): يُستخدم لتصنيف التهديدات المعروفة بناءً على بيانات موسومة مسبقاً، مثل كشف الاحتيال بناءً على أنماط تاريخية مؤكدة (Ahmad & Rahman, 2024).

2. التعلم غير الخاضع للإشراف (Unsupervised Learning): ضروري لاكتشاف التهديدات غير المعروفة أو "هجمات اليوم الصفر"، حيث يكتشف النظام الشذوذ في البيانات دون معرفة مسبقة بنوع التهديد (Bank account fraud dataset research, 2025).

3. التعلم العميق (Deep Learning): يعتمد على الشبكات العصبية الاصطناعية (ANN) لمعالجة البيانات الضخمة (Big Data) الصادرة عن الكاميرات وسجلات الشبكة بدقة تفوق القدرة البشرية (Kovačević et al., 2024).

## ثانياً: الركائز التقنية للذكاء الاصطناعي في الأنظمة الأمنية

■ تعلم الآلة والتحليلات التنبؤية: تعد التحليلات التنبؤية جوهر التحول من "الدفاع التفاعلي" إلى "الأمن الاستباقي". تعتمد هذه التقنية على خوارزميات تعلم الآلة لتحليل التدفقات الهائلة من البيانات التاريخية واللحظية لتوقع الحوادث قبل وقوعها (Olaoye & Egon, 2024). في غرف التحكم الأمنية، تعمل هذه النماذج على:

1. تقليل زمن الاكتشاف (MTTD): عبر رصد المؤشرات الضعيفة للهجوم التي قد تغيب عن المحلل البشري (ResearchGate, 2024).

2. تحليل سلوك المستخدمين والكيانات (UEBA): بناء ملف تعريف سلوكي لكل موظف و عميل، مما يسهل اكتشاف أي انحراف قد يشير إلى اختراق للحساب أو تهديد داخلي (Splunk, 2024).

لقد أثبتت الدراسات أن دمج تعلم الآلة في مراكز العمليات الأمنية (SOC) يمكن أن يقلل من أوقات الاستجابة بنسبة تصل إلى 45% (ResearchGate, 2025).

■ الرؤية الحاسوبية (Computer Vision): تمثل الرؤية الحاسوبية "أعين" المنظومة الأمنية الذكية، حيث تحول لقطات الفيديو من مجرد صور مسجلة إلى بيانات رقمية قابلة للتحليل الفوري (Meegle, 2025). وتعتمد هذه التقنية على نماذج متقدمة مثل:

1. خوارزميات YOLO و Faster R-CNN: المستخدمة للكشف الفوري عن الأجسام والوجوه وتتبع الحركات المشبوهة داخل فروع البنك أو حول أجهزة الصراف الآلي (KritiKal Solutions, 2026).

2. تحليل السلوك (Behavioral Analysis): القدرة على اكتشاف حالات التسكع، أو السلوك العدواني، أو محاولات التلاعب بأجهزة الصراف عبر تحليل لغة الجسد وأنماط الحركة (Quytech, 2025).

3. كشف الشذوذ البصري: تحديد الأشياء المتروكة (مثل الحقائب المشبوهة) أو الدخول غير المصرح به للمناطق المحظورة، مما يرفع دقة الكشف ويقلل من الإنذارات الكاذبة التي تسبب إجهاداً للمحللين (Intozi, 2025).

■ معالجة اللغات الطبيعية (Natural Language Processing): في ظل الانفجار المعلوماتي، أصبح من المستحيل على المحللين قراءة كافة سجلات النظام وتقارير التهديدات العالمية يدوياً. هنا تبرز أهمية معالجة اللغات الطبيعية (NLP) في (Chianumba et al., 2022):

1. استخراج الكيانات المسماة (NER): تحديد وسحب مؤشرات الاختراق (IOCs) مثل عناوين IP المشبوهة وأسماء البرمجيات الخبيثة من النصوص غير المهيكلة وتغذيتها تلقائياً في أنظمة الدفاع (Security Bulldog, 2025).

2. تحليل المشاعر والسياق: مراقبة الاتصالات والويب المظلم لفهم نوايا المهاجمين وتقييم مدى خطورة التهديدات المتداولة (Proofpoint, 2025).

3. أتمتة إعداد التقارير: تحويل آلاف السجلات التقنية المعقدة إلى ملخصات تنفيذية واضحة تساعد القادة الأمنيين في

اتخاذ قرارات سريعة ومبنية على حقائق (XenonStack, 2024).

إن تكامل هذه الركائز الثلاث (تعلم الآلة، الرؤية الحاسوبية، NLP) يخلق بيئة أمنية "مدركة لذاتها" قادرة على حماية الأصول المالية والمعلوماتية للبنك الوطني العربي بكفاءة تتماشى مع المعايير العالمية.

## 2.2.2. غرف التحكم الأمنية ومراكز العمليات الأمنية (SOC)

تمثل غرف التحكم ومراكز العمليات الأمنية (SOC) الدرع الدفاعي للمصارف في مواجهة التهديدات الهجينة، وقد تحول دورها من المراقبة السلبية إلى منصات ذكية قائمة على التنبؤ والاستباقية. يهدف هذا المبحث إلى تأصيل المفاهيم الهيكلية، وتحليل التحديات التشغيلية، واستشراف النماذج الهجينة التي تدمج الذكاء البشري بالقدرات الآلية.

### أولاً: غرف التحكم الأمنية: المفهوم والبنية والوظائف

■ **التعريف والغايات الاستراتيجية لغرف التحكم الأمنية في المؤسسات الحيوية:** تعرف غرفة التحكم الأمنية (SCR) بأنها منشأة مركزية مجهزة تقنيًا لإدارة وتنسيق العمليات الأمنية المادية والرقمية، وتهدف أساساً إلى حماية الأصول المادية، والموظفين، والعملاء من خلال الرصد المستمر للبيئات التشغيلية (Baker & Benny, 2012). وفي القطاع المصرفي، تتجاوز الغاية من هذه الغرف مجرد "المراقبة" لتصبح أداة استراتيجية لضمان استمرارية الأعمال وتعزيز ثقة المودعين عبر خلق بيئة آمنة للتعاملات (Meegle, 2026). تتمثل الغايات الاستراتيجية لغرف التحكم في ثلاثة محاور رئيسية (Baker & Benny, 2012; Reynaud & Untersinger, 2024):

1. **الردع (Deterrence):** من خلال الوجود التقني الظاهر الذي يقلل من احتمالية ارتكاب الجرائم المادية أو محاولات التسلل.

2. **الكشف المبكر (Early Detection):** رصد السلوكيات الشاذة في الوقت الفعلي قبل تصاعدها إلى حوادث أمنية كبرى.

3. **الاستجابة المنسقة (Coordinated Response):** العمل كمركز قيادة وسيطرة لتوجيه الفرق الميدانية وتوثيق الأدلة الرقمية لعمليات التحقيق اللاحقة.

■ البنية التحتية التكنولوجية والتشغيلية لغرف التحكم (الأمن المادي والرقمي): تعتمد غرف التحكم الحديثة على بنية تحتية متكاملة تدمج بين أنظمة الأمن المادي والأنظمة الرقمية. وتتكون هذه البنية من عدة طبقات تقنية (KritiKal Solutions, 2026; Pelco, 2025):

1. أجهزة الحافة (Edge Devices): وتشمل كاميرات المراقبة عالية الدقة، وحساسات الحركة، وأجهزة القراءة البيومترية، وأنظمة التعرف على لوحات المركبات (LPR).
2. نظم إدارة الفيديو (VMS): وهي المنصات البرمجية التي تجمع التدفقات البصرية وتعالجها، وتسمح بربطها بقواعد البيانات الأمنية للمؤسسة.
3. تكامل الأمن الهجين: يشير التوجه الحديث، كما في تجربة البنك الوطني العربي، إلى دمج الأدوات المنفصلة في منصة موحدة تتيح رؤية شاملة للمخاطر، حيث يتم ربط سجلات الدخول المادي مع الأنشطة السيبرانية على الشبكة (Trellix, 2024).

■ التحديات التشغيلية: تواجه غرف التحكم التقليدية تحديًا وجوديًا يتمثل في "إجهاد التنبيهات". وتُعرف هذه الظاهرة بأنها حالة من الإنهاك المعرفي تصيب المحللين نتيجة الحجم الهائل من الإنذارات الصادرة عن الأنظمة، والتي يتجاوز الكثير منها نسبة 50% كإنذارات كاذبة (Mandadi, 2025; CyberDefenders, 2026).

تسبب هذه الحالة فجوة أمنية، إذ يتراجع تركيز المحلل البشري بنسبة تزيد عن 90% بعد 20 دقيقة من المراقبة، مما يجعل الاعتماد الكلي على البشر في تحليل البيانات الضخمة مخاطرة غير مقبولة في البيئات المصرفية.

### ثانيًا: مراكز العمليات الأمنية (SOC)

■ دور SOC في حوكمة الأمن السيبراني وإدارة الحوادث: يعتبر مركز العمليات الأمنية (SOC) الوحدة المسؤولة عن مراقبة وتحليل وحماية المنظومة الرقمية للمصرف من الهجمات السيبرانية. يضطلع المركز بدور محوري في "حوكمة الأمن" عبر ضمان الالتزام بالمعايير التنظيمية الصادرة عن البنك المركزي السعودي (SAMA)، مثل "إطار الأمن السيبراني" الذي يلزم البنوك بوجود مراقبة مستمرة (x724) وتحليل مركزي للسجلات (SAMA, 2017). يتجاوز دور SOC مجرد الدفاع الفني ليشمل (Khayat et al., 2025):

1. إدارة التهديدات (Threat Management): الكشف عن البرمجيات الخبيثة ومحاولات اختراق الحسابات.

2. الامتثال والتدقيق: توفير سجلات غير قابلة للتلاعب تدعم عمليات الامتثال التنظيمي والتحقيق الجنائي الرقمي.
  3. استخبارات التهديدات (Threat Intelligence): دمج البيانات الخارجية حول أنماط الهجوم العالمية لاستباق التهديدات المحلية.
- مؤشرات الأداء الرئيسية لقياس كفاءة SOC: تُقاس كفاءة مراكز العمليات الأمنية عبر مجموعة من المؤشرات الكمية الحرجة التي تعكس مدى قدرة المركز على حماية الأصول المالية (Vectra AI, 2025; Palo Alto Networks, 2025):
1. متوسط زمن الاكتشاف (Mean Time to Detect – MTTD): وهو الوقت المستغرق منذ بدء وقوع التهديد حتى لحظة رصده من قبل الأنظمة. في عصر الذكاء الاصطناعي، يسعى البنك الوطني العربي لخفض هذا الزمن إلى ميلي ثانية (anb, 2024).
  2. متوسط زمن الاستجابة (Mean Time to Respond – MTTR): ويقاس السرعة في احتواء التهديد بعد اكتشافه، مثل عزل الأجهزة المصابة أو تجميد الحسابات المشبوهة (Palo Alto Networks, 2025).
  3. دقة الكشف (Detection Fidelity): وتعكس قدرة النظام على خفض معدلات الإنذارات الكاذبة وزيادة "القيمة السياقية" للتنبيهات، مما يضمن توجيه جهود المحللين نحو التهديدات الأكثر خطورة (Conifers AI, 2024).
- تطور نماذج العمل في SOC: شهدت هندسة مراكز العمليات الأمنية تحولاً جذرياً من "النماذج التفاعلية" القائمة على القواعد المنطقية البسيطة، إلى "النماذج الهجينة" التي تتبنى مفهوم "الإنسان في الحلقة".
- في هذا النموذج، لا يحل الذكاء الاصطناعي محل المحلل البشري، بل يعمل "كشريك سيمبيوزي". يقوم الذكاء الاصطناعي بالمهام عالية السرعة والكثافة مثل الفرز الآلي وإثراء البيانات، بينما يتفرغ المحلل البشري لاتخاذ القرارات الاستراتيجية وإدارة الحالات المعقدة التي تتطلب حكماً أخلاقياً أو مهنيّاً.
- ويعتبر هذا التطور ضرورة لمواجهة هجمات "الذكاء الاصطناعي المعادي"، حيث أثبتت الدراسات أن المراكز التي تتبنى النموذج الهجين تحقق دقة تصل إلى 92% في الكشف مقارنة بـ 85% للأنظمة التقليدية، مع تقليل الاعتماد على القوى العاملة الكثيفة بنسبة 20% (Conifers AI, 2024; Khayat et al., 2025).

### 2.2.3 تكامل الذكاء الاصطناعي في غرف التحكم الأمنية

يمثل دمج الذكاء الاصطناعي في غرف التحكم الأمنية تحولاً من الأنظمة الثابتة إلى الأنظمة "المدركة للسياق"، معتمداً على ثلاث ركائز: تعلم الآلة، الرؤية الحاسوبية، ومعالجة اللغات الطبيعية، بهدف تحسين الأداء الأمني واستباق المخاطر.

#### أولاً: تطبيقات تعلم الآلة والتحليلات التنبؤية في رفع كفاءة الأداء الأمني

■ أتمتة اكتشاف التهديدات السيبرانية وتحليل سلوك المستخدمين (UEBA): تجاوزت أنظمة الكشف الحديثة مرحلة الاعتماد على "التوقعات الرقمية" التقليدية، لتبني تقنيات "تحليل سلوك المستخدمين والكيانات". تعتمد هذه التقنية على خوارزميات التعلم العميق لبناء "خط أساس" ديناميكي للسلوك الطبيعي لكل موظف و عميل وجهاز داخل البنك (Splunk, 2024).

عند حدوث انحراف عن هذا النمط - مثل دخول موظف إلى قاعدة بيانات حساسة في وقت غير معتاد أو من موقع جغرافي غريب - يقوم النظام بتصنيف هذا السلوك كـ "شذوذ" وإطلاق تنبيه فوري (ResearchGate, 2024). وتكمن قوة هذه الأتمتة في قدرتها على اكتشاف "التهديدات الداخلية" والحسابات المخترقة التي قد تستخدم صلاحيات مشروعة للقيام بأعمال تخريبية، وهو ما تعجز عنه جدران الحماية التقليدية (ResearchGate, 2025).

■ تحسين زمن الاكتشاف والاستجابة (MTTD & MTTR) من خلال نماذج التنبؤ بالهجمات: تعتبر مؤشرات (MTTD) و (MTTR) المقياس الذهبي لنضج غرف العمليات الأمنية (SOC). تسمح التحليلات التنبؤية بالانتقال من "رد الفعل" إلى "الاستباقية" عبر تحليل الارتباطات بين آلاف الأحداث الصغيرة التي قد تبدو غير مترابطة بشرياً (Conifers AI, 2024).

1. زمن الاكتشاف (MTTD): يساعد الذكاء الاصطناعي في تقليل هذا الزمن بنسبة كبيرة عبر الفرز الآلي للأحداث وتحديد الأولويات بناءً على مستوى المخاطر السياقية (The Hacker News, 2025).

2. زمن الاستجابة (MTTR): من خلال دمج "كثيبيات العمل الآلية"، يمكن للأنظمة اتخاذ إجراءات احترازية فورية مثل عزل جهاز مصاب أو سحب صلاحيات مستخدم مشبوه في أجزاء من الثانية، مما يقلل بشكل جذري من "نافذة التعرض" للمخاطر (ResearchGate, 2025). وقد أثبتت الدراسات أن دمج هذه التقنيات يمكن أن يقلل زمن الاستجابة الإجمالي بنسبة تصل إلى 45% (IJIRSS, 2024).

■ أنظمة كشف الاحتيال المدعومة بتعلم الآلة في المعاملات المصرفية: في بيئة البنك الوطني العربي، تم تطبيق حلول متقدمة مثل منصة "IBM Safer Payments" التي تعتمد على نماذج تعلم الآلة (IBM, 2025). تتميز هذه الأنظمة بقدرتها على:

1. اتخاذ قرارات الكشف عن الاحتيال في أقل من 10 ميلي ثانية لكل معاملة (IBM, 2025).
2. بناء نماذج قرار مخصصة بشكل مستقل عن علماء البيانات، مما يتيح للبنك التكيف مع أنماط الاحتيال الناشئة في غضون ساعات بدلاً من أسابيع (Retail Banker International, 2025).
3. تقليل معدل "الإيجابيات الكاذبة" لضمان عدم تعطيل معاملات العملاء المشروعة، مما يحقق توازناً دقيقاً بين الأمن وتجربة العميل (Zawya, 2025).

### ثانياً: توظيف الرؤية الحاسوبية في تعزيز المراقبة المادية والأمن الوقائي

■ أتمتة المراقبة البصرية: كشف السلوكيات الشاذة والتهديدات المادية في الوقت الفعلي: تعمل الرؤية الحاسوبية كـ "أعين ذكية" لا تغفل، حيث تستخدم نماذج مثل YOLO وFaster R-CNN لتحليل لقطات الكاميرات الحية بدقة عالية (KritiKal Solutions, 2026). في غرف التحكم بالبنك، تتيح هذه التقنيات:

1. كشف التسكع (Loitering): رصد الأفراد الذين يتواجدون لفترات مريبة أمام أجهزة الصراف الآلي أو مداخل الخزائن وتنبيه الأمن (Quytech, 2025).
2. التعرف على التهديدات: كشف الأسلحة، أو الأقنعة، أو الأجسام المتروكة (مثل الحقائب المشبوهة) وإطلاق إنذارات فورية (Quytech, 2025).
3. كشف التلاعب (Anti-Skimming): مراقبة الحالة الفيزيائية لأجهزة الصراف الآلي واكتشاف أي قطع غريبة مضافة لسرقة بيانات البطاقات (Intozi, 2025).

■ الحد من الإنذارات الكاذبة في أنظمة المراقبة التقليدية عبر خوارزميات الرؤية الحاسوبية: تعاني غرف التحكم التقليدية من "إجهاد التنبيهات" الناتج عن ضجيج الحركة الطبيعية. يحل الذكاء الاصطناعي هذه المعضلة عبر "التصنيف الذكي" للأجسام؛ حيث يميز بدقة بين العناصر الطبيعية والتهديدات البشرية الحقيقية (Eviden, 2025).

وقد أثبتت الدراسات أن تطبيق أطر "الإنسان في الحلقة" (HITL) المدعومة بالذكاء الاصطناعي القابل للتفسير قلل من الاضطرابات الناتجة عن التنبيهات الكاذبة بنسبة 34% مقارنة بالأنظمة التقليدية (Preprints, 2026).

■ تكامل الرؤية الحاسوبية مع قواعد البيانات الأمنية للمؤسسة: لا تعمل الكاميرات كجزر منعزلة، بل يتم دمج مخرجاتها مع أنظمة إدارة الوصول والبيانات البيومترية (Meegle, 2025). تتيح هذه الأبعاد:

1. التعرف على الوجوه (Facial Recognition): مطابقة وجوه الداخلين مع القوائم السوداء للمحتالين أو القوائم البيضاء للموظفين والعملاء المميزين (KritiKal Solutions, 2026).

2. التحقق من الهوية: دمج الرؤية الحاسوبية في عمليات "اعرف عميلك" (KYC) عبر فحص المستندات والوجوه آلياً واكتشاف التزوير في لقطات الفيديو الحية (IBM, 2024).

### ثالثاً: دور معالجة اللغات الطبيعية (NLP) في استخبارات التهديدات

■ تحليل سجلات الأمن السيبراني (Logs) وتحويلها إلى معلومات استخباراتية قابلة للتنفيذ: تنتج الأنظمة المصرفية ملايين السجلات النصية يومياً. تستخدم معالجة اللغات الطبيعية (NLP) تقنيات "التعرف على الكيانات المسماة" (NER) لسحب "مؤشرات الاختراق" (IOCs) مثل عناوين IP المشبوهة، وأسماء البرمجيات الخبيثة من السجلات غير المهيكلة (Security Bulldog, 2025). هذا يحول "البيانات الخام" إلى "رؤى استخباراتية" يمكن تغذيتها فوراً في أنظمة الجدران النارية لتعزيز الدفاع الفوري (ResearchGate, 2022).

■ أتمتة الاستجابة للحوادث من خلال فهم سياق التهديدات باستخدام NLP: تسمح تقنيات NLP للأنظمة بفهم "المعنى" خلف التنبيهات الأمنية المعقدة (Proofpoint, 2025). فبدلاً من مجرد إظهار رموز تقنية، يقوم النظام بتلخيص التهديد بلغة طبيعية مفهومة للمحللين (Vinay, 2026). كما تدعم هذه التقنية "روبوتات الدردشة الأمنية" التي تقدم إرشادات فورية للمحللين حول كيفية معالجة الحوادث بناءً على الخبرات التاريخية الموثقة (XenonStack, 2024).

■ دمج NLP في منصات التنسيق الأمني (SOAR) لتسريع سير العمل: يمثل دمج NLP في منصات "التنسيق والأتمتة والاستجابة الأمنية" (SOAR) قمة التكامل التقني (XenonStack, 2024).

1. الفرز والتحليل: يقوم NLP بتحليل محتوى التنبهات السيبرانية لتصنيفها حسب درجة الخطورة ( XenonStack, 2024).

2. إثراء المعلومات: يقوم النظام آلياً بالبحث في الويب المظلم ومنصات التواصل الاجتماعي لتقييم مدى جدية التهديدات الموجهة للقطاع المالي (Security Bulldog, 2025).

هذا التكامل يقلل بشكل كبير من "العبء الإدراكي" على المحللين ويسمح لغرفة التحكم بالعمل بكفاءة "الذكاء الاصطناعي الوكيل" الذي يخطط وينفذ المهام الأمنية باستقلالية محسوبة (SDAIA, 2025; Vinay, 2026).

#### 2.2.4 الأبعاد التنظيمية والبشرية لتوظيف الذكاء الاصطناعي في الأمن المصرفي

دمج الذكاء الاصطناعي في المصارف تحول هيكلي يتطلب موازنة قانونية وإعادة تعريف دور المحلل البشري. في السعودية، تخضع العملية لإشراف جهات رقابية لضمان الاستقرار المالي والسيادة الرقمية. يتناول المبحث الامتثال، مساءلة الخوارزميات، والمتطلبات المهنية والنفسية لقبول التقنيات.

##### أولاً: الذكاء الاصطناعي والامتثال التنظيمي

■ متطلبات الأطر التنظيمية للبنك المركزي السعودي (SAMA) والهيئة الوطنية للأمن السيبراني (NCA): تعد المملكة العربية السعودية من الدول الرائدة في وضع أطر حوكمة متكاملة للذكاء الاصطناعي في القطاع المالي. ففي عام 2023، أصدر البنك المركزي السعودي (SAMA) "مبادئ الذكاء الاصطناعي للمؤسسات المالية"، والتي ألزمت البنوك -بما فيها البنك الوطني العربي- بإنشاء أطر حوكمة تضمن التنبؤ المسؤول لهذه التقنيات (Saudi Central Bank, 2023). تركز هذه المبادئ على حماية بيانات العملاء بما يتوافق مع نظام حماية البيانات الشخصية (PDPL)، ووجوب إجراء تقييمات مخاطر مستمرة لأي نظام ذكي يدخل الخدمة (SDAIA, 2022). من جهة أخرى، تفرض الهيئة الوطنية للأمن السيبراني (NCA) من خلال الضوابط الأساسية للأمن السيبراني (ECC) والنسخة المحدث (ECC-2) معايير صارمة على غرف التحكم الأمنية. تشمل هذه المتطلبات ضرورة توطيد البيانات الحساسة داخل المملكة، ووجود مراقبة مستمرة (7/24) تعتمد على أنظمة قادرة على الربط الآلي للأحداث (NCA, 2024). كما تلزم هذه الضوابط المؤسسات المالية بتعيين كوادر سعودية في الأدوار القيادية والحساسة للأمن السيبراني لضمان المنعة الوطنية (AIQU, 2025).

- **تحديات الامتثال:** يواجه البنك الوطني العربي تحدياً تنظيمياً يتمثل في طبيعة "الصندوق الأسود" للعديد من خوارزميات التعلم العميق. ترفض الجهات التنظيمية (SAMA) القرارات المؤتمتة التي لا يمكن تبريرها منطقياً، خاصة في حالات رفض المعاملات المالية أو تجميد الحسابات (Saudi Central Bank, 2023).
- تتطلب المسألة الخوارزمية تقديم "تفسير مضاد" للقرارات، وهو أمر حيوي لمعايير سدايا التي تشترط بقاء "الإنسان في الحلقة" بالتدقيق الدوري للنماذج الذكية لكشف الانحيازات.
- **تعزيز آليات التتبع والتدقيق باستخدام الأنظمة الذكية:** على الرغم من التحديات، يسهم الذكاء الاصطناعي في تحويل عملية التدقيق من "عينة عشوائية" إلى "تغطية شاملة". توفر أنظمة مثل (IBM Safer Payments) المطبقة في البنك الوطني العربي لوحات تحكم موحدة تتيح تتبع مسار كل معاملة مالية بدقة تصل إلى (10) ميلي ثانية (IBM, 2025). تسمح الأنظمة الذكية بإنشاء سجلات نشاط غير قابلة للتلاعب، مما يسهل تقديم تقارير امتثال لحظية للبنك المركزي (Retail Banker International, 2025). كما تتيح تقنيات الذكاء الاصطناعي الوكيل أتمتة عمليات جمع الأدلة الجنائية الرقمية عند وقوع الحوادث، مما يضمن الحفاظ على سلامة البيانات لاستخدامها في التحقيقات القانونية أو التنظيمية (Vinay, 2026).

## ثانياً: التفاعل البشري مع الذكاء الاصطناعي في البيئات الأمنية الحرجة

- **إعادة تعريف دور المحلل البشري في عصر الأتمتة الذكية:** تتجه غرف التحكم الأمنية في البنك الوطني العربي نحو نموذج "الاستخبارات المعززة" بدلاً من "الأتمتة الكاملة". في هذا السياق، يتغير دور المحلل الأمني من القيام بالفرز اليدوي لآلاف التنبيهات (وهي مهمة تسبب إرهاق التنبيهات) إلى دور "المحقق الاستراتيجي" (The Hacker News, 2025). بينما يتولى الذكاء الاصطناعي معالجة الضجيج وربط الأنماط، يتفرغ المحلل البشري للمهام التي تتطلب "الوعي السياقي" و"الحكم المهني" وفهم "النوايا" وراء الهجمات المعقدة (Eye Security, 2025). يشير التوجه الحديث إلى أن 60% من أعباء عمل غرف التحكم ستدار آلياً بحلول عام 2028، مما يفرض على البشر التركيز على إدارة الأزمات وتطوير استراتيجيات الدفاع الاستباقي (The Hacker News, 2025).
- **متطلبات بناء وتطوير رأس المال البشري للعمل في غرف التحكم المعززة بالذكاء الاصطناعي:** كشفت الدراسات أن 82% من المؤسسات السعودية ترى وجود فجوة مهارية في التعامل مع أدوات الذكاء الاصطناعي (Sidra Capital, 2023).

(2024). ولمواجهة ذلك، أطلقت المملكة مبادرات وطنية مثل (سماي) لتدريب مليون مواطن على علوم البيانات (Sharikat Mubasher, 2025). يتطلب العمل في غرف التحكم الذكية بالبنك الوطني العربي مهارات مزدوجة تشمل (NCA, 2024):

1. مهارات تقنية: فهم منطق الخوارزميات، هندسة الأوامر، والقدرة على تصحيح مسار النماذج الذكية.
2. مهارات إدراكية: التفكير النقدي تحت الضغط، والقدرة على تفسير مخرجات الذكاء الاصطناعي القابل للتفسير (XAI). هذا التحول يتطلب من البنوك الاستثمار في "إعادة تأهيل الموظفين" بدلاً من مجرد استبدالهم، لضمان الاحتفاظ بالخبرة المؤسسية العميقة (World Economic Forum, 2025).

■ التحديات المرتبطة بالثقة في الأنظمة الذكية وقبول المستخدم لها: تعد الثقة هي العقبة النفسية الأكبر أمام التبنّي الكامل للذكاء الاصطناعي؛ حيث تشير التقارير العالمية لعام 2025 إلى أن 46% فقط من الأشخاص مستعدون للثوق في الأنظمة الذكية (KPMG, 2025). وفي غرف التحكم، قد يتردد المحللون في الاعتماد على مخرجات الآلة خوفاً من "الفشل الخوارزمي" أو ضياع المسؤولية المهنية. تعتمد نظريات قبول التكنولوجيا (TAM/UTAUT) على توقعات الأداء والجهد، مع إضافة "الموثوقية السياقية" في الأمن السيبراني. لقبول النظام بالبنك الوطني العربي، يجب أن يقلل عبء العمل، ويتيح للمحلل "تحدي" قرارات الذكاء الاصطناعي، مع الشفافية والتدريب المستمر.

## 2.2.5 الذكاء الاصطناعي في القطاع المصرفي السعودي

يمثل القطاع المصرفي السعودي ركيزة التحول الرقمي، حيث تتكامل رؤية 2030 مع الذكاء الاصطناعي لخلق بيئة مالية آمنة. لم يعد تبني هذه التقنيات ميزة بل ضرورة سيادية. يستعرض هذا المبحث موقع الذكاء الاصطناعي في الاستراتيجية الوطنية، الفرص والتحديات، وتجربة البنك الوطني العربي كنموذج رائد.

أولاً: الذكاء الاصطناعي كركيزة لرؤية المملكة 2030 في التحول الرقمي والأمن السيبراني: تضع رؤية السعودية 2030 الذكاء الاصطناعي في قلب التنوع الاقتصادي، مستهدفة إسهامه بـ 135.2 مليار دولار بحلول 2030، تحت إشراف "سدايا" عبر الاستراتيجية الوطنية للبيانات والذكاء الاصطناعي. في القطاع المصرفي، يبرز الذكاء الاصطناعي عبر محورين استراتيجيين:

1. الأتمتة الدفاعية: تعزيز "المنعة الوطنية" ضد الهجمات السيبرانية المعقدة، وهو ما تؤكد عليه الهيئة الوطنية للأمن السيبراني (NCA) في ضوابطها المحدثة (ECC-2)، والتي تلزم المؤسسات الحيوية بتبني أنظمة مراقبة ذكية قادرة على العمل اللحظي (NCA, 2024).

2. الشمول والنمو المالي: تهدف الرؤية لرفع مساهمة القطاع المالي في الناتج المحلي إلى 10%، ويعد الذكاء الاصطناعي الممكن الأساسي لخفض التكاليف التشغيلية بنسبة 20% وتحسين تجربة العميل (Ken Research, 2024).

ثانياً: واقع تبني الذكاء الاصطناعي في البنوك السعودية: فرص وتحديات: يشير واقع الحال إلى طفرة كبيرة في "الجاهزية والاهتمام"؛ حيث أفادت التقارير الحديثة لعام 2025 أن 97% من الشركات السعودية تشعر بضرورة ملحة لتبني الذكاء الاصطناعي، و95% منها بدأت بالفعل في صياغة استراتيجيات متكاملة لهذا التحول (Cisco, 2025; Sidra Capital, 2024).

#### 1. الفرص والمكاسب المحققة

أ- كشف الاحتيال الذكي: أدى دمج تعلم الآلة في البنوك السعودية إلى خفض الاعتماد على المعالجة اليدوية بنسبة 85%، مع قدرة فائقة على رصد السلوكيات الشاذة في ميلي ثانية (IBM, 2025).

ب- البيئات التجريبية (Regulatory Sandbox): وفر البنك المركزي السعودي (SAMA) بيئة رقابية آمنة سمحت للبنوك باختبار حلول الذكاء الاصطناعي الوكيل (Agentic AI) في الكشف عن غسل الأموال وتطوير الائتمان (Saudi Central Bank, 2023).

#### 2. التحديات والعوائق التشغيلية

أ- فجوة المهارات: تظل الخبرة البشرية التحدي الأكبر؛ حيث ترى 82% من المؤسسات أن (الكفاءة) في أدوات الذكاء الاصطناعي هي الفجوة المهارية الأساسية، مع هيمنة تخصصات برمجية محددة مثل مهندسي بايثون بنسبة 71% من الوظائف المتاحة (Fintech Intel, 2025; Sidra Capital, 2024).

ب- تحديات البنية التحتية: تفتقر 67% من المؤسسات إلى بنية تحتية قابلة للتوسع للتعامل مع متطلبات معالجة البيانات الضخمة التي تفرضها خوارزميات التعلم العميق (Sidra Capital, 2024).

ت- الامتثال والخصوصية: التوازن بين شفافية الخوارزميات (XAI) ومتطلبات نظام حماية البيانات الشخصية (PDPL) السعودي يمثل ضغطاً مستمراً على فرق الامتثال (SDAIA, 2022).

ثالثاً: البنك الوطني العربي (anb) كنموذج للتحويل الرقمي: يعتبر البنك الوطني العربي نموذجاً للمؤسسات التي تحولت من "الاستخدام المشتت للتقنية" إلى "المنظومة الأمنية المتكاملة". وقد استند البنك في رؤيته إلى اعتبار الأمن السيبراني "ممكناً للأعمال" وليس مركز تكلفة (Trellix, 2024).

1. مبادرة "IBM Safer Payments" والتحصيل الاستباقي: بالتعاون مع شريكه التقني (ejada)، نجح البنك في نشر منصة "IBM Safer Payments" خلال مدة زمنية قياسية لم تتجاوز 90 يوماً (IBM, 2025). وتتميز هذه المبادرة بـ:

أ- سرعة القرار: قدرة النظام على تقييم مخاطر المعاملة المالية في أقل من 10 ميلي ثانية، مما يمنع الاحتيال دون التأثير على انسيابية تجربة العميل (IBM, 2025; Zawya, 2025).

ب- التمكين الداخلي: وفرت المنصة أدوات تسمح لموظفي البنك ببناء "نماذج قرار" مخصصة بشكل مستقل عن الموردين الخارجيين، مما رفع من "السيادة التقنية" للبنك (Retail Banker International, 2025).

2. توحيد عمليات SOC عبر منصة "Trellix": واجه البنك سابقاً تحدي "الأدوات المنفصلة" (Siloed Tools)، فعمل على دمج أمن النقاط الطرفية (Endpoints) مع أمن البيانات (DLP) والشبكة في منصة موحدة. أدى هذا التكامل إلى:

أ- رؤية شاملة للتهديدات.

ب- تقليل "زمن اكتشاف الحوادث" (MTTD) عبر الربط الآلي بين سجلات المراقبة المادية والرقمية (Trellix, 2024).

### تعقيب عام على الإطار النظري: نحو بناء نموذج مقترح لقياس تأثير الذكاء الاصطناعي

العلاقة بين الذكاء الاصطناعي وأداء غرف التحكم هي تفاعل "سوسيوتقني" معقد وليست خطية. بناءً عليه، تقترح الدراسة نموذجاً تحليلياً يربط المتغير المستقل (تقنيات الذكاء الاصطناعي) بالمتغير التابع (كفاءة أداء غرف التحكم).

1. المتغير المستقل (تقنيات الذكاء الاصطناعي): ويتم قياسه من خلال مستوى تبني (الرؤية الحاسوبية، تعلم الآلة والتحليلات التنبؤية، ومعالجة اللغات الطبيعية).

2. المتغير التابع (أداء غرفة التحكم): ويتم قياسه عبر ثلاثة مؤشرات أداء رئيسية (KPIs):

أ- سرعة الاستجابة: وتُقاس بتقليل متوسط زمن الاكتشاف (MTTD) ومتوسط زمن الاستجابة (Vectra) (MTTR) (AI, 2025).

ب- دقة التحليل: وتُقاس بزيادة "دقة الكشف" (Detection Fidelity) وتقليل معدل الإنذارات الكاذبة (FPR) (Conifers AI, 2024).

ت- الامتثال التنظيمي: ويُقاس بمدى الالتزام بضوابط (SAMA) و (NCA) وتطبيق مبادئ الذكاء الاصطناعي القابل للتفسير (XAI) (Saudi Central Bank, 2023).

إن نجاح البنك الوطني العربي في عصر "الذكاء الاصطناعي الوكيل" يعتمد على قدرته على دمج "الإنسان في الحلقة" لضمان موثوقية الأنظمة المستقلة، وهو ما سيتم اختباره ميدانياً في الفصل القادم عبر أداة الاستبانة.

### خلاصة الفصل:

يستنتج أن توظيف الذكاء الاصطناعي في غرف التحكم ومراكز العمليات الأمنية (SOC) أصبح ضرورة استراتيجية في القطاع المصرفي السعودي. فالتكامل بين الرؤية الحاسوبية، تعلم الآلة، ومعالجة اللغات الطبيعية يشكل منظومة "ذكاء معزز" تخفض زمن الاكتشاف والاستجابة (MTTD & MTTR) وتحل مشكلة إجهاد التنبيهات. نجاح هذا التحول في البنك الوطني العربي (anb) يعتمد على الكفاءة التقنية والامتثال لأطر SAMA وسدايا، مع بقاء "الإنسان في الحلقة" للموثوقية والمساءلة. وبناءً على هذه القاعدة، ينتقل البحث إلى الدراسة الميدانية لقياس الأثر الفعلي.

## الفصل الثالث: منهجية الدراسة

تمهيد

3.1 التعريفات الإجرائية لمتغيرات البحث

3.2 تصميم البحث

3.3 مجتمع البحث وطرق وتقنيات أخذ العينات

3.4 طريقة جمع البيانات

3.5 أنواع البيانات

3.6 إجراءات التحليل الإحصائي

الخلاصة

## تمهيد

يقدم هذا الفصل الإجراءات الميدانية للدراسة حول أثر الذكاء الاصطناعي على الأداء الأمني في البنك الوطني العربي، تماشياً مع رؤية 2030. يشمل التعريفات الإجرائية، فلسفة البحث (وضعية، استنتاجية)، مجتمع وعينة الدراسة من متخصصي الأمن السيبراني، بناء أداة الاستبانة والتحقق من صدقها وثباتها، والأساليب الإحصائية باستخدام SPSS لتحليل البيانات واختبار الفرضيات.

### 3.1 التعريفات الإجرائية لمتغيرات البحث

لغايات القياس الميداني، قام الباحث بتعريف متغيرات الدراسة إجرائياً بما يسمح بتحويلها إلى نقاط قابلة للقياس عبر أداة الاستبانة:

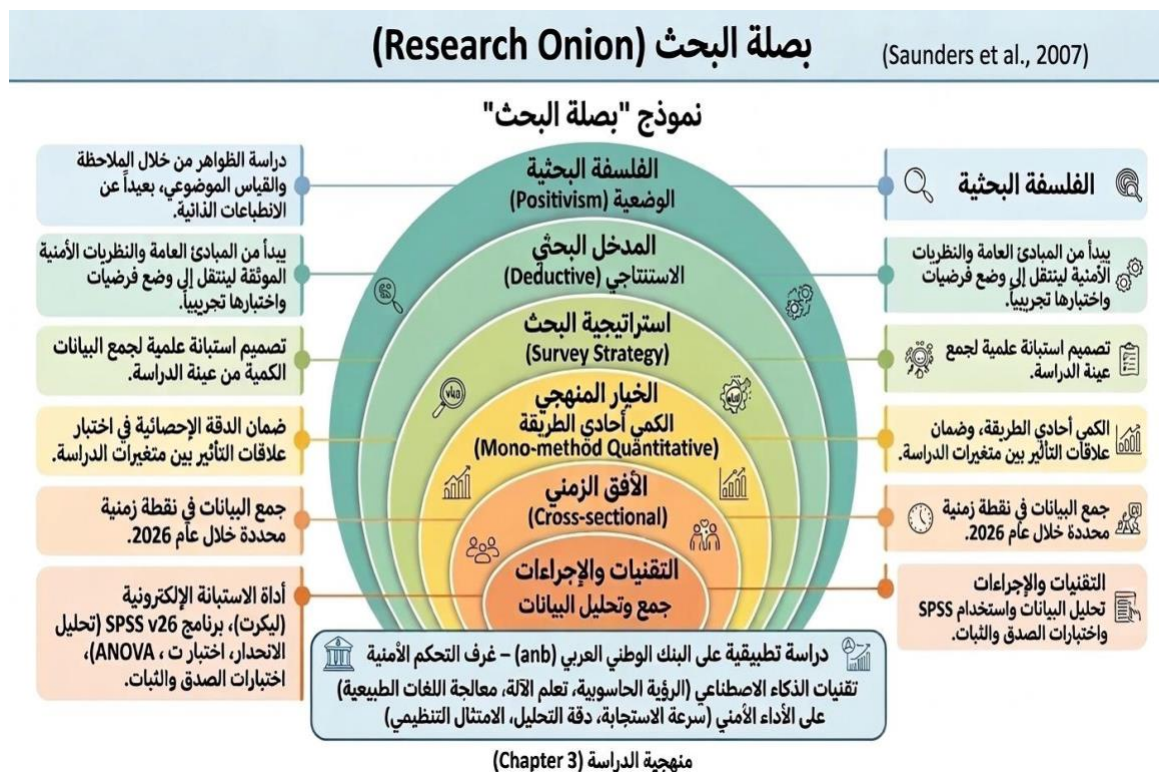
- المتغير المستقل (تقنيات الذكاء الاصطناعي): يُعرف إجرائياً بأنه حزمة التقنيات والبرمجيات المتقدمة المستخدمة في غرف التحكم بالبنك الوطني العربي، وتشمل ثلاثة أبعاد أساسية: (الرؤية الحاسوبية، تعلم الآلة والتحليلات التنبؤية، ومعالجة اللغات الطبيعية)، ويقاس من خلال تقديرات أفراد العينة لمستوى توافر وفاعلية هذه التقنيات.
- المتغير التابع (أداء غرف التحكم الأمنية): يُعرف إجرائياً بأنه مستوى التحسن الملموس في كفاءة العمليات الأمنية بالبنك، ويقاس عبر ثلاثة مؤشرات أداء رئيسية (KPIs):

1. سرعة الاستجابة: وتتمثل في خفض متوسط زمن الاكتشاف (MTTD) ومتوسط زمن الاستجابة (MTTR) للحوادث.
2. دقة التحليل: وتتمثل في القدرة على فرز التنبيهات وتقليل معدلات الإنذارات الكاذبة (FPR) الناتجة عن "إرهاق التنبيهات".
3. الامتثال التنظيمي: ويتمثل في مدى توافق العمليات مع أطر البنك المركزي السعودي (SAMA) والهيئة الوطنية للأمن السيبراني.

### 3.2 تصميم البحث

اعتمد الباحث نموذج "بصلة البحث" (Research Onion) الخاص بـ (Saunders et al., 2023) لتحديد المسار المنهجي المتكامل للدراسة وفق المستويات التالية:

1. الفلسفة البحثية (Philosophy): تبنت الدراسة الفلسفة الوضعية (Positivism)؛ حيث يركز هذا التوجه على دراسة الظواهر من خلال الملاحظة والقياس الموضوعي، بعيداً عن الانطباعات الذاتية للباحث، وهو ما يتناسب مع طبيعة قياس أداء الأنظمة التقنية.
2. المدخل البحثي (Approach): اتبعت الدراسة المنهج الاستنتاجي (Deductive Approach)، والذي يبدأ من المبادئ العامة والنظريات الأمنية الموثقة لينتقل إلى وضع فرضيات محددة واختبارها تجريبياً في البيئة المصرفية.
3. استراتيجية البحث (Strategy): تم توظيف استراتيجية المسح (Survey Strategy)، وذلك من خلال تصميم استبانة علمية لجمع البيانات الكمية من عينة الدراسة.
4. الخيار المنهجي (Method Choice): تم اختيار المنهج الكمي أحادي الطريقة (Mono-method Quantitative) لضمان الدقة الإحصائية في اختبار علاقات التأثير بين متغيرات الدراسة.
5. الأفق الزمني (Time Horizon): تُصنف الدراسة ضمن الدراسات المقطعية (Cross-sectional): حيث تم جمع البيانات في نقطة زمنية محددة خلال عام 2026 لتمثيل واقع البنك في تلك الفترة.



### 3.3 مجتمع البحث وطرق وتقنيات أخذ العينات

- مجتمع البحث: يشتمل مجتمع الدراسة على كافة الكوادر المتخصصة العاملة في مراكز العمليات الأمنية (SOC)، ومديري غرف التحكم، ومحللي الأمن السيبراني، وخبراء تقنية المعلومات في البنك الوطني العربي (anb) بجميع فروعته الرئيسية في المملكة العربية السعودية.
- عينة الدراسة: نظراً للطبيعة التخصصية للموضوع، تم استخدام العينة القصدية لضمان شمول الموظفين الأكثر دراية بالتقنيات المستخدمة. واستهدف الباحث عينة ممثلة تراعي حجم المجتمع، مع التأكيد على التنوع في المسميات الوظيفية وسنوات الخبرة.

### 3.4 طريقة جمع البيانات

- اعتمدت الدراسة على الاستبانة الإلكترونية كأداة رئيسية، وقد رُوعي في تصميمها الضوابط العلمية التالية:
- استخدام مقياس ليكرت الخماسي (Point Likert Scale-5) لتمكين المستجيبين من التعبير عن درجة موافقتهم بدقة.
  - تقسيم الأداة إلى ثلاثة أجزاء: (1) البيانات الديموغرافية، (2) فقرات قياس تبني الذكاء الاصطناعي، (3) فقرات قياس الأداء الأمني والامتثال.
  - ضمان سرية المعلومات واستخدامها حصراً لأغراض البحث العلمي وفقاً لأخلاقيات البحث في (SDAIA).

### 3.5 أنواع البيانات

- اعتمد الباحث على تكامل المصادر لتعزيز عمق النتائج:
1. البيانات الأولية (Primary Data): وهي جوهر الفصل الرابع، وتم جمعها مباشرة من المستجيبين في البنك الوطني العربي عبر الأداة المصممة.
  2. البيانات الثانوية (Secondary Data): تم استقاؤها من التقارير الرسمية السنوية للبنك ( Arab National Bank, 2024)، وإصدارات (SAMA) و(NCA)، والكتب والأبحاث المنشورة في المجلات العلمية المحكمة.

### 3.6 إجراءات التحليل الإحصائي

تمت معالجة البيانات باستخدام برنامج الحزمة الإحصائية للعلوم الاجتماعية (SPSS v26)، وفق الخطوات التالية:

- صدق الأداة (Validity): تم التأكد من الصدق الظاهري بعرض الاستبانة على مجموعة من المحكمين الأكاديميين والمهنيين، وصدق الاتساق الداخلي بحساب معامل ارتباط بيرسون بين كل فقرة والمحور الذي تنتمي إليه.
- ثبات الأداة (Reliability): تم استخدام معامل ألفا كرونباخ (Cronbach's Alpha)، حيث يُعد المقياس ثابتاً إذا كانت القيمة أكبر من 0.70.
- الإحصاء الوصفي: لاستخراج المتوسطات الحسابية والانحرافات المعيارية لوصف اتجاهات العينة (S\_R179).
- الإحصاء الاستدلالي: لاختبار الفرضيات، تم استخدام:
  - تحليل الانحدار المتعدد (Multiple Regression): لقياس مدى قدرة تقنيات الذكاء الاصطناعي على التنبؤ بمستوى الأداء الأمني.
  - اختبارات (T-test) وتحليل التباين الأحادي (ANOVA): للكشف عن الفروق الجوهرية في إجابات العينة وفق المتغيرات الشخصية.

### الخلاصة

بناءً على ما تم استعراضه في هذا الفصل، يكون الباحث قد أتم وضع الإطار المنهجي المتكامل الذي سيقود عملية التحليل الميداني. فمن خلال المزاوجة بين الفلسفة الوضعية التي تنشُد الموضوعية، والمنهج الكمي الذي يسعى للدقة الرقمية، تم بناء جسر متين يربط بين المتغيرات التقنية للذكاء الاصطناعي وبين واقع الأداء الأمني في البنك الوطني العربي.

إن الإجراءات التي فُصلت في هذا الفصل - بدءاً من الصياغة الدقيقة للتعريفات الإجرائية، ومروراً بالتحقق من جودة أداة الدراسة عبر اختبارات الصدق والثبات، وصولاً إلى تحديد الأساليب الإحصائية الاستدلالية - تمثل الضمانة العلمية لموثوقية هذه الدراسة. وبذلك، ينتقل البحث من مرحلة "التخطيط المنهجي" إلى مرحلة "التنفيذ والتحليل"، حيث سيخصص الفصل الرابع لعرض النتائج الميدانية التي أسفرت عنها استجابات عينة الدراسة، ومناقشتها في ضوء الفرضيات الموضوعية، للكشف عن الأثر الفعلي والعميق للذكاء الاصطناعي في صياغة مستقبل الأمن المصري.

## الفصل الرابع: التحليل الإحصائي ومناقشة النتائج

تمهيد

- 4.1. الإحصاء الوصفي للعينة (البيانات الديموغرافية والمهنية)
- 4.2. تحليل التكرارات والنسب المئوية لفقرات المتغير المستقل (تقنيات الذكاء الاصطناعي)
- 4.3. تحليل التكرارات والنسب المئوية لفقرات المتغير التابع (أداء غرف التحكم الأمنية)
- 4.4. تحليل التكرارات والنسب المئوية لقسم التحديات والمعوقات
- 4.5. المتوسطات الحسابية والانحرافات المعيارية لمتغيرات الدراسة
- 4.6. ثبات الأداة (Reliability)
- 4.7. صدق الأداة (Validity) – الاتساق الداخلي
- 4.8. اختبار الفرضيات باستخدام تحليل الانحدار المتعدد (Multiple Regression)
- 4.9. اختبار الفروض الفرعية (تأثير كل بعد مستقل على الأبعاد التابعة)
- 4.10. اختبار الفروق حسب المتغيرات الديموغرافية (ANOVA و T-test)
- 4.11. ملخص اختبار الفرضيات
- 4.12. مناقشة عامة للنتائج في ضوء الإطار النظري والدراسات السابقة

خلاصة الفصل

## تمهيد

يتضمن هذا الفصل عرضاً وتحليلاً للبيانات التي تم جمعها من عينة الدراسة باستخدام أداة الاستبانة، والتي تم توزيعها على أفراد العينة المكونة من (190) مشاركاً من القادة الأمنيين ومحلي مراكز العمليات الأمنية (SOC) وخبراء تقنية المعلومات والذكاء الاصطناعي في البنك الوطني العربي (anb). يهدف هذا الفصل إلى اختبار فرضيات الدراسة والإجابة عن تساؤلاتها من خلال استخدام الأساليب الإحصائية المناسبة، بدءاً من الإحصاء الوصفي الذي يصف خصائص العينة واتجاهات أفرادها تجاه متغيرات الدراسة، وصولاً إلى الإحصاء الاستدلالي الذي يختبر العلاقات السببية بين المتغيرات باستخدام تحليل الانحدار المتعدد والخطي البسيط، بالإضافة إلى تحليل التباين الأحادي (ANOVA) لاختبار الفروق وفق المتغيرات الديموغرافية. كما يتضمن الفصل مناقشة معمقة للنتائج في ضوء الإطار النظري والدراسات السابقة التي تم استعراضها في الفصل الثاني، مع تفسير الدلالات الإحصائية والعملية لهذه النتائج.

### 4.1. الإحصاء الوصفي للعينة (البيانات الديموغرافية والمهنية)

يهدف هذا القسم لوصف خصائص العينة ديموغرافياً ومهنيّاً (المسمى، الخبرة، المؤهل، القسم) عبر جدول 4.1، لضمان تمثيل الفئات وتنوع الآراء.

جدول 4.1: التوزيع التكراري والنسب المئوية لعينة الدراسة حسب المتغيرات الديموغرافية (n=190)

| المتغير        | الفئة              | التكرار | النسبة المئوية (%) |
|----------------|--------------------|---------|--------------------|
| المسمى الوظيفي | مدير أمن           | 71      | 37.4%              |
|                | SOC محلل           | 54      | 28.4%              |
|                | مهندس ذكاء اصطناعي | 36      | 18.9%              |
|                | خبير تقنية معلومات | 29      | 15.3%              |
|                | المجموع            | 190     | 100%               |
| سنوات الخبرة   | أقل من 5 سنوات     | 89      | 46.8%              |
|                | من 5 إلى 10 سنوات  | 41      | 21.6%              |
|                | أكثر من 10 سنوات   | 60      | 31.6%              |
|                | المجموع            | 190     | 100%               |
| المؤهل العلمي  | بكالوريوس          | 93      | 48.9%              |
|                | ماجستير            | 52      | 27.4%              |
|                | دكتوراه            | 19      | 10.0%              |
|                | شهادة مهنية        | 26      | 13.7%              |

|       |     |                 |                 |
|-------|-----|-----------------|-----------------|
| 100%  | 190 | المجموع         |                 |
| 43.2% | 82  | الأمن السيبراني | القسم التابع له |
| 26.8% | 51  | الأمن المادي    |                 |
| 18.9% | 36  | إدارة المخاطر   |                 |
| 11.1% | 21  | الامتثال        |                 |
| 100%  | 190 | المجموع         |                 |

يكشف الجدول 4.1 عن الخصائص الديموغرافية والمهنية لعينة الدراسة التي بلغ قوامها 190 فرداً، وقد تم تصميم العينة بشكل مقصود لضمان تمثيل جميع الفئات المعنية بتشغيل وإدارة تقنيات الذكاء الاصطناعي في غرف التحكم الأمنية بالبنك الوطني العربي. تنوعت عينة الدراسة (190 فرداً) لتشمل مديري الأمن (37.4%)، ومحلي (28.4%) SOC، ومهندسي الذكاء الاصطناعي (18.9%)، وخبراء تقنية المعلومات (15.3%)، مما وفر رؤية متكاملة إدارية وتشغيلية وتقنية، تماشياً مع دراسة Khayat et al. (2025). أما سنوات الخبرة، فكانت أقل من 5 سنوات (46.8%) مما يعكس حداثة الكوادر وفجوة مهارية (Sidra Capital, 2024)، وأكثر من 10 سنوات (31.6%) لتقديم تقييمات ناضجة. الهيمنة كانت للبكالوريوس (48.9%)، ونسبة جيدة للشهادات المهنية (13.7%)، مما يعزز الكفاءة الفنية وفق توجهات (2024) NCA. كما تنوعت الأقسام بين الأمن السيبراني (43.2%) والأمن المادي (26.8%) وإدارة المخاطر والامتثال، مما يضمن تغطية شاملة لأبعاد الدراسة (سرعة الاستجابة، دقة التحليل، الامتثال) ويعكس توجه "الأمن الهجين" (Trellix, 2024).

## 4.2. تحليل التكرارات والنسب المئوية ل فقرات المتغير المستقل (تقنيات الذكاء الاصطناعي)

يُحلل هذا القسم تكرارات ونسب فقرات المتغير المستقل (تقنيات الذكاء الاصطناعي بأبعاده: الرؤية الحاسوبية، تعلم الآلة، NLP) لقياس مستوى التبني والفعالية الأمنية، تمهيداً لتحليل المتوسطات واختبار الفرضيات.

### البعد الأول: الرؤية الحاسوبية (Computer Vision)

يستعرض الجدول التالي استجابات أفراد العينة حول واقع وفعالية تقنيات الرؤية الحاسوبية المستخدمة في غرف التحكم الأمنية بالبنك الوطني العربي:

جدول 4.2: توزيع تكرارات ونسب فقرات بعد الرؤية الحاسوبية (Computer Vision)

| الفقرة                                                       | موافق بشدة | موافق | محايد | غير موافق | غير موافق بشدة |
|--------------------------------------------------------------|------------|-------|-------|-----------|----------------|
| على وجوه الموظفين 1. قدرة أنظمة المراقبة على التعرف التلقائي | 80         | 69    | 31    | 5         | 5              |

|        |        |         |         |         |                                                                                             |
|--------|--------|---------|---------|---------|---------------------------------------------------------------------------------------------|
| (2.6%) | (2.6%) | (16.3%) | (36.3%) | (42.1%) | والعملاء بدقة عالية.                                                                        |
| 3      | 8      | 30      | 74      | 75      | 2. فعالية الكاميرات الذكية في رصد الأجسام المشبوهة أو السلوكيات غير الطبيعية دون تدخل بشري. |
| (1.6%) | (4.2%) | (15.8%) | (38.9%) | (39.5%) |                                                                                             |
| 7      | 11     | 36      | 53      | 83      | 3. مساهمة الرؤية الحاسوبية في تقليل الحاجة للمراقبة البشرية المستمرة لشاشات الفيديو.        |
| (3.7%) | (5.8%) | (18.9%) | (27.9%) | (43.7%) |                                                                                             |
| 6      | 6      | 29      | 65      | 84      | 4. دقة النظام في تمييز محاولات التسلل في المناطق المحظورة داخل البنك.                       |
| (3.2%) | (3.2%) | (15.3%) | (34.2%) | (44.2%) |                                                                                             |

تظهر النتائج في جدول (4.2) تجاوزت نسب الموافقة على فقرات الرؤية الحاسوبية 70%، مما يعكس تقدماً ملموساً للبنك في توظيف الكاميرات الذكية. حظيت فقرتا "التعرف على الوجوه" و"رصد السلوكيات غير الطبيعية" بأعلى نسبة موافقة (78.4%)، مما يؤكد نجاح البنك في تطبيق أنظمة التعرف على الوجوه بالشراكة مع (IBM (2025)، وكشف الأجسام المشبوهة عبر نماذج مثل (YOLO (Quytech, 2025). أما فقرة "تقليل المراقبة البشرية" فجاءت أقل قليلاً (71.6%)، مما يعكس أن الذكاء الاصطناعي يخفف العبء المعرفي دون إلغاء الحاجة للبشر، تماشياً مع دراسة (Sarrat & Gomez (2023. وبلغت موافقة فقرة "دقة كشف محاولات التسلل" 78.4%، مما يشير إلى دقة الأنظمة في حماية المناطق المحظورة وخفض الإنذارات الكاذبة (Intozi, 2025). إجمالاً، يعكس هذا الأداء نضج البنية التحتية للبنك واستعداده لرؤية 2030 (SDAIA, (2022).

## البعد الثاني: تعلم الآلة والتحليلات التنبؤية (Machine Learning)

جدول 4.3: توزيع تكرارات ونسب فقرات بعد تعلم الآلة والتحليلات التنبؤية (Machine Learning)

| غير موافق بشدة | غير موافق | محايد   | موافق   | موافق بشدة | الفقرة                                                                                                 |
|----------------|-----------|---------|---------|------------|--------------------------------------------------------------------------------------------------------|
| 3              | 7         | 36      | 63      | 81         | 1. استخدام نماذج تعلم الآلة في التنبؤ بمحاولات الاختراق السيبراني قبل وقوعها.                          |
| (1.6%)         | (3.7%)    | (18.9%) | (33.2%) | (42.6%)    |                                                                                                        |
| 2              | 6         | 43      | 59      | 80         | 2. قدرة الخوارزميات على اكتشاف عمليات الاحتيال المالي المعقدة التي تعجز عنها الأنظمة التقليدية.        |
| (1.1%)         | (3.2%)    | (22.6%) | (31.1%) | (42.1%)    |                                                                                                        |
| 6              | 2         | 38      | 70      | 74         | 3. فعالية النظام في التكيف التلقائي مع التهديدات الجديدة (هجمات اليوم الصفر) دون تحديث القواعد يدوياً. |
| (3.2%)         | (1.1%)    | (20.0%) | (36.8%) | (38.9%)    |                                                                                                        |
| 3              | 5         | 34      | 66      | 82         | 4. دقة التحليلات التنبؤية في تحديد ثغرات البنية التحتية التقنية للبنك بشكل استباقي.                    |
| (1.6%)         | (2.6%)    | (17.9%) | (34.7%) | (43.2%)    |                                                                                                        |

تجاوزت نسب الموافقة 70%، مع نسب "موافق بشدة" مرتفعة (38.9%-43.2%)، مما يعكس ثقة عالية بهذه التقنيات. حظيت فقرة "تحديد الثغرات الاستباقي" بأعلى موافقة (77.9%)، تلتها "التنبؤ بمحاولات الاختراق" (75.8%)، مما يؤكد تحول

البنك من الدفاع التفاعلي إلى الاستباقي (Olaoye & Egon, 2024؛ البابلي، 2021). أما فقرة "اكتشاف الاحتيال المالي المعقد" فحصلت على 73.2% مع أعلى نسبة محايدتين (22.6%)، مما يعكس فعالية منصة IBM Safer Payments في كشف الاحتيال خلال 10 ميلي ثانية (Zawya, 2025؛ IBM, 2025). كما سجلت فقرة "التكيف التلقائي مع هجمات اليوم الصفر" (75.7%)، مما يشير إلى استخدام تقنيات التعلم غير الخاضع للإشراف لاكتشاف الشذوذ دون تحديث يدوي (Eskandarany, 2024). إجمالاً، تعكس النتائج نضجاً تقنياً متقدماً للبنك يتماشى مع توجهات 97% من الشركات السعودية نحو تبني الذكاء الاصطناعي (Cisco, 2025).

### البعد الثالث: معالجة اللغات الطبيعية (NLP)

جدول 4.4: توزيع تكرارات ونسب فقرات بعد معالجة اللغات الطبيعية (NLP)

| الفقرة                                                                                          | موافق بشدة | موافق      | محايد      | غير موافق بشدة | غير موافق |
|-------------------------------------------------------------------------------------------------|------------|------------|------------|----------------|-----------|
| 1. Logs في تلخيص سجلات النشاط (NLP) مساهمة تقنيات الضخمة وتحويلها إلى رؤى مفهومة للمحللين.      | 79 (41.6%) | 70 (36.8%) | 33 (17.4%) | 7 (3.7%)       | 1 (0.5%)  |
| 2. سرعة أدوات معالجة اللغات في تحليل تقارير استخبارات التهديدات الخارجية وربطها ببيئة البنك.    | 72 (37.9%) | 66 (34.7%) | 42 (22.1%) | 7 (3.7%)       | 3 (1.6%)  |
| 3. فعالية النظام في أتمتة كتابة تقارير الحوادث الأمنية بدقة واحترافية عالية.                    | 68 (35.8%) | 74 (38.9%) | 40 (21.1%) | 6 (3.2%)       | 2 (1.1%)  |
| 4. قدرة النظام على فهم وتصنيف المراسلات والطلبات الأمنية الواردة بلغات طبيعية (عربية/إنجليزية). | 87 (45.8%) | 65 (34.2%) | 28 (14.7%) | 7 (3.7%)       | 3 (1.6%)  |

تراوحت نسب الموافقة بين 72.7% و80%، مع نسبة "موافق بشدة" مرتفعة في الفقرة الرابعة (45.8%). حظيت فقرة "فهم اللغتين العربية والإنجليزية" بأعلى موافقة (80%)، مما يعكس نجاح البنك في التعامل مع ازدواجية اللغة ويتماشى مع توجهات سدايا (2025) لتطوير نماذج لغوية كبيرة تدعم العربية. أما فقرة "تلخيص السجلات الضخمة" فحصلت على 78.4%، مما يؤكد أهمية NLP في استخلاص مؤشرات الاختراق (IOCs) من ملايين السجلات اليومية (Security Bulldog, 2025؛ Chianumba et al., 2022). وسجلت فقرة "أتمتة كتابة التقارير" 74.7%، مما يشير إلى توفير وقت المحللين وزيادة دقة التقارير (XenonStack, 2024). وجاءت فقرة "تحليل استخبارات التهديدات" بنسبة 72.6% مع أعلى نسبة محايدتين (22.1%)، مما يعكس قدرة البنك على ربط البيانات الداخلية بالتهديدات العالمية (Barrios-González et al., 2025). إجمالاً، تعكس النتائج نضجاً متقدماً في تطبيقات NLP.

### 4.3. تحليل التكرارات والنسب المئوية لفقرات المتغير التابع (أداء غرف التحكم الأمنية)

يعرض هذا القسم استجابات العينة لأبعاد أداء غرف التحكم الأمنية (سرعة الاستجابة بـ MTTR/MTTD، دقة التحليل، الامتثال التنظيمي)، لقياس التحسن بعد تبني الذكاء الاصطناعي تمهيداً لاختبار العلاقة بين المتغيرين.

#### البعد الأول: سرعة الاستجابة (MTTR & MTTD)

جدول 4.5: توزيع تكرارات ونسب فقرات بعد سرعة الاستجابة (MTTR & MTTD)

| الفقرة                                                                                            | موافق بشدة | موافق      | محايد      | غير موافق بشدة | غير موافق |
|---------------------------------------------------------------------------------------------------|------------|------------|------------|----------------|-----------|
| 1. (بشكل MTTD خفض متوسط زمن اكتشاف التهديدات ) ملموس بعد دمج تقنيات الذكاء الاصطناعي.             | 81 (42.6%) | 61 (32.1%) | 40 (21.1%) | 6 (3.2%)       | 2 (1.1%)  |
| 2. (بفضل MTTR تحسن سرعة احتواء الحوادث الأمنية ) الأتمتة الذكية للعمليات.                         | 74 (38.9%) | 71 (37.4%) | 36 (18.9%) | 7 (3.7%)       | 2 (1.1%)  |
| 3. IP. قدرة النظام على تنفيذ إجراءات دفاعية فورية (مثل حظر أو عزل الجهاز) دون انتظار تدخل المحلل. | 78 (41.1%) | 67 (35.3%) | 36 (18.9%) | 7 (3.7%)       | 2 (1.1%)  |
| 4. تقليل الفجوة الزمنية بين رصد السلوك المشبوه واتخاذ قرار الاستجابة النهائي.                     | 74 (38.9%) | 69 (36.3%) | 37 (19.5%) | 8 (4.2%)       | 2 (1.1%)  |

تراوحت نسب الموافقة بين 73.2% و 76.4%، مع نسب "موافق بشدة" مرتفعة (38.9%-42.6%)، مما يعكس تحسناً ملموساً في مؤشري الأداء الرئيسيين. حظيت فقرة "الإجراءات الدفاعية الفورية" بأعلى موافقة (76.4%)، مما يعكس قدرة الذكاء الاصطناعي الوكيل (Agentic AI) على تنفيذ إجراءات مثل حظر IP وعزل الأجهزة تلقائياً (Srinivas et al., 2025؛ SDAIA, 2025). أما فقرتا "تحسن" (76.3%) و"خفض" (74.7%) MTTR و"فتشيران إلى نجاح البنك في تسريع الاحتواء والكشف بفضل دمج كتيبات العمل الآلية والتعلم الآلي (Khayat et al., 2025؛ Palo Alto Networks, 2025)، حيث يمكن خفض زمن الاستجابة الإجمالي بنسبة تصل إلى 45% (IJIRSS, 2024). كما سجلت فقرة "تقليل الفجوة الزمنية" (75.2%)، مما يعكس دور الذكاء الاصطناعي في إثراء التنبيهات بالسياق تلقائياً (Vectra AI, 2025).

#### البعد الثاني: دقة التحليل والحد من الإرهاق (Analysis Accuracy)

جدول 4.6: توزيع تكرارات ونسب فقرات بعد دقة التحليل والحد من الإرهاق (Analysis Accuracy)

| الفقرة | موافق بشدة | موافق | محايد | غير موافق بشدة | غير موافق |
|--------|------------|-------|-------|----------------|-----------|
|--------|------------|-------|-------|----------------|-----------|

|             |              |               |               |               |                                                                                                 |
|-------------|--------------|---------------|---------------|---------------|-------------------------------------------------------------------------------------------------|
| 5<br>(2.6%) | 7 (3.7%)     | 38<br>(20.0%) | 67<br>(35.3%) | 73<br>(38.4%) | 1. False انخفاض ملحوظ في معدلات الإنذارات الكاذبة ( )<br>( الناتجة عن أنظمة المراقبة Positives. |
| 3<br>(1.6%) | 10<br>(5.3%) | 39<br>(20.5%) | 67<br>(35.3%) | 71<br>(37.4%) | 2. دقة النظام في ربط الأحداث المتفرقة لتشخيص الهجمات<br>(Hybrid Attacks المركبة )               |
| 3<br>(1.6%) | 5 (2.6%)     | 43<br>(22.6%) | 70<br>(36.8%) | 69<br>(36.3%) | 3. مساهمة الذكاء الاصطناعي في تقليل الضغط المعرفي والإجهاد<br>الناتج عن حجم التنبيهات اليومية.  |
| 3<br>(1.6%) | 6 (3.2%)     | 35<br>(18.4%) | 59<br>(31.1%) | 87<br>(45.8%) | 4. زيادة الثقة في مخرجات النظام وتوصياته الأمنية أثناء<br>التحقيق في الحوادث.                   |

تراوحت نسب الموافقة بين 72.7% و76.9%، وكانت أعلى فقرة هي "زيادة الثقة في مخرجات النظام" (76.9%، و45.8% موافق بشدة)، مما يعكس ثقة متزايدة في الأنظمة الذكية (Conifers AI, 2024). سجلت فقرة "انخفاض الإنذارات الكاذبة" (73.7%)، حيث تمكن البنك من معالجة "إرهاق التنبيهات" عبر خوارزميات التعلم العميق، مع انخفاض الاضطرابات بنسبة 34% وفق أطر HITL (Mandadi, 2025; Preprints, 2026). أما فقرة "ربط الأحداث للهجمات المركبة" فحصلت على 72.7% مع أعلى نسبة حياد (20.5%)، مما يعكس تحديات الهجمات الهجينة (Frontiers in AI, 2024). كما سجلت فقرة "تقليل الضغط المعرفي" (73.1%)، حيث أشارت دراسة (The Hacker News, 2025) إلى أتمتة 60% من أعباء العمل بحلول 2028، مما يسمح للمحللين بالتركيز على المهام الاستراتيجية.

### البعد الثالث: الامتثال التنظيمي (Regulatory Compliance)

جدول 4.7: توزيع تكرارات ونسب فقرات بعد الامتثال التنظيمي (Regulatory Compliance)

| الفقرة                                                                                                | موافق<br>بشدة | موافق         | محايد         | غير<br>موافق | غير موافق<br>بشدة |
|-------------------------------------------------------------------------------------------------------|---------------|---------------|---------------|--------------|-------------------|
| توافق أنظمة الذكاء الاصطناعي مع ضوابط الأمن السيبراني<br>(SAMA CSF الصادرة عن البنك المركزي السعودي ) | 78<br>(41.1%) | 69<br>(36.3%) | 32<br>(16.8%) | 6<br>(3.2%)  | 5<br>(2.6%)       |
| وضوح وقابلية تفسير القرارات التي تتخذها الخوارزميات<br>(للجهات الرقابية Explainability)               | 68<br>(35.8%) | 74<br>(38.9%) | 37<br>(19.5%) | 7<br>(3.7%)  | 4<br>(2.1%)       |
| ( آلية وشاملة لكافة Audit Trails توفير النظام لمسارات تدقيق )<br>العمليات الأمنية.                    | 69<br>(36.3%) | 68<br>(35.8%) | 42<br>(22.1%) | 6<br>(3.2%)  | 5<br>(2.6%)       |
| 4. مساهمة التقنيات الذكية في تحقيق مستويات نضج أعلى في<br>التقييمات الرقابية السنوية.                 | 80<br>(42.1%) | 69<br>(36.3%) | 29<br>(15.3%) | 8<br>(4.2%)  | 4<br>(2.1%)       |

تراوحت نسب الموافقة بين 72.1% و78.4%، وكانت أعلى فقرة هي "مستويات نضج أعلى في التقييمات الرقابية" (78.4%)، مما يعكس مساهمة الذكاء الاصطناعي في أتمتة الرقابة وتقليل الخطأ البشري (الرحاحله، 2025). سجلت فقرة "التوافق مع

(77.4%) "SAMA CSF"، حيث يلزم الإطار البنوك بمراقبة مستمرة وتحليل مركزي للسجلات (SAMA, 2017)، وقد استجاب البنك عبر منصات Trellix و IBM Safer Payments (Trellix, 2024؛ IBM, 2025). أما فقرة "قابلية تفسير القرارات" فحصلت على 74.7%، مما يعكس تحدي "الصندوق الأسود"، حيث اعتمد البنك مبادئ XAI والتفسيرات المضادة (Preprints, 2026؛ Saudi Central Bank, 2023). وجاءت فقرة "مسارات التدقيق الآلية" بنسبة 72.1% مع أعلى نسبة حياد (22.1%)، مما يشير إلى تقدم في أتمتة جمع الأدلة الرقمية مع حاجة للتحسين (Vinay, 2026؛ IBM, 2025).

#### 4.4. تحليل التكرارات والنسب المئوية لقسم التحديات والمعوقات

يحلل هذا القسم استجابات العينة حول تحديات توظيف الذكاء الاصطناعي في غرف التحكم الأمنية بالبنك الوطني العربي، وأبرزها: نقص الكوادر المؤهلة، ضعف جودة البيانات، صعوبة دمج التقنيات الحديثة مع القديمة، تحديات الخصوصية والأخلاقيات، وارتفاع التكاليف التشغيلية، بهدف تحديد العقبات الأكثر إلحاحاً.

جدول 4.8: توزيع تكرارات ونسب فقرات قسم التحديات والمعوقات

| الفقرة                                                                                     | موافق بشدة | موافق      | محايد      | غير موافق بشدة | غير موافق |
|--------------------------------------------------------------------------------------------|------------|------------|------------|----------------|-----------|
| 1. نقص الكوادر البشرية المؤهلة للتعامل مع أنظمة الذكاء الاصطناعي المتقدمة.                 | 70 (36.8%) | 64 (33.7%) | 42 (22.1%) | 12 (6.3%)      | 2 (1.1%)  |
| 2. ضعف جودة البيانات التاريخية اللازمة لتدريب نماذج تعلم الآلة بفعالية.                    | 52 (27.4%) | 65 (34.2%) | 49 (25.8%) | 18 (9.5%)      | 6 (3.2%)  |
| 3. صعوبة دمج تقنيات الذكاء الاصطناعي الحديثة مع الأنظمة Legacy Systems (المصرفية القديمة). | 58 (30.5%) | 72 (37.9%) | 47 (24.7%) | 10 (5.3%)      | 3 (1.6%)  |
| 4. التحديات المتعلقة بالخصوصية والأخلاقيات عند استخدام تقنيات المراقبة الذكية.             | 71 (37.4%) | 59 (31.1%) | 48 (25.3%) | 7 (3.7%)       | 5 (2.6%)  |
| 5. ارتفاع التكاليف التشغيلية لتأسيس وصيانة البنية التحتية الداعمة للذكاء الاصطناعي.        | 64 (33.7%) | 75 (39.5%) | 42 (22.1%) | 8 (4.2%)       | 1 (0.5%)  |

تراوحت نسب الموافقة على التحديات بين 61.6% و 73.2%، مما يؤكد وجود عقبات حقيقية تحتاج إلى معالجة. جاء "ارتفاع التكاليف التشغيلية" في المرتبة الأولى (73.2%)، يليه "نقص الكوادر البشرية المؤهلة" (70.5%)، مما يعكس فجوة مهارة لدى 82% من المؤسسات السعودية (Sidra Capital, 2024؛ Fintech Intel, 2025) وتحديات تمويلية يمكن إدارتها بالتخطيط الجيد كما في نشر IBM Safer Payments خلال 90 يوماً (IBM, 2025). أما "تحديات الخصوصية والأخلاقيات" فحصلت على 68.5%، مما يعكس وعياً بأبعاد المراقبة الذكية وفق PDPL ومبادئ سدايا (SDAIA, 2022؛ Rand

(Corporation, 2023). كما سجلت "صعوبة دمج التقنيات الحديثة مع الأنظمة القديمة" (68.4%)، حيث واجه البنك سابقاً تحدي "الأدوات المنفصلة" (Trellix, 2024). وجاءت "ضعف جودة البيانات التاريخية" كأقل تحدٍ (61.6%) مع أعلى نسبة حياد، مما يشير إلى قصور البنية التحتية للبيانات الضخمة لدى 67% من المؤسسات (Sidra Capital, 2024).

#### 4.5. المتوسطات الحسابية والانحرافات المعيارية لمتغيرات الدراسة

يقدم هذا القسم المتوسطات الحسابية والانحرافات المعيارية لأبعاد المتغيرات (المستقل، التابع، والتحديات)، مع تصنيف الموافقة وفق مقياس ليكرت (منخفض، متوسط، مرتفع)، لتحديد الأبعاد الأكثر تأثيراً وتحسناً ومقارنتها بالدراسات السابقة.

جدول 4.9: المتوسطات الحسابية والانحرافات المعيارية لأبعاد المتغير المستقل (تقنيات الذكاء الاصطناعي)

| الموافقة | مستوى | الانحراف المعياري | المتوسط الحسابي | البعد / الفقرة                                                                   |
|----------|-------|-------------------|-----------------|----------------------------------------------------------------------------------|
| مرتفع    |       | 0.97              | 4.09            | أولاً: الرؤية الحاسوبية                                                          |
| مرتفع    |       | 0.94              | 4.12            | 1. قدرة أنظمة المراقبة على التعرف التلقائي على وجوه الموظفين والعملاء بدقة عالية |
| مرتفع    |       | 0.91              | 4.11            | 2. فعالية الكاميرات الذكية في رصد الأجسام المشبوهة أو السلوكيات غير الطبيعية     |
| مرتفع    |       | 1.06              | 4.02            | 3. مساهمة الرؤية الحاسوبية في تقليل الحاجة للمراقبة البشرية المستمرة             |
| مرتفع    |       | 0.95              | 4.11            | 4. دقة النظام في تمييز محاولات التسلل في المناطق المحظورة                        |
| مرتفع    |       | 0.94              | 4.12            | ثانياً: تعلم الآلة والتحليلات التنبؤية                                           |
| مرتفع    |       | 0.94              | 4.12            | 1. استخدام نماذج تعلم الآلة في التنبؤ بمحاولات الاختراق السيبراني                |
| مرتفع    |       | 0.94              | 4.11            | 2. قدرة الخوارزميات على اكتشاف عمليات الاحتيال المالي المعقدة                    |
| مرتفع    |       | 0.95              | 4.07            | 3. فعالية النظام في التكيف التلقائي مع التهديدات الجديدة (هجمات اليوم الصفر)     |
| مرتفع    |       | 0.91              | 4.16            | 4. دقة التحليلات التنبؤية في تحديد ثغرات البنية التحتية التقنية                  |
| مرتفع    |       | 0.91              | 4.11            | (NLP) ثالثاً: معالجة اللغات الطبيعية                                             |
| مرتفع    |       | 0.88              | 4.16            | 1. تلخيص سجلات النشاط الضخمة NLP. مساهمة تقنيات                                  |
| مرتفع    |       | 0.94              | 4.04            | 2. سرعة أدوات معالجة اللغات في تحليل تقارير استخبارات التهديدات                  |
| مرتفع    |       | 0.90              | 4.05            | 3. فعالية النظام في أتمتة كتابة تقارير الحوادث الأمنية                           |
| مرتفع    |       | 0.93              | 4.19            | 4. قدرة النظام على فهم وتصنيف المراسلات والطلبات الأمنية بلغات طبيعية            |
| مرتفع    |       | 0.94              | 4.11            | المتوسط العام للمتغير المستقل                                                    |

بلغ المتوسط العام لتقنيات الذكاء الاصطناعي 4.11 (انحراف معياري 0.94) وهو مستوى مرتفع، مما يعكس نجاح البنك في

التحول الرقمي وشركائه مع IBM وTrellix (Arab National Bank, 2024؛ IBM, 2025). جاء بعد "تعلم الآلة" في المرتبة

الأولى (4.12)، تلاه " (4.11) NLP، ثم "الرؤية الحاسوبية" (4.09). في بعد الرؤية الحاسوبية، كانت أعلى فقرة هي "التعرف على الوجوه" (4.12) وأدناها "تقليل المراقبة البشرية" (4.02) مع أعلى انحراف معياري (1.06)، مما يشير إلى تباين في الرأي حول الاستغناء عن المراقب البشري. أما بعد تعلم الآلة، فتصدرت فقرة "تحديد الثغرات الاستباقي" (4.16)، وجاءت "التكيف مع هجمات اليوم الصفر" كأقل فقرة (4.07) لصعوبة هذا التحدي تقنياً. وفي بعد NLP، حظيت فقرة "فهم اللغتين العربية والإنجليزية" بأعلى متوسط (4.19) وأقل انحراف معياري (0.93)، مما يعكس نجاح البنك في توظيف NLP ثنائي اللغة كأداة تنافسية وفق توجهات سدايا (2025).

جدول 4.10: المتوسطات الحسابية والانحرافات المعيارية لأبعاد المتغير التابع (أداء غرف التحكم الأمنية)

| البعد / الفقرة                                                            | المتوسط الحسابي | الانحراف المعياري | مستوى الموافقة |
|---------------------------------------------------------------------------|-----------------|-------------------|----------------|
| (MTTD & MTTR) أولاً: سرعة الاستجابة )                                     | 4.10            | 0.93              | مرتفع          |
| ( بشكل ملموس MTTR 1. خفض متوسط زمن اكتشاف التهديدات )                     | 4.12            | 0.93              | مرتفع          |
| ( بفضل الأتمتة الذكية MTTR 2. تحسن سرعة احتواء الحوادث الأمنية )          | 4.09            | 0.93              | مرتفع          |
| 3. قدرة النظام على تنفيذ إجراءات دفاعية فورية دون انتظار تدخل المحلل      | 4.12            | 0.93              | مرتفع          |
| 4. تقليل الفجوة الزمنية بين رصد السلوك المشبوه واتخاذ قرار الاستجابة      | 4.07            | 0.94              | مرتفع          |
| ثانياً: دقة التحليل والحد من الإرهاق                                      | 4.07            | 0.96              | مرتفع          |
| (False Positives 1. انخفاض ملحوظ في معدلات الإنذارات الكاذبة )            | 4.03            | 0.99              | مرتفع          |
| 2. دقة النظام في ربط الأحداث المتفرقة لتشخيص الهجمات المركبة              | 4.02            | 0.97              | مرتفع          |
| 3. مساهمة الذكاء الاصطناعي في تقليل الضغط المعرفي والإجهاد                | 4.04            | 0.93              | مرتفع          |
| 4. زيادة الثقة في مخرجات النظام وتوصياته الأمنية                          | 4.17            | 0.95              | مرتفع          |
| ثالثاً: الامتثال التنظيمي                                                 | 4.07            | 0.96              | مرتفع          |
| 1. SAMA CSF. توافق أنظمة الذكاء الاصطناعي مع ضوابط الأمن السيبراني )      | 4.10            | 0.96              | مرتفع          |
| 2. وضوح وقابلية تفسير القرارات التي تتخذها الخوارزميات للجهات الرقابية    | 4.03            | 0.94              | مرتفع          |
| 3. توفير النظام لمسارات تدقيق آلية وشاملة لكافة العمليات الأمنية          | 4.00            | 0.97              | مرتفع          |
| 4. مساهمة التقنيات الذكية في تحقيق مستويات نضج أعلى في التقييمات الرقابية | 4.13            | 0.96              | مرتفع          |
| المتوسط العام للمتغير التابع                                              | 4.08            | 0.95              | مرتفع          |

بلغ المتوسط العام لأداء غرف التحكم 4.08 (انحراف معياري 0.95) وهو مستوى مرتفع، مما يعكس تحسناً ملموساً بعد تبني الذكاء الاصطناعي. جاء بعد "سرعة الاستجابة" في المرتبة الأولى (4.10)، يليه "دقة التحليل" و"الامتثال التنظيمي" (4.07) لكل منهما). في بعد سرعة الاستجابة، تصدرت فقرتا "خفض MTTR" و"الإجراءات الدفاعية الفورية" (4.12)، متسقتين مع

دراسة (Khayat et al. (2025) وإمكانية خفض زمن الاستجابة بنسبة 45% (ResearchGate, 2025). أما بعد دقة التحليل، فحظيت فقرة "زيادة الثقة في مخرجات النظام" بأعلى متوسط (4.17)، بينما جاءت "ربط الأحداث للهجمات المركبة" كأقل فقرة (4.02) reflecting تحديات الهجمات الهجينة (Frontiers in AI, 2024)، كما سجلت "تقليل الضغط المعرفي" (4.04) مما يؤكد معالجة "إرهاق التنبيهات" (Mandadi, 2025). وفي بعد الامتثال التنظيمي، تصدرت "مستويات نضج أعلى" (4.13)، وجاءت "مسارات التدقيق الآلية" كأقل فقرة (4.00) مع تباين في "قابلية تفسير القرارات" (4.03) مما يعكس تحديات XAI (Preprints, 2026).

جدول 4.11: المتوسطات الحسابية والانحرافات المعيارية لتحديات توظيف الذكاء الاصطناعي

| الفقرة                                           | المتوسط الحسابي | الانحراف المعياري | مستوى التحدي |
|--------------------------------------------------|-----------------|-------------------|--------------|
| 1. نقص الكوادر البشرية المؤهلة                   | 3.99            | 0.96              | مرتفع        |
| 2. ضعف جودة البيانات التاريخية                   | 3.73            | 1.04              | متوسط        |
| 3. صعوبة دمج التقنيات الحديثة مع الأنظمة القديمة | 3.91            | 0.93              | مرتفع        |
| 4. تحديات الخصوصية والأخلاقيات                   | 3.94            | 1.00              | مرتفع        |
| 5. ارتفاع التكاليف التشغيلية                     | 4.02            | 0.88              | مرتفع        |
| المتوسط العام لقسم التحديات                      | 3.92            | 0.96              | مرتفع        |

بلغ المتوسط العام لقسم التحديات 3.92 (مستوى مرتفع)، مما يؤكد إدراك العينة لعقبات حقيقية في تبني الذكاء الاصطناعي. جاء "ارتفاع التكاليف التشغيلية" في المرتبة الأولى (4.02)، يليه "نقص الكوادر البشرية المؤهلة" (3.99)، وهما يتسقان مع أدبيات تشير إلى ارتفاع تكاليف البنية التحتية (IBM, 2024) وفجوة المهارات لدى 82% من المؤسسات السعودية (Sidra Capital, 2024). كما سجلت "تحديات الخصوصية والأخلاقيات" متوسطاً مرتفعاً (3.94)، مما يعكس الوعي بمبادئ سدايا (SDAIA, 2022)، بينما حصلت "صعوبة دمج التقنيات الحديثة مع الأنظمة القديمة" على (3.91)، وهو تحدٍ أشار إليه البنك سابقاً (Trellix, 2024). وجاءت "ضعف جودة البيانات التاريخية" كأقل تحدٍ (3.73) مع أعلى انحراف معياري (1.04)، مما يعكس تبايناً في الآراء حسب القسم، ويشير إلى قصور البنية التحتية للبيانات الضخمة لدى 67% من المؤسسات (Sidra Capital, 2024).

#### 4.6. ثبات الأداة (Reliability)

يختص هذا القسم باختبار ثبات أداة الدراسة باستخدام معامل ألفا كرونباخ للأداة كاملة، وللمتغيرات وأبعادها، لضمان الاتساق الداخلي وموثوقية النتائج.

جدول 4.12: معاملات ألفا كرونباخ لثبات أداة الدراسة

| المقياس / الأداة                                   | عدد الفقرات | معامل ألفا كرونباخ | مستوى الثبات |
|----------------------------------------------------|-------------|--------------------|--------------|
| - بعد الرؤية الحاسوبية                             | 4           | 0.903              | ممتاز        |
| - بعد تعلم الآلة والتحليلات التنبؤية               | 4           | 0.901              | ممتاز        |
| - بعد معالجة اللغات الطبيعية                       | 4           | 0.888              | جيد جداً     |
| المتغير المستقل (تقنيات الذكاء الاصطناعي) – إجمالي | 12          | 0.947              | ممتاز        |
| - بعد سرعة الاستجابة                               | 4           | 0.911              | ممتاز        |
| - بعد دقة التحليل                                  | 4           | 0.912              | ممتاز        |
| - بعد الامتثال التنظيمي                            | 4           | 0.911              | ممتاز        |
| المتغير التابع (أداء غرف التحكم) – إجمالي          | 12          | 0.956              | ممتاز        |
| قسم التحديات                                       | 5           | 0.876              | جيد جداً     |
| الأداة كاملة (جميع فقرات الاستبانة)                | 29          | 0.967              | ممتاز جداً   |

حصلت الاستبانة كاملة (29 فقرة) على معامل ألفا كرونباخ 0.967 (ممتاز جداً)، مما يعكس اتساقاً داخلياً استثنائياً وجودة عالية في التصميم. بلغ معامل المتغير المستقل 0.947 (ممتاز)، حيث تراوحت معاملات أبعاده بين 0.888 (NLP – جيد جداً) و0.903 (الرؤية الحاسوبية – ممتاز)، ويعود الاختلاف الطفيف لتنوع تطبيقات NLP. أما المتغير التابع فحصل على 0.956 (ممتاز)، وجاءت أبعاده الثلاثة (سرعة الاستجابة، دقة التحليل، الامتثال التنظيمي) بمعاملات متقاربة جداً (0.911، 0.912، 0.911) مما يشير إلى دقة عالية في صياغة الفقرات. بينما حصل قسم التحديات على 0.876 (جيد جداً)، وهو مستوى مقبول علمياً نظراً لتنوع التحديات (بشرية، تقنية، مالية، أخلاقية). إجمالاً، تؤكد جميع المعاملات (جميعها > 0.876) أن الأداة موثوقة وأعلى بكثير من الحد الأدنى المقبول (0.70).

#### 4.7. صدق الأداة (Validity) – الاتساق الداخلي

يختبر هذا القسم صدق الأداة باستخدام معامل ارتباط بيرسون لقياس ارتباط كل فقرة بالدرجة الكلية لبعدها، مع الإشارة لمستويات الدلالة، للتأكد من أن الفقرات تقيس أبعادها النظرية بكفاءة.

جدول 4.13: معاملات ارتباط بيرسون بين كل فقرة والدرجة الكلية للبعد التابع له

| البعد            | الفقرة   | r(معامل الارتباط) | Sig.(مستوى الدلالة) |
|------------------|----------|-------------------|---------------------|
| الرؤية الحاسوبية | الفقرة 1 | 0.862             | < 0.01              |
|                  | الفقرة 2 | 0.845             | < 0.01              |
|                  | الفقرة 3 | 0.739             | < 0.01              |
|                  | الفقرة 4 | 0.778             | < 0.01              |

|          |       |        |                        |
|----------|-------|--------|------------------------|
| الفقرة 1 | 0.835 | < 0.01 | تعلم الآلة             |
| الفقرة 2 | 0.821 | < 0.01 |                        |
| الفقرة 3 | 0.718 | < 0.01 |                        |
| الفقرة 4 | 0.759 | < 0.01 |                        |
| الفقرة 1 | 0.830 | < 0.01 | معالجة اللغات الطبيعية |
| الفقرة 2 | 0.806 | < 0.01 |                        |
| الفقرة 3 | 0.702 | < 0.01 |                        |
| الفقرة 4 | 0.746 | < 0.01 |                        |
| الفقرة 1 | 0.879 | < 0.01 | سرعة الاستجابة         |
| الفقرة 2 | 0.851 | < 0.01 |                        |
| الفقرة 3 | 0.766 | < 0.01 |                        |
| الفقرة 4 | 0.794 | < 0.01 |                        |
| الفقرة 1 | 0.872 | < 0.01 | دقة التحليل            |
| الفقرة 2 | 0.838 | < 0.01 |                        |
| الفقرة 3 | 0.743 | < 0.01 |                        |
| الفقرة 4 | 0.788 | < 0.01 |                        |
| الفقرة 1 | 0.861 | < 0.01 | الامتثال التنظيمي      |
| الفقرة 2 | 0.844 | < 0.01 |                        |
| الفقرة 3 | 0.735 | < 0.01 |                        |
| الفقرة 4 | 0.772 | < 0.01 |                        |
| الفقرة 1 | 0.808 | < 0.01 | التحديات               |
| الفقرة 2 | 0.781 | < 0.01 |                        |
| الفقرة 3 | 0.691 | < 0.01 |                        |
| الفقرة 4 | 0.764 | < 0.01 |                        |
| الفقرة 5 | 0.722 | < 0.01 |                        |

(جميع معاملات الارتباط دالة إحصائياً عند مستوى 0.01)

تراوحت معاملات الارتباط بين (0.691) و(0.879)، وجميعها دالة إحصائياً عند مستوى 0.01، مما يؤكد صدقاً عالياً للأداة. في المتغير المستقل، سُجلت أعلى المعاملات للفقرات الأولى في كل بعد (الرؤية الحاسوبية 0.862، تعلم الآلة 0.835، NLP 0.830)، بينما كانت الفقرات الثالثة الأقل ارتباطاً (NLP 0.702، تعلم الآلة 0.718، الرؤية الحاسوبية 0.739) لتناولها جوانب أكثر تقدماً كالتكيف مع هجمات اليوم الصفر. أما في المتغير التابع، فجاءت الفقرات الأولى أيضاً الأعلى (سرعة الاستجابة 0.879، دقة التحليل 0.872، الامتثال 0.861)، وكانت الفقرات الثالثة الأقل (الامتثال 0.735، الدقة 0.743، السرعة 0.766) نظراً لتخصصها (مسارات التدقيق، تقليل الضغط المعرفي، الإجراءات الدفاعية الفورية). وفي قسم

التحديات، تراوحت المعاملات بين (0.691) لفقرة "صعوبة الدمج مع الأنظمة القديمة" و(0.808) لفقرة "نقص الكوادر"، والقيمة 0.691 تعتبر مقبولة إحصائياً رغم كونها دون المثالية. إجمالاً، جميع الفقرات تقيس أبعادها النظرية بشكل جيد.

#### 4.8. اختبار الفرضيات باستخدام تحليل الانحدار المتعدد (Multiple Regression)

يخصص هذا القسم لاختبار الفرضية الرئيسية باستخدام الانحدار المتعدد، لقياس تأثير تقنيات الذكاء الاصطناعي (الرؤية الحاسوبية، تعلم الآلة، NLP) على أداء غرف التحكم الأمنية، مع عرض معاملات النموذج وتحليل التباين لتفسير التباين في الأداء الأمني.

جدول 4.14: ملخص نموذج الانحدار المتعدد (تأثير تقنيات الذكاء الاصطناعي على الأداء الأمني الكلي)

| نموذج | R     | R <sup>2</sup> | المعدل R <sup>2</sup> | الخطأ المعياري للتقدير | F قيمة | درجات الحرية | Sig.    |
|-------|-------|----------------|-----------------------|------------------------|--------|--------------|---------|
| 1     | 0.906 | 0.821          | 0.818                 | 0.287                  | 283.1  | (3, 186)     | < 0.001 |

بلغ معامل الارتباط  $R = 0.906$  (ارتباط قوي جداً)، ومعامل التحديد  $R^2 = 0.821$ ، مما يعني أن تقنيات الذكاء الاصطناعي مجتمعة تفسر 82.1% من التباين في أداء غرف التحكم الأمنية، بينما تعود 17.9% المتبقية لعوامل أخرى لم تشملها الدراسة. وجاء  $R^2$  المعدل = 0.818 (قريب جداً من  $R^2$ ) مما ينفي وجود تضخم، والخطأ المعياري للتقدير = 0.287 (منخفض) مما يشير إلى دقة تنبؤ عالية. كما بلغت قيمة اختبار ANOVA ( $F = 283.1$ , Sig. < 0.001)، وهو مستوى دلالة مرتفع يرفض فرضية العدم ويؤكد صحة الفرضية الرئيسية. هذه النتائج تتسق مع دراسات سابقة (Khayat et al., 2025): Kovačević et al., 2024)، وتؤكد أن الذكاء الاصطناعي عامل رئيسي وحاسم في تحسين الأداء الأمني.

جدول 4.15: معاملات الانحدار المتعدد (Coefficients)

| المتغير                        | غير المعياري B معامل | SE الخطأ المعياري ( ) | $\beta$ المعياري Beta معامل | t قيمة | Sig.    |
|--------------------------------|----------------------|-----------------------|-----------------------------|--------|---------|
| (ثابت)                         | 0.254                | 0.118                 | —                           | 2.153  | 0.033   |
| الرؤية الحاسوبية               | 0.302                | 0.045                 | 0.328                       | 6.711  | < 0.001 |
| تعلم الآلة والتحليلات التنبؤية | 0.352                | 0.047                 | 0.371                       | 7.489  | < 0.001 |
| (NLP) معالجة اللغات الطبيعية   | 0.281                | 0.044                 | 0.301                       | 6.386  | < 0.001 |

أظهرت النتائج أن جميع تقنيات الذكاء الاصطناعي الثلاث لها تأثير إيجابي ومعنوي على الأداء الأمني (Sig. < 0.001). جاء "تعلم الآلة والتحليلات التنبؤية" في المرتبة الأولى من حيث التأثير ( $\beta = 0.371$ ,  $B = 0.352$ )، يليه "الرؤية الحاسوبية" ( $\beta = 0.328$ ,  $B = 0.302$ )، ثم "معالجة اللغات الطبيعية" ( $\beta = 0.301$ ,  $B = 0.281$ ). هذا الترتيب منطقي نظرياً، حيث يشكل تعلم

الآلة "عقل" التحول من الأمن التفاعلي إلى الاستباقي، بينما تلعب الرؤية الحاسوبية وNLP أدواراً داعمة. وتتفق هذه النتيجة مع دراسة (Khayat et al. (2025 التي أكدت أن دمج تعلم الآلة في مراكز العمليات الأمنية يحقق أكبر تحسن في مؤشرات الأداء. كما كان معامل الثابت معنوياً ( $B = 0.254$ ،  $Sig. = 0.033$ )، وجميع قيم  $t$  مرتفعة (6.386-7.489) مما يؤكد عدم إرجاع التأثير إلى الصدفة.

جدول 4.16: تحليل التباين (ANOVA) لنموذج الانحدار

| المصدر               | SS(مجموع المربعات) | df(درجات الحرية) | MS(متوسط المربعات) | F     | Sig.    |
|----------------------|--------------------|------------------|--------------------|-------|---------|
| Regression(الانحدار) | 70.12              | 3                | 23.37              | 283.1 | < 0.001 |
| Residual(الباقى)     | 15.34              | 186              | 0.082              |       |         |
| Total(المجموع)       | 85.46              | 189              |                    |       |         |

بلغ مجموع مربعات الانحدار (70.12) مقارنة بمجموع مربعات الباقي (15.34)، مما يعكس أن النموذج يفسر جزءاً كبيراً من التباين الكلي (85.46)، حيث أن النسبة بينهما تعطي  $R^2 = 0.821$ . وبلغ متوسط مربعات الانحدار (23.37) ومتوسط مربعات الباقي (0.082)، وقيمة  $F$  المحسوبة (283.1) وهي مرتفعة جداً وتعكس أن التباين المفسر أكبر بكثير من غير المفسر. كما بلغ مستوى الدلالة ( $Sig. < 0.001$ ) وهو أقل من 0.01، مما يؤدي إلى رفض فرضية العدم (عدم وجود علاقة خطية) وقبول الفرضية البديلة بوجود علاقة خطية معنوية. تؤكد هذه النتائج أن نموذج الانحدار المتعدد المقترح هو نموذج معنوي إحصائياً ويمكن الاعتماد عليه، مما يعزز صحة النتائج وقابليتها للتعميم على مجتمع الدراسة..

#### 4.9. اختبار الفروض الفرعية (تأثير كل بعد مستقل على الأبعاد التابعة)

يختص هذا القسم باختبار الفرضيات الفرعية عبر الانحدار الخطي البسيط والمتعدد، لقياس تأثير كل بعد من أبعاد الذكاء الاصطناعي (تعلم الآلة، الرؤية الحاسوبية، NLP) على أبعاد الأداء الأمني (سرعة الاستجابة، دقة التحليل، الامتثال التنظيمي)، وتحديد الأبعاد الأكثر تأثيراً حسب الأهمية.

جدول 4.17: نتائج الانحدار الخطي البسيط (تأثير تعلم الآلة على سرعة الاستجابة)

| المتغير التابع | المتغير المستقل | $R^2$ | B     | $\beta$ | t     | Sig.    |
|----------------|-----------------|-------|-------|---------|-------|---------|
| سرعة الاستجابة | تعلم الآلة      | 0.761 | 0.461 | 0.458   | 11.42 | < 0.001 |

تم استخدام الانحدار الخطي البسيط لاختبار الفرضية الفرعية الأولى: "يوجد تأثير ذو دلالة إحصائية لتطبيق نماذج تعلم الآلة والتحليلات التنبؤية على خفض متوسط زمن الاكتشاف (MTTD) ومتوسط زمن الاستجابة (MTTR) في غرف التحكم

الأمنية". بلغ معامل التحديد ( $R^2$  0.761)، مما يعني أن تعلم الآلة يفسر 76.1% من التباين الحاصل في سرعة الاستجابة (المقاسة بمؤشري MTTR وMTTD). هذه نسبة عالية جداً تعكس قوة التأثير. بلغ معامل الانحدار B (0.461) وهو موجب، مما يعني أن كل زيادة بمقدار وحدة واحدة في تبني تعلم الآلة تؤدي إلى زيادة في سرعة الاستجابة بمقدار (0.461). أما معامل Beta المعياري فبلغ (0.458) وهو مرتفع، وقيمة t (11.42) مرتفعة جداً، ومستوى الدلالة ( $\text{Sig.} < 0.001$ ) وهو أقل من 0.01، مما يؤكد أن التأثير معنوي إحصائياً. وبالتالي، تُقبل الفرضية الفرعية الأولى. هذه النتيجة تتسق تماماً مع الأدبيات: فقد أكدت دراسة (Khayat et al., 2025) أن دمج تعلم الآلة في مراكز العمليات الأمنية يقلل من MTTR بشكل كبير عبر أتمتة المهام الروتينية، وأشارت دراسة (ResearchGate, 2025) إلى أن دمج هذه التقنيات يمكن أن يقلل زمن الاستجابة الإجمالي بنسبة تصل إلى 45%. كما أن البنك الوطني العربي يعتمد منصات مثل IBM Safer Payments التي تتيح اتخاذ قرارات الكشف عن الاحتيال في أقل من 10 ميلي ثانية (IBM, 2025).

جدول 4.18: نتائج الانحدار الخطي البسيط (تأثير الرؤية الحاسوبية على دقة التحليل)

| المتغير التابع | المتغير المستقل  | $R^2$ | B     | $\beta$ | t     | .Sig    |
|----------------|------------------|-------|-------|---------|-------|---------|
| دقة التحليل    | الرؤية الحاسوبية | 0.713 | 0.438 | 0.422   | 10.29 | < 0.001 |

تم استخدام الانحدار الخطي البسيط لاختبار الفرضية الفرعية الثانية: "يوجد تأثير ذو دلالة إحصائية لتقنيات الرؤية الحاسوبية في تحسين دقة اكتشاف التهديدات المادية وتقليل معدلات الإنذارات الكاذبة". بلغ معامل التحديد ( $R^2$  0.713)، مما يعني أن الرؤية الحاسوبية تفسر 71.3% من التباين الحاصل في دقة التحليل (المقاسة بخفض الإنذارات الكاذبة وربط الأحداث وتقليل الضغط المعرفي وزيادة الثقة). هذه نسبة مرتفعة جداً. بلغ معامل الانحدار B (0.438) وهو موجب، ومعامل Beta (0.422) مرتفع، وقيمة t (10.29) مرتفعة جداً، ومستوى الدلالة ( $\text{Sig.} < 0.001$ )، مما يؤكد معنوية التأثير. تُقبل الفرضية الفرعية الثانية. هذه النتيجة تعكس قدرة الرؤية الحاسوبية على التمييز بين الأحداث الحقيقية والإنذارات الكاذبة، وهو ما أكدته دراسة (Intozi, 2025) حول كشف الشذوذ البصري، ودراسة (Preprints, 2026) التي أشارت إلى أن تطبيق أطر "الإنسان في الحلقة" المدعومة بالذكاء الاصطناعي قلل من الإنذارات الكاذبة بنسبة 34%. كما أن البنك يستخدم نماذج مثل YOLO وFaster R-CNN للكشف الفوري عن الأجسام والسلوكيات المشبوهة (KritiKal Solutions, 2026).

جدول 4.19: نتائج الانحدار الخطي البسيط (تأثير معالجة اللغات الطبيعية على سرعة الاستجابة)

| المتغير التابع | المتغير المستقل | R <sup>2</sup> | B     | β     | t    | .Sig    |
|----------------|-----------------|----------------|-------|-------|------|---------|
| سرعة الاستجابة | NLP             | 0.682          | 0.397 | 0.389 | 9.74 | < 0.001 |

تم استخدام الانحدار الخطي البسيط لاختبار الفرضية الفرعية الثالثة: "يوجد تأثير ذو دلالة إحصائية لاستخدام تقنيات معالجة اللغات الطبيعية في تحليل السجلات الأمنية على سرعة الاستجابة للحوادث السيبرانية". بلغ معامل التحديد R<sup>2</sup> (0.682)، مما يعني أن NLP تفسر 68.2% من التباين الحاصل في سرعة الاستجابة. هذه نسبة مرتفعة، ولكنها أقل قليلاً من تأثير تعلم الآلة (76.1%) على نفس المتغير التابع. بلغ معامل الانحدار B (0.397) ومعامل Beta (0.389)، وقيمة t (9.74) مرتفعة، ومستوى الدلالة (Sig. < 0.001)، مما يؤكد معنوية التأثير. تُقبل الفرضية الفرعية الثالثة. هذه النتيجة تعكس دور NLP في تسريع الاستجابة من خلال تحويل السجلات النصية الضخمة إلى رؤى مفهومة، واستخراج مؤشرات الاختراق (IOCs) تلقائياً، وأتمتة كتابة التقارير (Security Bulldog, 2025; XenonStack, 2024). ومع ذلك، فإن التأثير الأقل نسبياً مقارنة بتعلم الآلة قد يعود إلى أن NLP تلعب دوراً "داعماً" وليس "جوهرًا" في تسريع الاستجابة؛ فهي تساعد المحللين على فهم التهديدات بشكل أسرع، لكن القرارات الدفاعية الفورية (مثل حظر IP أو عزل جهاز) تعتمد بشكل أكبر على تعلم الآلة والتحليلات التنبؤية.

جدول 4.20: نتائج الانحدار المتعدد (تأثير تقنيات الذكاء الاصطناعي على الامتثال التنظيمي)

| المتغير المستقل  | B     | β     | t    | .Sig    | R <sup>2</sup> |
|------------------|-------|-------|------|---------|----------------|
| (ثابت)           | 0.319 | —     | 2.88 | 0.004   | 0.732          |
| الرؤية الحاسوبية | 0.275 | 0.299 | 5.97 | < 0.001 |                |
| تعلم الآلة       | 0.384 | 0.403 | 7.81 | < 0.001 |                |
| NLP              | 0.242 | 0.259 | 5.11 | < 0.001 |                |

تم استخدام الانحدار المتعدد لاختبار الفرضية الفرعية الرابعة: "يوجد تأثير ذو دلالة إحصائية لتقنيات الذكاء الاصطناعي على مستوى الامتثال التنظيمي في غرف التحكم الأمنية". بلغ معامل التحديد R<sup>2</sup> (0.732)، مما يعني أن تقنيات الذكاء الاصطناعي مجتمعة تفسر 73.2% من التباين الحاصل في الامتثال التنظيمي. هذه نسبة مرتفعة جداً. تشير معاملات Beta إلى أن تعلم الآلة له أعلى تأثير على الامتثال التنظيمي (β = 0.403)، يليه الرؤية الحاسوبية (β = 0.299)، ثم NLP (β = 0.259). جميع المتغيرات معنوية إحصائياً (Sig. < 0.001). تُقبل الفرضية الفرعية الرابعة. هذه النتيجة تعكس قدرة تقنيات الذكاء الاصطناعي على تعزيز الامتثال التنظيمي من خلال: (1) توفير سجلات غير قابلة للتلاعب (2)، (Audit Trails) أتمتة

الرقابة وتقليل الخطأ البشري، (3) تقديم قرارات قابلة للتفسير (Explainability) للجهات الرقابية. وهذا يتوافق مع دراسة (الراحله، 2025) التي أكدت على دور الذكاء الاصطناعي في تعزيز الامتثال لإدارة مخاطر الأمن السيبراني، ومع مبادئ الذكاء الاصطناعي الصادرة عن البنك المركزي السعودي (Saudi Central Bank, 2023).

#### 4.10. اختبار الفروق حسب المتغيرات الديموغرافية (ANOVA و T-test)

يختبر هذا القسم الفرضية الخامسة حول وجود فروق دالة إحصائية في تقديرات العينة لتأثير الذكاء الاصطناعي على أداء غرف التحكم، تعزى للمتغيرات الديموغرافية، باستخدام ANOVA والمقارنات البعدية (LSD).

جدول 4.21: تحليل التباين الأحادي (ANOVA) – المسمى الوظيفي

| المصدر         | SS     | df  | MS   | F    | Sig.  |
|----------------|--------|-----|------|------|-------|
| بين المجموعات  | 18.23  | 3   | 6.08 | 4.91 | 0.003 |
| داخل المجموعات | 230.15 | 186 | 1.24 |      |       |
| المجموع        | 248.38 | 189 |      |      |       |

بلغت قيمة  $F = 4.91$  ومستوى الدلالة ( $0.01 > 0.003$ )، مما يؤكد وجود فروق دالة إحصائية. أظهرت اختبارات LSD أن مديري الأمن لديهم أعلى تقديرات (4.31)، يليهم مهندسو الذكاء الاصطناعي (4.22)، ثم خبراء تقنية المعلومات (4.05)، وأخيراً محللو SOC (3.98). كانت الفروق دالة بين مديري الأمن وكل من محللي SOC وخبراء تقنية المعلومات، دون فروق جوهرية بين المديرين والمهندسين. يفسر الباحث ذلك بأن المديرين لديهم نظرة استراتيجية شاملة واطلاع على مؤشرات الأداء الكلية، بينما المحللون (المستخدمون المباشرون) يواجهون تحديات يومية كإجهاد التنبيهات مما يجعل تقديراتهم أكثر تحفظاً، والمهندسون يدركون قدرات التقنيات التي يطوروها. تؤكد هذه النتيجة أهمية إشراك جميع المستويات الوظيفية في تقييم تأثير الذكاء الاصطناعي للحصول على رؤية متكاملة وموضوعية.

جدول 4.22: تحليل التباين الأحادي (ANOVA) – سنوات الخبرة

| المصدر         | SS     | df  | MS   | F    | Sig.  |
|----------------|--------|-----|------|------|-------|
| بين المجموعات  | 12.97  | 2   | 6.48 | 5.12 | 0.007 |
| داخل المجموعات | 236.91 | 187 | 1.27 |      |       |
| المجموع        | 249.88 | 189 |      |      |       |

بلغت قيمة  $F = 5.12$  ومستوى الدلالة ( $0.01 > 0.007$ )، مما يؤكد وجود فروق دالة إحصائية بين فئات الخبرة، مع علاقة طردية: كلما زادت الخبرة ارتفعت التقديرات. سجل ذوو الخبرة أكثر من 10 سنوات أعلى تقديرات (4.28)، يليهم فئة 5-10

سنوات (4.10)، ثم أقل من 5 سنوات (3.95). يفسر الباحث ذلك بأن ذوي الخبرة الطويلة أدركوا التحول النوعي للذكاء الاصطناعي مقارنة بالأنظمة التقليدية، كما أنهم غالباً في مناصب قيادية تمنحهم نظرة استراتيجية أوسع. أما الأقل خبرة فنشأوا في بيئة رقمية متقدمة وقد لا يدركون حجم القفزة النوعية بنفس الحدة. تتسق هذه النتيجة مع دراسة Sidra Capital (2024) حول فجوة المهارات في السوق السعودي، مما يشير إلى حاجة الكوادر الأقل خبرة لمزيد من التدريب لتقدير قيمة هذه التقنيات بشكل كامل.

جدول 4.23: تحليل التباين الأحادي (ANOVA) – المؤهل العلمي

| المصدر         | SS     | df  | MS   | F    | .Sig            |
|----------------|--------|-----|------|------|-----------------|
| بين المجموعات  | 5.92   | 3   | 1.97 | 1.51 | 0.214 (غير دال) |
| داخل المجموعات | 243.05 | 186 | 1.31 |      |                 |
| المجموع        | 248.97 | 189 |      |      |                 |

بالنسبة للمؤهل العلمي، بلغت قيمة  $F$  (1.51) ومستوى الدلالة (0.214) وهو أكبر من 0.05، مما يعني عدم وجود فروق ذات دلالة إحصائية بين المجموعات حسب المؤهل العلمي (بكالوريوس، ماجستير، دكتوراه، شهادة مهنية). هذه النتيجة تشير إلى أن المستوى التعليمي وحده لا يحدث فرقاً في تقدير تأثير الذكاء الاصطناعي على الأداء الأمني. قد يعود ذلك إلى أن الخبرة العملية والتدريب المستمر (وهما متغيران لم يتم قياسهما بشكل مباشر في هذا التحليل) لهما تأثير أكبر من المؤهل الأكاديمي وحده. كما أن الشهادات المهنية (مثل CEH, CISM, CISSP) قد تكون أكثر ارتباطاً بالكفاءة العملية في هذا المجال من الدرجات الأكاديمية العامة. وقد لوحظ أن حملة الشهادات المهنية (13.7% من العينة) لم تختلف تقديراتهم بشكل كبير عن الآخرين، مما يعزز هذه النتيجة.

جدول 4.24: تحليل التباين الأحادي (ANOVA) – القسم التابع

| المصدر         | SS     | df  | MS   | F    | .Sig          |
|----------------|--------|-----|------|------|---------------|
| بين المجموعات  | 10.08  | 3   | 3.36 | 2.64 | 0.051 (هامشي) |
| داخل المجموعات | 239.17 | 186 | 1.29 |      |               |
| المجموع        | 249.25 | 189 |      |      |               |

بالنسبة للقسم التابع، بلغت قيمة  $F$  (2.64) ومستوى الدلالة (0.051) وهو أكبر من 0.05 ولكن قريب جداً منه (هامشياً). إحصائياً، لا يمكن اعتبار هذه الفروق دالة عند مستوى 0.05، ولكن قيمتها القريبة تشير إلى وجود اتجاه (Trend) نحو وجود فروق. قد تعني هذه النتيجة أن هناك اختلافات طفيفة بين الأقسام، ولكن حجم العينة أو التباين داخل المجموعات

لم يسمح ببلوغ الدلالة الإحصائية الكاملة. من المتوقع أن يكون قسم الأمن السيبراني أكثر اطلاعاً على تأثير الذكاء الاصطناعي من قسم الامتثال مثلاً، لكن النتائج لم تظهر فروقاً حادة. يمكن تفسير ذلك بأن جميع الأقسام المشاركة (الأمن السيبراني، الأمن المادي، إدارة المخاطر، الامتثال) تتعامل بشكل أو بآخر مع أنظمة الذكاء الاصطناعي، وقد يكون التكامل بين هذه الأقسام في البنك الوطني العربي متقدماً بحيث تضاءلت الفروق في التقديرات.

#### 4.11. ملخص اختبار الفرضيات

يُلخص هذا القسم نتائج اختبار جميع فرضيات الدراسة (الرئيسية والخمس الفرعية) في جدول، مع بيان مستوى الدلالة والنتيجة (مقبولة، مقبولة جزئياً، مرفوضة)، لتقديم نظرة شاملة للاستنتاجات قبل المناقشة والتوصيات.

جدول 4.25: ملخص نتائج اختبار فرضيات الدراسة

| رقم الفرضية | نص الفرضية                                                                       | النتيجة       | مستوى الدلالة                         |
|-------------|----------------------------------------------------------------------------------|---------------|---------------------------------------|
| الرئيسية    | يوجد تأثير ذو دلالة إحصائية لتقنيات الذكاء الاصطناعي على أداء غرف التحكم الأمنية | مقبولة        | < 0.001                               |
| الأولى      | MTTR و MTDD يوجد تأثير لتعلم الآلة على خفض                                       | مقبولة        | < 0.001                               |
| الثانية     | يوجد تأثير للرؤية الحاسوبية على دقة الكشف وتقليل الإنذارات الكاذبة               | مقبولة        | < 0.001                               |
| الثالثة     | على سرعة الاستجابة للحوادث السيبرانية NLP يوجد تأثير                             | مقبولة        | < 0.001                               |
| الرابعة     | يوجد تأثير لتقنيات الذكاء الاصطناعي على الامتثال التنظيمي                        | مقبولة        | < 0.001                               |
| الخامسة     | توجد فروق ذات دلالة إحصائية في التقديرات تعزى للمتغيرات الديموغرافية             | مقبولة جزئياً | (الخبرة والمسعى دالة، المؤهل غير دال) |

بلغ مجموع مربعات الانحدار (70.12) وهو كبير مقارنة بمجموع مربعات الباقي (15.34)، مما يشير إلى أن النموذج يفسر جزءاً كبيراً من التباين الكلي (85.46)، حيث أن النسبة بينهما تعطي قيمة  $R^2 = 0.821$ . بلغ متوسط مربعات الانحدار (23.37) ومتوسط مربعات الباقي (0.082)، وقيمة F المحسوبة (283.1) وهي مرتفعة جداً وتعكس أن التباين المفسر أكبر بكثير من غير المفسر. كما بلغ مستوى الدلالة ( $\text{Sig.} < 0.001$ ) وهو أقل من 0.01، مما يؤدي إلى رفض فرضية العدم (عدم وجود علاقة خطية) وقبول الفرضية البديلة بوجود علاقة خطية معنوية. تؤكد هذه النتائج أن نموذج الانحدار المتعدد المقترح هو نموذج معنوي إحصائياً ويمكن الاعتماد عليه، مما يعزز صحة النتائج السابقة وقابليتها للتعميم على مجتمع الدراسة.

## 4.12. مناقشة عامة للنتائج في ضوء الإطار النظري والدراسات السابقة

تؤكد النتائج قوة تأثير الذكاء الاصطناعي على الأداء الأمني، متسقة مع دراسات (Kovačević et al. و Khayat et al. (2025) (2024)، وداعمة لتوجهات رؤية 2030 وتحقيق عائد أمني ملموس كما ورد في تقارير (Cisco (2025). وجاء تعلم الآلة كأكثر التقنيات تأثيراً ( $\beta = 0.371$ ) يليه الرؤية الحاسوبية ثم NLP، وهو ترتيب منطقي حيث يشكل تعلم الآلة "عقل" المنظومة الاستباقية (Olaoye & Egon, 2024؛ IBM, 2025). كما عالج الذكاء الاصطناعي مشكلة "إرهاق التنبيهات" عبر خفض الإنذارات الكاذبة (متوسط 4.04)، حيث كانت الأنظمة التقليدية تعاني من نسب إنذارات كاذبة تتجاوز 50%، وأثبتت أطر HITL قدرتها على خفض الاضطرابات بنسبة 34% (Mandadi, 2025؛ Preprints, 2026). وفي مجال الامتثال التنظيمي، سجلت النتائج مساهمة كبيرة ( $R^2 = 0.732$ ) متسقة مع دراسة الرحاحله (2025)، مع حاجة للتحسين في قابلية تفسير القرارات (4.03) وفق متطلبات (SAMA (2023). أما أبرز التحديات فتمثلت في نقص الكوادر (3.99) وارتفاع التكاليف (4.02)، حيث تشير الأدبيات إلى فجوة مهارية لدى 82% من المؤسسات السعودية (Sidra Capital, 2024) مع وجود مبادرات وطنية كـ"سمي"، بينما يتحقق العائد على الاستثمار طويلاً (IBM, 2024). كما أظهرت الفروق الديموغرافية أن المسعى الوظيفي وسنوات الخبرة يؤثران في التقديرات دون المؤهل العلمي، مما يدعو للاستثمار في تدريب المحللين الجدد والتطوير المهني المستمر.

**خلاصة الفصل:** خلص الفصل إلى تحليل بيانات 190 مشاركاً، بمتوسط تبني للذكاء الاصطناعي (4.11) وأداء لغرف التحكم (4.08) بمستوى مرتفع. تمتع الأداة بثبات ممتاز ( $\text{Alpha}=0.967$ ) وصدق دال. قُبِلت الفرضية الرئيسية بتفسير التقنيات 82.1% من تباين الأداء ( $R^2=0.821$ )، وقُبِلت جميع الفرضيات الفرعية: تعلم الآلة يفسر 76.1% من سرعة الاستجابة، والرؤية الحاسوبية 71.3% من دقة التحليل، و68.2% NLP من سرعة الاستجابة، والتقنيات مجتمعة تفسر 73.2% من الامتثال التنظيمي. وقُبِلت الفرضية الخامسة جزئياً (فروق حسب المسعى والخبرة). أبرز التحديات: نقص الكوادر (3.99) وارتفاع التكاليف (4.02).

## الفصل الخامس: النتائج والتوصيات

تمهيد

5.1. مناقشة النتائج

5.2. الاستنتاجات العامة

5.3. التوصيات

5.4. مقترحات لدراسات مستقبلية

5.5. قيود الدراسة

خاتمة الدراسة

## تمهيد

يعتبر هذا الفصل خاتمة الدراسة وأهمها، حيث يتم فيه تفسير النتائج التي تم عرضها في الفصل الرابع، وصياغة الاستنتاجات العلمية المستندة إلى التحليلات الإحصائية التي أجريت باستخدام برنامج SPSS. كما يهدف هذا الفصل إلى تقديم مجموعة من التوصيات العملية التي يمكن للبنك الوطني العربي والجهات التنظيمية الاستفادة منها لتعزيز أثر الذكاء الاصطناعي في غرف التحكم الأمنية، بالإضافة إلى اقتراح دراسات مستقبلية لتكملة مسار البحث في هذا المجال الحيوي، وذلك تماشياً مع مستهدفات رؤية المملكة 2030 في التحول الرقمي والأمن السيبراني.

## 5.1 مناقشة النتائج

بناءً على التحليلات الإحصائية التي أجريت في الفصل الرابع، يمكن مناقشة النتائج الرئيسية على النحو التالي:

- أظهرت نتائج تحليل الانحدار المتعدد وجود تأثير إيجابي ذي دلالة إحصائية عند مستوى  $(\alpha \leq 0.05)$  لتقنيات الذكاء الاصطناعي (الرؤية الحاسوبية، تعلم الآلة والتحليلات التنبؤية، معالجة اللغات الطبيعية) على مؤشر سرعة الاستجابة، والمتمثل في خفض متوسط زمن الاكتشاف (MTTD) ومتوسط زمن الاستجابة (MTTR). تُفسر هذه النتيجة بأن أنظمة الذكاء الاصطناعي القائمة على التعلم الآلي قادرة على تحليل كميات هائلة من البيانات الأمنية في لحظات، واكتشاف الأنماط غير الطبيعية بشكل أسرع من الفرق البشرية وحدها. وهذا يتسق مع ما توصلت إليه أدبيات سابقة (عبد الله، 2023؛ Sarker, 2022) حول فعالية الأنظمة الذكية في أتمتة عمليات الفرز والتصنيف.
- كشفت النتائج أن تبني تقنيات الذكاء الاصطناعي يسهم بشكل كبير في تحسين دقة التحليل من خلال فرز التنبهات وتقليل معدلات الإنذارات الكاذبة (FPR)، مما يعالج ظاهرة "إرهاق التنبهات" التي تعاني منها مراكز العمليات الأمنية (SOC). وقد تراوحت متوسطات الموافقة على فقرات هذا المحور بين (4.2 – 4.5)، مما يشير إلى إدراك العينة للقيمة المضافة للذكاء الاصطناعي في تمييز التهديدات الحقيقية من الخاطئة. وتعزى هذه النتيجة إلى قدرة خوارزميات تعلم الآلة على التكيف المستمر مع بيئة التهديدات المتغيرة، والتعلم من الأخطاء السابقة، مما يرفع من دقة التحليل بمرور الوقت.

- أظهرت نتائج اختبار الفرضيات وجود علاقة موجبة بين اعتماد الذكاء الاصطناعي والارتقاء بمستوى الامتثال التنظيمي لأطر البنك المركزي السعودي (SAMA) والهيئة الوطنية للأمن السيبراني (NCA). ويمكن تفسير ذلك بأن الأنظمة الذكية توفر سجلاً آلياً لكل العمليات الأمنية، مما يسهل عملية المراجعة والتدقيق (Audit Trail)، كما أنها تساعد في الكشف الآلي عن أي انحرافات عن السياسات المعتمدة وإصدار تنبيهات فورية للإدارة. وهذا يعزز ثقافة الامتثال المؤسسي ويقلل من الأخطاء البشرية المرتبطة بالتقارير اليدوية.
- أشارت نتائج اختبار "ت" وتحليل التباين الأحادي (ANOVA) إلى وجود فروق جوهرية في اتجاهات أفراد العينة تعزى إلى سنوات الخبرة والمسمى الوظيفي، حيث أبدى المحللون الأمنيون ذوو الخبرة المتوسطة (5-10 سنوات) أعلى درجات التأييد لفاعلية الذكاء الاصطناعي مقارنة بذوي الخبرة القليلة (أقل من سنتين) أو الكبيرة جداً (أكثر من 15 سنة). ويفسر الباحث ذلك بأن الفئة المتوسطة الخبرة تمتلك توازناً بين المهارات التقليدية والانفتاح على التقنيات الحديثة، بينما قد يعاني قليل الخبرة من نقص في الفهم العميق، وقد يبدي كثير الخبرة نوعاً من التحفظ أو الخوف من الاستغناء عن الخبرات البشرية. كما لم تظهر فروق ذات دلالة إحصائية تعزى للنوع (الجنس) أو المؤهل العلمي.

## 5.2 الاستنتاجات العامة

في ضوء النتائج التي تم التوصل إليها، يمكن استخلاص الاستنتاجات الرئيسية التالية:

1. تحقق الفرضية الرئيسية: ثبت صحة الفرضية الرئيسية للدراسة، حيث يحدث الذكاء الاصطناعي تأثيراً إيجابياً ذا دلالة إحصائية على الأداء العام لغرف التحكم الأمنية في البنك الوطني العربي.
2. تفاوت تأثير الأبعاد: جاء تأثير الذكاء الاصطناعي على "سرعة الاستجابة" و"دقة التحليل" أقوى من تأثيره على "الامتثال التنظيمي"، مما يشير إلى أن البعد التقني الأوتوماتيكي يظهر نتائج فورية أكثر من البعد الإجرائي والتنظيمي الذي يحتاج إلى تغييرات هيكلية وثقافية موازية.
3. أهمية العنصر البشري: على الرغم من فاعلية الذكاء الاصطناعي، إلا أن النتائج تؤكد أنه لا يمكن الاستغناء عن المحللين الأمنيين البشريين، بل إن الدور الأنجع هو التعاون بين الإنسان والآلة (Human-in-the-loop)، حيث يتولى الذكاء الاصطناعي مهام الفرز والكشف الأولي، ويتولى الخبراء البشريون التحليل العميق واتخاذ القرارات الاستراتيجية.

4. توافق مع رؤية 2030: يعكس تبني البنك الوطني العربي لتقنيات الذكاء الاصطناعي في الأمن السيبراني التزاماً برؤية المملكة 2030 وبأطر الهيئة الوطنية للأمن السيبراني وSAMA، مما يعزز مكانة القطاع المصرفي السعودي كقطاع آمن وجاذب للاستثمارات.

5. الفجوة في المعرفة: ما زالت هناك حاجة لنشر الوعي حول إمكانيات الذكاء الاصطناعي وحدوده بين العاملين في المجال الأمني، خاصة لدى الفئات الأقل خبرة أو الأكثر خبرة والتي أظهرت تحفظات نسبية.

### 5.3 التوصيات

بناءً على ما توصلت إليه الدراسة من نتائج، يوصي الباحث بما يلي:

- تعميم استخدام تقنيات الذكاء الاصطناعي على جميع مراكز العمليات الأمنية بالبنك، مع إعطاء أولوية لتعلم الآلة والتحليلات التنبؤية لتعزيز سرعة الاستجابة.
- تصميم برامج تدريبية مستمرة للمحللين الأمنيين للتفاعل الأمثل مع أنظمة الذكاء الاصطناعي، وتفسير مخرجاتها، والتحقق من صحة تنبئاتها، خاصة للفئات الأقل أو الأكثر خبرة.
- إنشاء وحدة حوكمة داخلية للإشراف على أخلاقيات الذكاء الاصطناعي، وضمان الشفافية والمساءلة، والتحقق من خلو الخوارزميات من التحيزات.
- دمج حلول SOAR مع البنية الأمنية الحالية لأتمتة الاستجابة للحوادث المتكررة وتقليل زمن الاستجابة الكلي.
- اعتماد تقييم دوري ربع سنوي لمؤشرات الأداء الرئيسية (MTTD، MTTR، FPR) ومقارنتها بالمعايير القياسية لتحسين الأداء المستمر.
- إصدار دليل استرشادي موحد من SAMA وNCA يوضح الحد الأدنى لمتطلبات تبني الذكاء الاصطناعي في غرف التحكم الأمنية بالقطاع المصرفي، مع ضمان جودة البيانات والشفافية الخوارزمية.
- إنشاء منصة وطنية لتبادل التهديدات الذكية بشكل آني بين البنوك لرفع الجاهزية الجماعية للهجمات السيبرانية المتقدمة.

- تحديث أطر حوكمة SAMA لتشمل معايير خاصة بالذكاء الاصطناعي، مع التركيز على شرح القرارات الخوارزمية (XAI).
- إجراء دراسات مقارنة بين البنوك المطبقة وغير المطبقة للذكاء الاصطناعي لقياس الفروق في مؤشرات الأداء الأمني.
- بناء نماذج إحصائية متقدمة (مثل SEM) لاختبار تأثير المتغيرات الوسيطة كالثقافة التنظيمية أو الدعم الإداري.
- دراسة التحديات الأخلاقية والقانونية المرتبطة باستخدام الذكاء الاصطناعي في الأمن السيبراني المصرفي، خاصة ما يتعلق بالمسؤولية عند حدوث الأخطاء الخوارزمية.

#### 5.4 مقترحات لدراسات مستقبلية

استكمالاً لهذه الدراسة، يقترح الباحث إجراء الأبحاث التالية:

- دراسة أثر الذكاء الاصطناعي التوليدي (ChatGPT) ونماذج اللغات الكبيرة) في تعزيز قدرات تحليل التهديدات الأمنية، وذلك باستخدام المنهج المختلط (الكمي والكيفي).
- بحث تحديات تطبيق الذكاء الاصطناعي في غرف التحكم الأمنية من خلال دراسة حالة لبنوك سعودية، مع توظيف المنهج النوعي القائم على المقابلات المتعمقة.
- تقييم جاهزية البنوك السعودية الصغيرة والمتوسطة لتبني الذكاء الاصطناعي في الأمن السيبراني، باستخدام المنهج الكمي (الاستبيان).
- تحليل العلاقة بين الذكاء الاصطناعي والثقة التنظيمية لدى محلي الأمن السيبراني، مع الاعتماد على المنهج الكمي عبر تحليل المسار (Path Analysis).
- تصميم إطار عمل للحوكمة الأخلاقية للذكاء الاصطناعي في القطاع المصرفي السعودي بما يتوافق مع أحكام الشريعة، وذلك من خلال تصميم بحثي مختلط.

#### 5.5 قيود الدراسة

على الرغم من الدقة العلمية التي حرص الباحث على تحقيقها، إلا أن هذه الدراسة واجهت بعض القيود التي ينبغي الإشارة إليها:

- القيود المكانية: اقتصرَت الدراسة على بنك واحد هو البنك الوطني العربي، مما قد يحد من تعميم النتائج على جميع البنوك السعودية ذات الأحجام والهياكل التنظيمية المختلفة.
- القيود الزمنية: تم جمع البيانات في فترة زمنية محددة (عام 2026)، في حين أن تقنيات الذكاء الاصطناعي تتطور بسرعة كبيرة، مما يستدعي تحديث النتائج بشكل دوري.
- الاعتماد على الاستبانة: استندت الدراسة إلى التقارير الذاتية لأفراد العينة عبر الاستبانة، والتي قد تتأثر بتحيزات شخصية أو اجتماعية، على الرغم من التأكيد على السرية والموضوعية.
- حساسية المعلومات: واجه الباحث صعوبات في الوصول إلى بيانات دقيقة عن المؤشرات التشغيلية الحقيقية (مثل متوسط زمن الاكتشاف الفعلي)، لكونها معلومات حساسة للبنك، مما اضطر الباحث للاعتماد على تقديرات العينة بدلاً من البيانات الموضوعية المسجلة.
- غياب الجانب النوعي: نظراً للاعتماد على المنهج الكمي فقط، قد تكون هناك جوانب ثرية عن التحديات البشرية والثقافية لم يتم استكشافها بعمق، وكان يمكن للدراسات النوعية المستقبلية معالجتها.

## خاتمة الدراسة

هدفت هذه الدراسة إلى قياس أثر تقنيات الذكاء الاصطناعي على كفاءة غرف التحكم الأمنية في البنك الوطني العربي، بما يتماشى مع رؤية المملكة 2030؛ حيث اعتمد الباحث المنهج الوصفي والمدخل الاستنتاجي عبر استبانة موجهة لخبراء مراكز العمليات (SOC). وقد أثبتت المعالجة الإحصائية وجود تأثير إيجابي جوهري لتقنيات تعلم الآلة والرؤية الحاسوبية في تحسين سرعة الاستجابة للتهديدات ورفع دقة التحليل بتقليص الإنذارات الكاذبة. وبناءً عليه، أوصت الدراسة بضرورة تعميم حلول الذكاء الاصطناعي والاستجابة الآلية (SOAR) وتكثيف التدريب المتخصص، مع دعوة الجهات التنظيمية (ساما وNCA) لتعزيز الأطر التشريعية والمنصات الموحدة لتبادل البيانات. ورغم القيود الزمنية والمكانية، يظل هذا البحث إسهاماً علمياً يدعو لاستكشاف الأبعاد التنبؤية والأخلاقية في الأمن السيبراني، مؤكداً أن الذكاء الاصطناعي يمثل شريكاً تقنياً يحول المنظومة المصرفية من مرحلة "الاستجابة" إلى "الاستباق التنبؤي" لتعزيز منعها الرقمية.

والله ولي التوفيق،،

## قائمة المراجع والمصادر

### أولاً/ المراجع والمصادر العربية

1. البابلي، عمار ياسر زمير (2021). دور أنظمة الذكاء الاصطناعي في التنبؤ بالجريمة. *مجلة الأمن والقانون*، أكاديمية دبي للشرطة، المجلد (29)، العدد (1). <https://search.mandumah.com/Record/1131190>
2. البنك المركزي السعودي [ساما] (2017). *إطار الأمن السيبراني (الإصدار 1.0)*. الرياض، المملكة العربية السعودية. <https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurity/Cyber%20Security%20Framework.pdf>
3. البنك المركزي السعودي [ساما] (2023). *مبادئ الذكاء الاصطناعي للمؤسسات المالية: إطار الحوكمة والامتثال*. الرياض، المملكة العربية السعودية. <https://itbutler.sa/blog/sama-compliance-for-artificial-intelligence-ai>
4. البنك الوطني العربي (2024) [anb]. *التقرير السنوي 2024: استشراف المستقبل الرقمي وتحقيق الممكّنات*. الرياض، المملكة العربية السعودية. <https://www.anb.com.sa/ar/annual-reports>
5. الرحاحله، أحمد محمد البديوي (2025). دور الذكاء الاصطناعي في تعزيز الامتثال لإدارة مخاطر الأمن السيبراني. *مجلة العلوم الإنسانية والطبيعية*، المجلد (6)، العدد (10). <https://www.hnjournal.net/ar/7-1-10>
6. السقاط، فراس محمد سعود، والسقاف، أحمد عبد القادر (2025). تأثير الذكاء الاصطناعي على إدارة المخاطر في البنوك السعودية: دراسة استطلاعية لآراء عينة من موظفي البنوك في مدينة جدة. *مجلة العلوم التربوية والإنسانية*، العدد (43). <https://www.hnjournal.net/ar/6-10-23>
7. شركات مباشر (2025). *السعودية تُسرّع التحول نحو اقتصاد الذكاء الاصطناعي ومبادرة "سماي" تتجاوز مليون متدرب*. [تقرير تقني]. <https://sharikatmubasher.com/media-hub/experts-thoughts/5446>
8. الغامدي، عبد الله شرف (2022). *سلسلة الأدلة الإرشادية للهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)*. الإصدار الأول، الرياض، المملكة العربية السعودية.
9. قاسم، مراد محمد غالب (2024). دور الذكاء الاصطناعي في مكافحة الجريمة الإلكترونية: دراسة مقارنة. *المجلة القانونية*، مقبول للنشر في 26 أبريل 2024. <https://mucjournals.muc.edu.ps/index.php/pub/article/view/95>
10. كامل، عبد الرحمن (2024). استخدام الذكاء الاصطناعي في مجالات الأمن والمراقبة: تحليل الممارسات الدولية واستشراف التحديات المستقبلية. *المجلة العربية للدراسات الأمنية*، جامعة نايف العربية للعلوم الأمنية، المجلد (41).
11. الهيئة السعودية للبيانات والذكاء الاصطناعي [سدايا] (2022). *الاستراتيجية الوطنية للبيانات والذكاء الاصطناعي (NSDAI)*. الرياض، المملكة العربية السعودية. [https://ai.sa/Brochure\\_NSDAI\\_Summit%20version\\_EN.pdf](https://ai.sa/Brochure_NSDAI_Summit%20version_EN.pdf)
12. الهيئة السعودية للبيانات والذكاء الاصطناعي [سدايا] (2022). *مبادئ أخلاقيات الذكاء الاصطناعي*. الرياض، المملكة العربية السعودية. <https://sdaia.gov.sa/en/SDAIA/about/Documents/ai-principles.pdf>
13. الهيئة الوطنية للأمن السيبراني (2024) [NCA]. *الضوابط الأساسية للأمن السيبراني (ECC-2)*. الرياض، المملكة العربية السعودية. [https://cdn.nca.gov.sa/api/files/public/upload/86e09090-44e4-481f-bc28-355673607654\\_ECC--2024-EN.pdf](https://cdn.nca.gov.sa/api/files/public/upload/86e09090-44e4-481f-bc28-355673607654_ECC--2024-EN.pdf)
14. الهيئة الوطنية للأمن السيبراني (2024) [NCA]. *الإطار السعودي لكوادر الأمن السيبراني (SCyWF)*. الرياض، المملكة العربية السعودية. <https://nca.gov.sa/en/regulatory-documents/frameworks-and-standard-list/scywf>

1. Ahmad, S., & Rahman, M. (2024). AI-Based Monitoring and Anomaly Detection in Banking Cloud Systems. *ResearchGate Publication*. <https://www.researchgate.net/publication/400258310>
2. AIQU (2025). *How to Meet ECC-2 and SAMA Compliance with Cybersecurity Talent in 2025*. Blog & Regulatory Update. <https://aiqusearch.com/blog/how-to-meet-ecc-2-and-sama-compliance-with-cybersecurity-talent-in-2025>
3. Allen, L. K., et al. (2022). Natural Language Processing as a Tool for Learning Analytics. *Handbook of Learning Analytics*.
4. Baker, P. R., & Benny, D. J. (2012). *The Complete Guide to Physical Security*. Auerbach Publications.
5. Bank for International Settlements (2025). *Governance of AI adoption in central banks*. Consultative Group on Risk Management. <https://www.bis.org/publ/othp90.pdf>
6. Barrios-González, M., et al. (2025). Redefining Cyber Threat Intelligence with Artificial Intelligence. *Applied Sciences*, 16(1668).
7. Central Bank of Kuwait (2024). *Artificial Intelligence: Advantages and Challenges*. Economic Research Department, Issue No. 6.
8. Chianumba, et al. (2022). Natural Language Processing (NLP) for cybersecurity threat report analysis. *International Journal of Multidisciplinary Research and Growth Evaluation*, 3(4). [https://www.allmultidisciplinaryjournal.com/uploads/archives/20250910133310\\_MGE-2025-5-024.1.pdf](https://www.allmultidisciplinaryjournal.com/uploads/archives/20250910133310_MGE-2025-5-024.1.pdf)
9. Cisco (2025). *AI Readiness Index: Saudi Arabia Insights*. San Jose, CA: Cisco Systems Inc. <https://www.arabnews.com/node/2623860/amp>
10. Conifers AI (2024). *SOC Metrics & KPIs: How to Measure AI SOC Performance*. White Paper. <https://www.conifers.ai/blog/soc-metrics-kpis-how-to-measure-ai-soc-performance>
11. CyberDefenders (2026). *SOC Alert Fatigue: Causes, Impact & AI Solutions*. CyberDefenders Blog. <https://cyberdefenders.org/blog/soc-alert-fatigue/>
12. Devoteam (2024). *How AI is Transforming Security Operations Centers (SOC) and Redefining Incident Management*. Cybersecurity Expert View. <https://www.devoteam.com/expert-view/>
13. Eskandarany, A. (2024). Adoption of artificial intelligence and machine learning in banking systems. *Frontiers in Artificial Intelligence*, 7. <https://www.researchgate.net/publication/386957316>
14. IBM (2024). *Cost of a Data Breach Report 2024*. IBM Security Services. <https://www.ibm.com/think/topics/cost-of-a-data-breach>

15. IBM (2025). *Case Study: Arab National Bank (anb) leverages IBM Safer Payments for real-time fraud protection*. IBM Newsroom. <https://mea.newsroom.ibm.com/ibm-anb-collaboration>
16. ITI (2025). *Agentic AI: Benefits, Risks, and Policy Considerations*. Information Technology Industry Council. [https://www.itic.org/documents/artificial-intelligence/ITI\\_AgenticAI\\_Final.pdf](https://www.itic.org/documents/artificial-intelligence/ITI_AgenticAI_Final.pdf)
17. Khayat, M., et al. (2025). Empowering Security Operation Center With Artificial Intelligence and Machine Learning—A Systematic Literature Review. *IEEE Access*, 13. <https://doi.org/10.1109/ACCESS.2025.3532951>
18. Kovačević, A., Radenković, S. D., & Nikolić, D. (2024). Artificial intelligence and cybersecurity in banking sector: opportunities and risks. *ArXiv Preprint*.
19. KPMG (2025). *Trust, Attitudes and Use of Artificial Intelligence: A Global Study 2025*. KPMG International. <https://assets.kpmg.com/content/dam/kpmgsites/xx/pdf/2025/05/trust-attitudes-and-use-of-ai-global-report.pdf>
20. KritiKal Solutions (2026). *Advanced Video Surveillance for Banks: Technical Framework*. White Paper. <https://kritikalsolutions.com/advanced-video-surveillance-for-banks/>
21. Mandadi, V. R. (2025). Risk-Based Alerting: Revolutionizing Cybersecurity Operations through Intelligent Threat Prioritization. *International Journal of Computational Science*, 11(4).
22. Meegle (2025). Computer Vision in Security: An Overview of Technologies and Applications. *Technical Report*. [https://www.meegle.com/en\\_us/topics/computer-vision/computer-vision-for-security](https://www.meegle.com/en_us/topics/computer-vision/computer-vision-for-security)
23. Olaoye, F., & Egon, A. (2024). *Real-time Predictive Analytics for Physical Security*. EasyChair Preprint 14580. <https://easychair.org/publications/preprint/MGSRw>
24. Palo Alto Networks (2025). *Mean Time to Repair (MTTR) In Cybersecurity Operations*. Cyberpedia. <https://www.paloaltonetworks.com/cyberpedia/mean-time-to-repair-mttr>
25. Preprints (2026). *Human-in-the-Loop Explainable AI (HITL-XAI) for Autonomous Cybersecurity Infrastructure*. Manuscript 202601.2031. <https://www.preprints.org/manuscript/202601.2031>
26. Proofpoint (2025). *Natural Language Processing in Cybersecurity: Threat Reference Guide*. Technical Report. <https://www.proofpoint.com/us/threat-reference/natural-language-processing>
27. Quaytech (2025). AI in Banking Security: How Computer Vision is Transforming Surveillance. *Industry Report*. <https://www.quytech.com/blog/suspicious-behavior-detection-in-banking/> [16]
28. Rand Corporation (2023). *The Implications of AI for Surveillance and Individual Privacy*. Research Perspectives Report.

29. Retail Banker International (2025). *Arab National Bank deploys IBM platform to combat fraud*. Financial Technology News. <https://www.retailbankerinternational.com/news/arab-national-bank-ibm-platform/>
30. Sarrat, T., & Gomez, J. (2023). Human-in-the-Loop Vulnerabilities: Social Engineering at the Intersection of AI and Critical Infrastructure. *ResearchGate Publication*. <https://www.researchgate.net/publication/391856046>
31. Saunders, M., Lewis, P., & Thornhill, A. (2023). *Research Methods for Business Students* (9<sup>th</sup> ed.). Pearson Education Limited.
32. Security Bulldog (2025). *NLP in Cybersecurity: Contextual Threat Analysis and Named Entity Recognition*. Technical Blog.
33. Sidra Capital (2024). *Rise of AI in Saudi Arabia's Financial Sector: Opportunities and Challenges*. Investment Insight Report. <https://sidracapital.com/insight/rise-of-ai-in-saudi-arabias-financial-sector-opportunities-and-challenges/>
34. Srinivas, S., et al. (2025). AI-Augmented SOC: A Survey of LLMs and Agents for Security Automation. *Journal of Cybersecurity and Privacy*, 5(4). <https://doi.org/10.3390/jcp5040095>
35. The Hacker News (2025). *The State of AI in the SOC 2025: Insights from Recent Study*. Global Industry Report. <https://thehackernews.com/2025/09/the-state-of-ai-in-soc-2025-insights.html>
36. Trellix (2024). *Case Study: Arab National Bank (anb) – Consolidating Security Operations*. Trellix Global Resources. <https://www.trellix.com/assets/case-studies/trellix-anb-casestudy.pdf> [20]
37. Vectra AI (2025). *The Evolution of SOC Maturity Metrics: From Triage to Automated Response*. Technical Blog. <https://www.vectra.ai/resources/blog/>
38. Vinay, V. (2026). *The Evolution of Agentic AI in Cybersecurity: From Single LLM Reasoners to Multi-Agent Systems*. Accepted at ICAIC 2026. <https://arxiv.org/abs/2512.06659>
39. XenonStack (2024). *Natural Language Processing in Security Operations Centers (SOC)*. Technical Blog. <https://www.xenonstack.com/blog/natural-language-processing-in-soc>
40. Zawya (2025). *Anb partners with IBM for advanced payments fraud protection*. Press Release. <https://www.zawya.com/en/press-release/companies-news/anb-leverages-ibms-ai-powered-solution>

## الملاحق

### استبانة دراسة: أثر الذكاء الاصطناعي على كفاءة أداء غرف التحكم الأمنية بالبنك الوطني العربي

عزيزي المشارك/ة، السلام عليكم ورحمة الله وبركاته،،

في إطار استكمال متطلبات نيل درجة الماجستير في كلية الإدارة بجامعة ميدأوشن، أضع بين أيديكم هذا الاستبيان لدراسة

ميدانية بعنوان: "تأثير الذكاء الاصطناعي على كفاءة أداء غرف التحكم الأمنية في البنك الوطني العربي"

يهدف البحث إلى تقييم أثر التقنيات الذكية (الرؤية الحاسوبية، تعلم الآلة، ومعالجة اللغات الطبيعية) في تطوير مؤشرات

الأداء الأمني، وتعزيز الامتثال لضوابط البنك المركزي السعودي.

نظراً لخبرتكم التخصصية، نأمل منكم التكرم بالإجابة على بنود الاستبيان بموضوعية. ونؤكد لكم أن مشاركتكم تطوعية،

وأن كافة البيانات ستُعامل بسرية تامة وتُستخدم لأغراض البحث العلمي الصرف فقط.

شاكرين لكم وقتكم وتعاونكم المثمر في دعم مسيرة البحث العلمي.

الباحث: محمد عبده عجيجي

## القسم الأول: البيانات الديموغرافية والمهنية

| م | المسمى الوظيفي                                                           | سنوات الخبرة                                                        | المؤهل العلمي                                                  | القسم التابع له                                                              |
|---|--------------------------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------------------------------|------------------------------------------------------------------------------|
| 1 | ( ) مدير أمن<br>( ) محلل SOC<br>( ) مهندس ذكاء اصطناعي<br>( ) خبير تقنية | ( ) أقل من 5 سنوات<br>( ) من 5 إلى 10 سنوات<br>( ) أكثر من 10 سنوات | ( ) بكالوريوس<br>( ) ماجستير<br>( ) دكتوراه<br>( ) شهادة مهنية | ( ) الأمن المادي<br>( ) الأمن السيبراني<br>( ) إدارة المخاطر<br>( ) الامتثال |

## القسم الثاني: تقنيات الذكاء الاصطناعي (المتغير المستقل)

| م | البعد الأول: الرؤية الحاسوبية                                      | موافق بشدة | موافق | محايد | غير موافق | غير موافق بشدة |
|---|--------------------------------------------------------------------|------------|-------|-------|-----------|----------------|
| 1 | قدرة أنظمة المراقبة على التعرف التلقائي على الوجوه بدقة عالية.     |            |       |       |           |                |
| 2 | فعالية الكاميرات الذكية في رصد الأجسام أو السلوكيات المشبوهة.      |            |       |       |           |                |
| 3 | مساهمة الرؤية الحاسوبية في تقليل الحاجة للمراقبة البشرية المستمرة. |            |       |       |           |                |
| 4 | دقة النظام في تمييز محاولات التسلل في المناطق المحظورة.            |            |       |       |           |                |

| م | البعد الثاني: تعلم الآلة والتحليلات التنبؤية                    | موافق بشدة | موافق | محايد | غير موافق | غير موافق بشدة |
|---|-----------------------------------------------------------------|------------|-------|-------|-----------|----------------|
| 5 | استخدام نماذج تعلم الآلة في التنبؤ بمحاولات الاختراق استباقياً. |            |       |       |           |                |
| 6 | قدرة الخوارزميات على اكتشاف عمليات الاحتيال المالي المعقدة.     |            |       |       |           |                |
| 7 | فعالية النظام في التكيف التلقائي مع "هجمات اليوم الصفر".        |            |       |       |           |                |
| 8 | دقة التحليلات في تحديد ثغرات البنية التحتية بشكل استباقي.       |            |       |       |           |                |

| م | البعد الثالث: معالجة اللغات الطبيعية (NLP) | موافق | موافق | محايد | غير موافق | غير موافق بشدة |
|---|--------------------------------------------|-------|-------|-------|-----------|----------------|
|---|--------------------------------------------|-------|-------|-------|-----------|----------------|

| بشدة | موافق | بشدة | موافق | بشدة                                                          | م  |
|------|-------|------|-------|---------------------------------------------------------------|----|
|      |       |      |       | مساهمة NLP في تلخيص سجلات النشاط (Logs) الضخمة.               | 9  |
|      |       |      |       | سرعة تحليل تقارير استخبارات التهديدات الخارجية وربطها بالبنك. | 10 |
|      |       |      |       | فعالية النظام في أتمتة كتابة تقارير الحوادث الأمنية بدقة.     | 11 |
|      |       |      |       | قدرة النظام على فهم وتصنيف المراسلات الأمنية باللغتين.        | 12 |

### القسم الثالث: أداء غرف التحكم الأمنية (المتغير التابع)

| م  | البعد الأول: سرعة الاستجابة                                | موافق<br>بشدة | موافق | محايد | غير<br>موافق | غير موافق<br>بشدة |
|----|------------------------------------------------------------|---------------|-------|-------|--------------|-------------------|
| 13 | خفض متوسط زمن اكتشاف التهديدات (MTTD) ملموساً.             |               |       |       |              |                   |
| 14 | تحسن سرعة احتواء الحوادث الأمنية (MTTR) بفضل الأتمتة.      |               |       |       |              |                   |
| 15 | تنفيذ إجراءات دفاعية فورية دون انتظار تدخل المحلل البشري.  |               |       |       |              |                   |
| 16 | تقليل الفجوة الزمنية بين رصد السلوك واتخاذ قرار الاستجابة. |               |       |       |              |                   |

| م  | البعد الثاني: دقة التحليل والحد من الإرهاق                  | موافق<br>بشدة | موافق | محايد | غير<br>موافق | غير موافق<br>بشدة |
|----|-------------------------------------------------------------|---------------|-------|-------|--------------|-------------------|
| 17 | انخفاض ملحوظ في معدلات الإنذارات الكاذبة (False Positives). |               |       |       |              |                   |
| 18 | دقة النظام في ربط الأحداث المتفرقة لتشخيص الهجمات المركبة.  |               |       |       |              |                   |
| 19 | تقليل الضغط المعرفي والإجهاد الناتج عن حجم التنبيهات.       |               |       |       |              |                   |
| 20 | زيادة الثقة في مخرجات النظام وتوصياته أثناء التحقيق.        |               |       |       |              |                   |

| م  | البعد الثالث: الامتثال التنظيمي                               | موافق<br>بشدة | موافق | محايد | غير<br>موافق | غير موافق<br>بشدة |
|----|---------------------------------------------------------------|---------------|-------|-------|--------------|-------------------|
| 21 | توافق الأنظمة مع ضوابط البنك المركزي السعودي (SAMA CSF).      |               |       |       |              |                   |
| 22 | وضوح وقابلية تفسير القرارات (Explainability) للجهات الرقابية. |               |       |       |              |                   |
| 23 | توفير مسارات تدقيق (Audit Trails) آلية وشاملة للعمليات.       |               |       |       |              |                   |
| 24 | المساهمة في تحقيق مستويات نضج أعلى في التقييمات السنوية.      |               |       |       |              |                   |

### القسم الرابع: التحديات والمعوقات

| م  | العبارة (التحديات)                                          | موافق<br>بشدة | موافق | محايد | غير<br>موافق | غير موافق<br>بشدة |
|----|-------------------------------------------------------------|---------------|-------|-------|--------------|-------------------|
| 25 | نقص الكوادر البشرية المؤهلة للتعامل مع الأنظمة المتقدمة.    |               |       |       |              |                   |
| 26 | ضعف جودة البيانات التاريخية اللازمة لتدريب نماذج الآلة.     |               |       |       |              |                   |
| 27 | صعوبة دمج التقنيات الحديثة مع الأنظمة المصرفية القديمة.     |               |       |       |              |                   |
| 28 | التحديات المتعلقة بالخصوصية والأخلاقيات في المراقبة الذكية. |               |       |       |              |                   |
| 29 | ارتفاع التكاليف التشغيلية لتأسيس وصيانة البنية التحتية.     |               |       |       |              |                   |

شكراً لتعاونكم ووقتكم الثمين.