السنة الرابعة والعشرون/ عدد خاص/ تموز 2026
https://doi.org/10.31272/ijes.v24.1544

المجلة العراقية للعلوم الاقتصادية
Iraqi Journal For
Economic Sciences

PISSN : 1812-8742 EISSE : 2791-092X Arcif : 0.375

The Impact of Intelligent Audit Automation on Cyber Resilience: An Applied Study at Iraq's Cyber Emergency Response Team (IQ-CERT)

أثر تبنّي الأتمتة الذكية في عمليات التدقيق على تعزيز المرونة السيبرانية دراسة تطبيقية في فريق الاستجابة للطوارئ الميدانية (IQ – CERT)

م. د. منار حيدر علي الغانمي
Manar Haider Ali
manar.hayder@iku.edu.iq

م.د. عقيل علوان محسن الجبوري
Aqeel Alwan Mohsen
finbabel9@iku.edu.iq

كلية الامام الكاظم (ع) للعلوم الاسلامية الجامعة/ اقسام بابل

Abstract

The present study examines the impact of intelligent audit automation on enhancing cyber resilience through an applied investigation at Iraq's Cyber Emergency Response Team. Cyber threats are becoming increasingly sophisticated, and traditional manual auditing approaches are often insufficient to detect and mitigate risks promptly. This research addresses the critical question of how advanced automated auditing tools can improve the accuracy, efficiency, and responsiveness of cyber incident management. An applied research methodology is adopted, relying on official reports, operational records, and verified data provided by IQ-CERT and other trusted governmental sources. The study systematically analyzes the relationship between the deployment of intelligent audit automation and the organization's capacity to anticipate, detect, and respond to cyber threats. The findings reveal that intelligent audit automation significantly enhances cyber resilience by reducing response times, improving threat detection accuracy, and optimizing resource allocation during cyber incidents. Moreover, the research highlights practical implications for policy-making and organizational strategies, emphasizing the necessity of integrating automation technologies within national cybersecurity frameworks. The study contributes to both theoretical understanding and practical application by providing evidence-based insights into the role of automation in strengthening organizational cyber resilience. Recommendations for optimizing audit automation practices and leveraging emerging technologies to reinforce national cybersecurity capabilities are also presented.

Keywords: Intelligent Audit Automation, Cyber Resilience, IQ-CERT, Applied

Study, Cybersecurity Management

المستخلص

تتناول هذه الدراسة أثر أتمتة التدقيق الذكي على تعزيز الأمن السيبراني، من خلال دراسة تطبيقية فريق الاستجابة للأحداث السيبرانية بالعراق. تتزايد تعقيدات التهديدات السيبرانية، وغالبًا ما تكون أساليب التدقيق اليدوي التقليدية غير كافية للكشف عن المخاطر والتخفيف من آثارها بسرعة. يتناول هذا البحث السؤال المحوري حول كيفية مساهمة أدوات التدقيق الآلي المتقدمة في تحسين دقة وكفاءة وسرعة استجابة إدارة الحوادث السيبرانية. تعتمد الدراسة منهجية بحث تطبيقية، بالاعتماد على التقارير الرسمية والسجلات التشغيلية والبيانات الموثقة المقدمة من فريق الاستجابة للطوارئ السيبرانية بالعراق ومصادر حكومية موثوقة أخرى. تحلل الدراسة بشكل منهجي العلاقة بين تطبيق أتمتة التدقيق الذكي وقدرة المنظمة على توقع التهديدات السيبرانية والكشف عنها والاستجابة لها. تكشف النتائج أن أتمتة التدقيق الذكي تعزز بشكل ملحوظ الأمن السيبراني من خلال تقليل أوقات الاستجابة، وتحسين دقة الكشف عن التهديدات، وترشيد تخصيص الموارد أثناء الحوادث السيبرانية. علاوة على ذلك، يسلط البحث الضوء على الآثار العملية على صنع السياسات والاستراتيجيات التنظيمية، مؤكدًا على ضرورة دمج تقنيات الأتمتة ضمن أطر الأمن السيبراني الوطنية. تُسهم هذه الدراسة في تعزيز الفهم النظري والتطبيق العملي من خلال تقديم رؤى قائمة على الأدلة حول دور الأتمتة في تعزيز المرونة السيبرانية للمؤسسات. كما تُقدم توصيات لتحسين ممارسات أتمتة التدقيق والاستفادة من التقنيات الناشئة لتعزيز القدرات الوطنية في مجال الأمن السيبراني.

الكلمات الرئيسية: الأتمتة الذكية للتدقيق، الصمود السيبراني، فريق الاستجابة للأحداث السيبرانية العراقي (IQ-CERT)، دراسة تطبيقية، إدارة الأمن السيبراني

المقدمة

في عصرنا الرقمي، تتطور التهديدات السيبرانية بوتيرة غير مسبوقة، مما يشكل تحديات جسيمة للمؤسسات والأمن القومي على حد سواء. غالبًا ما تكون أساليب التدقيق والمراقبة اليدوية التقليدية غير كافية لتحديد المخاطر السيبرانية المعقدة والتخفيف من آثارها في الوقت المناسب. ونتيجة لذلك، تتجه المؤسسات بشكل متزايد إلى أدوات أتمتة التدقيق الذكية، التي تستفيد من الخوارزميات المتقدمة والذكاء الاصطناعي وتحليلات البيانات الآنية لتعزيز دقة وكفاءة واستجابة تدابير الأمن السيبراني. أصبحت المرونة السيبرانية - أي قدرة المؤسسة على توقع الحوادث السيبرانية ومواجهتها والتعافي منها - هدفًا بالغ الأهمية للمؤسسات الحكومية والخاصة على حد سواء. في العراق، يضطلع فريق الاستجابة للطوارئ السيبرانية بدور محوري في حماية البنية التحتية الرقمية الوطنية والاستجابة للحوادث السيبرانية. وعلى الرغم من أهميته الاستراتيجية، إلا أن هناك بحوثًا تجريبية محدودة تتناول كيفية تأثير تبني أتمتة التدقيق الذكية على المرونة السيبرانية لهذه المؤسسات الحيوية. تهدف هذه الدراسة إلى سدّ هذه الفجوة من خلال إجراء بحث تطبيقي في مركز الاستجابة للحوادث السيبرانية وتحليل أثر أتمتة التدقيق الذكي على قدرة المركز على كشف التهديدات السيبرانية ومنعها والتصدي لها. يستند البحث إلى تقارير رسمية وبيانات تشغيلية ومصادر حكومية موثوقة لتقديم تقييم قائم على أسس علمية. ومن خلال دراسة العلاقة بين أتمتة التدقيق والمرونة السيبرانية، تسعى الدراسة إلى تقديم رؤى عملية لصناع السياسات، والمتخصصين في الأمن السيبراني، والباحثين المهتمين بتعزيز فعالية آليات الدفاع السيبراني. لا تكمن أهمية هذا البحث في إسهامه في المعرفة الأكاديمية فحسب، بل في تطبيقاته العملية لتعزيز قدرات العراق الوطنية في مجال الأمن السيبراني. ومن المتوقع أن تُسهم النتائج في توجيه عملية صنع القرار الاستراتيجي، وتحسين تخصيص الموارد، وتوجيه تطبيق أدوات التدقيق الذكي لتحسين جاهزية المؤسسات لمواجهة التهديدات السيبرانية.

منهجية البحث

أولا: مشكلة البحث: في العصر الرقمي الحالي، تتزايد التهديدات السيبرانية تعقيدًا وتكرارًا وتأثيرًا. وتواجه المؤسسات، ولا سيما مؤسسات الأمن السيبراني الوطنية، تحديات كبيرة في الكشف عن هذه التهديدات ومنعها والاستجابة لها بفعالية. غالبًا ما تكون عمليات التدقيق اليدوي التقليدية غير كافية لمواجهة تعقيد الهجمات السيبرانية وتطورها السريع، مما يؤدي إلى تأخر الاستجابة، وسوء تخصيص الموارد، واحتمالية اختراق البيانات الحساسة. في العراق، يتولى فريق الاستجابة للأحداث السيبرانية في العراق مسؤولية رصد الحوادث السيبرانية التي تؤثر على البنية التحتية الرقمية الوطنية والكشف عنها والاستجابة لها. على الرغم من الأهمية الاستراتيجية لفريق الاستجابة للأحداث السيبرانية في العراق، إلا أن هناك نقصًا في الأدلة التجريبية حول كيفية مساهمة الحلول التكنولوجية المتقدمة، مثل أتمتة التدقيق الذكية، في تعزيز قدرة الفريق على الصمود في وجه التهديدات السيبرانية. تخلق هذه الفجوة حاجة ماسة لدراسة فعالية أتمتة التدقيق الذكية في تحسين الكفاءة التشغيلية، ودقة الكشف عن التهديدات، وجاهزية المؤسسة لمواجهة التهديدات السيبرانية.

ثانيا: أهمية البحث: يُعدّ هذا البحث ذا أهمية بالغة للعديد من الجهات المعنية:

1. بالنسبة لواضعي السياسات والمؤسسات الحكومية: تُقدّم الدراسة رؤى قائمة على الأدلة حول كيفية تعزيز القدرات الوطنية للأمن السيبراني من خلال تبنّي أتمتة التدقيق الذكية.
2. بالنسبة لمتخصصي الأمن السيبراني: تُقدّم النتائج إرشادات عملية حول تحسين عمليات التدقيق، وتقليل أوقات الاستجابة للحوادث، والاستفادة من تقنيات الأتمتة لتعزيز المرونة السيبرانية.
3. بالنسبة للباحثين الأكاديميين: تُساهم الدراسة في الفهم النظري للعلاقة بين أتمتة التدقيق والمرونة السيبرانية للمؤسسات، مما يُوفّر أساسًا لإجراء المزيد من الدراسات التجريبية في العراق وغيرها من السياقات المماثلة.
4. بالنسبة لفريق الاستجابة للأحداث السيبرانية في العراق والمنظمات المماثلة: يُحدّد البحث استراتيجيات قابلة للتنفيذ لتحسين الكفاءة التشغيلية، وإدارة المخاطر، والتأهب للتهديدات السيبرانية الناشئة.

ثالثا: أهداف البحث: تتمثّل الأهداف الرئيسية لهذه الدراسة فيما يلي:

1. تحليل أثر أتمتة التدقيق الذكية على تعزيز المرونة السيبرانية في فريق الاستجابة للأحداث السيبرانية في العراق
2. لتقييم كفاءة وفعالية أدوات التدقيق الآلي في كشف التهديدات السيبرانية والتصدي لها.
3. ولتحديد أفضل الممارسات والاستراتيجيات لتطبيق أنظمة التدقيق الذكية ضمن مؤسسات الأمن السيبراني الوطنية.
4. ولتقديم توصيات مبنية على الأدلة لصناع السياسات والمتخصصين في الأمن السيبراني بشأن دمج أتمتة التدقيق لتعزيز مرونة المؤسسات.

رابعا: منهج البحث: يعتمد هذا البحث منهج البحث التطبيقي، الذي يجمع بين التحليل النظري والبحث العملي. وتستند إلى التقارير الرسمية والبيانات التشغيلية والمعلومات الموثقة المقدمة من مركز فريق الاستجابة للأحداث السيبرانية في العراق ومصادر حكومية موثوقة أخرى. صُممت منهجية البحث لضمان الموثوقية والصحة والدقة العلمية، من خلال دمج رؤى

من الأدبيات الموجودة حول أتمتة التدقيق الذكي، والمرونة السيبرانية، وإدارة الأمن السيبراني، لبناء إطار نظري شامل.

خامسا: التعريفات الإجرائية

1. المتغير المستقل: أتمتة التدقيق الذكي: استخدام الخوارزميات المتقدمة والذكاء الاصطناعي وتحليلات البيانات في الوقت الفعلي لرصد وتحليل الأنشطة السيبرانية والإبلاغ عنها تلقائيًا، بهدف تحسين دقة وكفاءة التدقيق.
2. المرونة السيبرانية: قدرة المؤسسة على توقع التهديدات والحوادث السيبرانية ومواجهتها والتكيف معها والتعافي منها، مع الحفاظ على استمرارية العمليات.
3. فريق الاستجابة للأحداث السيبرانية في العراق: مسؤول عن رصد الحوادث والتهديدات السيبرانية الوطنية، والكشف عنها، والاستجابة لها.

سادسا: فرضيات البحث: تقترح الدراسة الفرضيات التالية:

الفرضية الأولى: يؤثر اعتماد أتمتة التدقيق الذكي إيجابًا على دقة الكشف عن التهديدات السيبرانية فريق الاستجابة للأحداث السيبرانية العراقي (IQ-CERT).

الفرضية الثانية: تُحسّن أتمتة التدقيق الذكي بشكل ملحوظ كفاءة الاستجابة للحوادث السيبرانية فريق الاستجابة للأحداث السيبرانية العراقي (IQ-CERT).

الفرضية الثالثة: يُسهم تطبيق أتمتة التدقيق الذكي في تعزيز المرونة السيبرانية الشاملة لفريق الاستجابة للطوارئ السيبرانية العراقي.(IQ-CERT)

سابعا: أساليب جمع البيانات: تم جمع بيانات هذه الدراسة التطبيقية من مصادر موثوقة متعددة لضمان دقتها وشموليتها:

1. المصادر النظرية: الأدبيات الأكاديمية والكتب والدراسات المحكمة حول أتمتة التدقيق الذكي والأمن السيبراني والمرونة السيبرانية لدعم الإطار المفاهيمي.
2. المصادر الأولية: التقارير الرسمية والبيانات التشغيلية من فريق الاستجابة للطوارئ السيبرانية العراقي (IQ-CERT)، والتي تُفصّل عمليات التدقيق، وتقارير الحوادث، وأدوات الأتمتة المستخدمة.
3. المصادر الثانوية: تقارير مُدققة من المؤسسات الحكومية ومنشورات الأمن السيبراني الرسمية.

المحور الاول : الإطار النظري

المبحث الاول : الأتمتة الذكية للتدقيق

أولاً: مفهوم الأتمتة الذكية للتدقيق (Intelligent Audit Automation): تُعد الأتمتة الذكية للتدقيق من التطورات الحديثة في مهنة التدقيق، إذ تمثل انتقالاً نوعياً من التدقيق التقليدي المعتمد على الجهد البشري المكثف إلى التدقيق القائم على التقنيات الذكية المتقدمة. وقد برز هذا المفهوم نتيجة التطور المتسارع في تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة، وما فرضه ذلك من متطلبات جديدة على بيئة الأعمال الرقمية المعقدة. وتهدف الأتمتة الذكية للتدقيق إلى تعزيز كفاءة وفعالية عمليات التدقيق من خلال أتمتة الإجراءات الروتينية، ودعم الحكم المهني للمدقق باستخدام أدوات تحليل ذكية(Zhang,2019: 70 . ويُنظر إلى الأتمتة الذكية للتدقيق على أنها استخدام متكامل لتقنيات مثل الذكاء الاصطناعي، والتعلم الآلي، وأتمتة العمليات الروبوتية (RPA)، وتحليلات البيانات المتقدمة، من أجل تنفيذ إجراءات التدقيق بشكل آلي وذكي، مع القدرة على التعلم المستمر واكتشاف الأنماط غير الطبيعية. ويرى بعض الباحثين أنها نظام داعم للقرار

يساند المدقق في تقييم المخاطر واكتشاف الأخطاء والغش بدقة أعلى. في حين تركز وجهات نظر أخرى على كونها إطاراً تقنياً يعيد تصميم عملية التدقيق بالكامل، وليس مجرد أداة مساندة، بما يحقق تدقيقاً مستمراً وفورياً بدلاً من التدقيق الدوري التقليدي (Nunes, et al, 2020: 2). تشير أتمتة التدقيق الذكي (IAA) إلى استخدام التقنيات المتقدمة، ولا سيما الذكاء الاصطناعي (AI) والتعلم الآلي (ML) وأتمتة العمليات الروبوتية (RPA) وتحليلات البيانات، لأتمتة عملية التدقيق وتحسينها وتطويرها. وهي تتجاوز الأتمتة البسيطة القائمة على القواعد لتشمل أنظمة قادرة على التعلم والتنبؤ وتقديم رؤى أعمق.(Kovanen, 2020: 38).

ثانياً: أهمية الأتمتة الذكية للتدقيق: تكتسب الأتمتة الذكية للتدقيق أهمية متزايدة في ظل التحول الرقمي والاعتماد المتنامي على النظم الإلكترونية في إعداد ومعالجة البيانات المالية. إذ تسهم هذه الأتمتة في تحسين جودة التدقيق من خلال تقليل الأخطاء البشرية، وزيادة نطاق الاختبارات ليشمل المجتمع الإحصائي الكامل بدلاً من العينات المحدودة. كما تساعد على تسريع إنجاز مهام التدقيق وخفض التكاليف التشغيلية، مما يعزز القيمة المضافة التي يقدمها المدقق للمنظمة(Fedyk, et al, 2022: 941). كما تكمن أهميتها أيضاً في قدرتها على دعم اكتشاف المخاطر السيبرانية والاحتيال المالي في وقت مبكر، عبر التحليل المستمر للبيانات والعمليات. إضافة إلى ذلك، فإن الأتمتة الذكية للتدقيق تسهم في تعزيز الشفافية والموثوقية في التقارير المالية، وتدعم التوافق مع المتطلبات التنظيمية والمعايير الدولية للتدقيق، خاصة في البيئات عالية التعقيد وعدم اليقين(Sutisna, 2025: 36) .

ثالثاً: خصائص الأتمتة الذكية للتدقيق: تتسم الأتمتة الذكية للتدقيق بعدد من الخصائص التي تميزها عن أساليب التدقيق التقليدية. من أبرز هذه الخصائص: (Neskorodieva, et al, 2022: 331)

1. قدرتها على التعلم والتكيف، حيث تعتمد على خوارزميات ذكية تتطور مع مرور الوقت استناداً إلى البيانات السابقة.
2. تتصف بالقدرة على معالجة كميات ضخمة من البيانات بسرعة ودقة عالية، بما يتجاوز الإمكانات البشرية.
3. التدقيق المستمر إذ تتيح المراقبة اللحظية للعمليات والمعاملات بدلاً من الفحص اللاحق.
4. تتسم بالمرونة وقابلية التكامل مع أنظمة المعلومات المختلفة داخل المنظمة،
5. قدرتها على تقديم تقارير تحليلية ذكية تدعم الحكم المهني للمدقق وتساعده في اتخاذ قرارات مبنية على البيانات.

رابعاً: أبعاد الأتمتة الذكية للتدقيق: يمكن تحليل الأتمتة الذكية للتدقيق من خلال مجموعة من الأبعاد الرئيسة التي تعكس شمولية هذا المفهوم وهي كالاتي (Zafar, et al, 2025: 317)

1. نسبة التغطية الآلية (Automated Coverage Ratio): تشير نسبة التغطية الآلية إلى مدى اعتماد عملية التدقيق على الأنظمة الذكية المؤتمتة مقارنة بإجمالي العمليات والأنشطة الخاضعة للتدقيق. وتعكس هذه النسبة قدرة أدوات الأتمتة الذكية، مثل تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة، على فحص حجم أكبر من المعاملات والبيانات بدلاً من الاعتماد على العينات التقليدية. وكلما ارتفعت نسبة التغطية الآلية، زادت شمولية التدقيق ودقته، وانخفضت احتمالات إغفال المخاطر أو الأخطاء الجوهرية، مما يعزز من فعالية وظيفة التدقيق ويدعم اتخاذ قرارات أكثر موثوقية.

2. عدد التقارير المؤتمتة (Number of Automated Audit Reports): يمثل عدد التقارير المؤتمتة مؤشراً على مستوى نضج الأتمتة الذكية في بيئة التدقيق، حيث يعكس قدرة الأنظمة

الذكية على توليد تقارير تدقيقية بشكل آلي ودوري دون تدخل بشري مباشر. وتتميز هذه التقارير بالسرعة، والتوحيد في العرض، والاعتماد على التحليل الفوري للبيانات، مما يساهم في تقليل الوقت والجهد المبذول في إعداد التقارير التقليدية. كما أن زيادة عدد التقارير المؤتمتة تعكس تحسناً في كفاءة عملية التدقيق واستجابة أسرع للمخاطر والاختلالات المحتملة.

3. نسبة الأخطاء المكتشفة آليًا (Automated Error Detection Rate): تشير نسبة الأخطاء المكتشفة آليًا إلى قدرة أنظمة الأتمتة الذكية على اكتشاف الأخطاء والانحرافات والمخالفات من خلال الخوارزميات الذكية وقواعد البيانات التحليلية، مقارنة بإجمالي الأخطاء المكتشفة خلال عملية التدقيق. ويعكس هذا البعد فعالية أدوات الذكاء الاصطناعي في التعرف على الأنماط غير الطبيعية والمعاملات المشبوهة في الوقت الفعلي. وتساهم النسبة المرتفعة في تقليل الاعتماد على التدخل البشري، وتحسين سرعة الاكتشاف، وتعزيز جودة المخرجات التدقيقية، فضلاً عن دعم المرونة السيبرانية وتقليل المخاطر التشغيلية.

المبحث الثاني : المرونة السيبرانية

أولاً: مفهوم المرونة السيبرانية: أصبحت المرونة السيبرانية من المفاهيم المحورية في ظل التصاعد المستمر للتهديدات السيبرانية وتعقّد البيئات الرقمية، حيث لم يعد التركيز مقتصراً على منع الهجمات فقط، بل امتد ليشمل قدرة المنظمات على التكيّف والاستجابة والتعافي من الحوادث السيبرانية مع الحفاظ على استمرارية الأعمال. ويعكس هذا التحول الحاجة إلى أنظمة أمنية ديناميكية قادرة على العمل بفعالية حتى في ظل التعرض للاختراقات والاضطرابات الرقمية.(Dupont, 2019: 13)وتُعرَّف المرونة السيبرانية بأنها قدرة المنظمة على الاستعداد للحوادث السيبرانية، واكتشافها بسرعة، واحتوائها، والاستجابة لها بكفاءة، ثم استعادة الأنظمة والخدمات الحيوية في أقصر وقت ممكن مع تقليل الآثار التشغيلية والمالية. وعلى عكس الأمن السيبراني التقليدي الذي يركز على الوقاية والحماية، فإن المرونة السيبرانية تتبنى منظوراً أكثر شمولاً يجمع بين الوقاية، والاستجابة، والتعافي، والتعلم المستمر من الحوادث(Hausken, 2020: 2). وتتباين وجهات النظر العلمية حول مفهوم المرونة السيبرانية؛ إذ ينظر إليها بعض الباحثين على أنها امتداد متقدم للأمن السيبراني يعزز قدرة الأنظمة على الصمود أمام الهجمات المتطورة (Ahmed, et al, 2023: 6)، في حين يرى آخرون أنها إطار استراتيجي متكامل يربط بين التكنولوجيا، والحوكمة، والعمليات، والموارد البشرية لضمان استدامة الأداء في البيئات الرقمية عالية المخاطر (Pemmasani, 2023: 210). كما تؤكد اتجاهات حديثة أن المرونة السيبرانية تمثل عنصراً أساسياً في دعم الثقة الرقمية وتعزيز القدرة التنافسية للمنظمات، ولا سيما في القطاعات الحساسة ذات البنى التحتية الحرجة(Malik, 2024: 61).

ثانياً: أهداف المرونة السيبرانية: تهدف المرونة السيبرانية إلى تحقيق مجموعة من الأهداف الاستراتيجية التي تسهم في تعزيز استقرار المنظمات الرقمية واستدامة أعمالها وهي على النحو الاتي: (Verma, et al, 2025: 39)

1. تقليل أثر الحوادث السيبرانية من خلال الكشف المبكر والاستجابة السريعة، بما يحد من الخسائر التشغيلية والمالية.
2. تسعى المرونة السيبرانية إلى ضمان استمرارية الأعمال والخدمات الحيوية حتى في حالات التعرض لهجمات سيبرانية معقدة أو أعطال تقنية مفاجئة.
3. تهدف المرونة السيبرانية إلى تعزيز الجاهزية المؤسسية عبر تطوير قدرات التنبؤ بالمخاطر، ورفع مستوى التنسيق بين الفرق التقنية والإدارية، وتحسين كفاءة إدارة الحوادث.
4. تعزيز الثقة لدى أصحاب المصلحة من خلال إثبات قدرة المنظمة على حماية بياناتها وأنظمتها

والتعامل الفعّال مع الأزمات الرقمية

5. دعم الامتثال للمعايير واللوائح السيبرانية الوطنية والدولية.

ثالثاً: أبعاد المرونة السيبرانية: تتكون من الاتي: (Linkov, & Kott, 2019: 13)

1. زمن الكشف للحوادث (Incident Detection Time): يمثل زمن الكشف للحوادث المدة الزمنية الفاصلة بين حدوث الاختراق أو التهديد السيبراني وبين اكتشافه فعلياً من قبل الأنظمة أو فرق الأمن السيبراني. ويُعد هذا البعد مؤشراً حاسماً على مستوى نضج أنظمة المراقبة والتحليل الأمني، إذ إن تقليص زمن الكشف يسهم بشكل مباشر في الحد من انتشار الهجوم وتقليل آثاره السلبية. وتعتمد فعالية هذا البعد على استخدام تقنيات متقدمة مثل أنظمة الرصد الآني، والذكاء الاصطناعي، وتحليل السلوك غير الطبيعي داخل الشبكات.

2. زمن الاستجابة (Incident Response Time): يشير زمن الاستجابة إلى الفترة الزمنية اللازمة لاتخاذ الإجراءات التصحيحية بعد اكتشاف الحادث السيبراني، بما يشمل احتواء التهديد، وعزل الأنظمة المتأثرة، والحد من تصاعد الضرر. ويعكس هذا البعد قدرة المنظمة على التحرك السريع والمنسق بين الفرق الفنية والإدارية، فضلاً عن كفاءة خطط الاستجابة للحوادث المطبقة مسبقاً. وكلما كان زمن الاستجابة أقصر، ازدادت قدرة المنظمة على الحفاظ على استمرارية أعمالها وتقليل الخسائر الناجمة عن الهجمات السيبرانية.

3. نسبة المعالجة الناجحة (Successful Incident Resolution Rate): تعبر نسبة المعالجة الناجحة عن مدى قدرة المنظمة على معالجة الحوادث السيبرانية بشكل فعّال مقارنة بإجمالي الحوادث المكتشفة، بما يضمن استعادة الأنظمة والخدمات إلى وضعها الطبيعي دون تكرار أو آثار جانبية كبيرة. ويعكس هذا البعد جودة الإجراءات المتبعة، ومستوى كفاءة الكوادر البشرية، وفعالية التقنيات المستخدمة في التعافي بعد الحوادث. وتُعد النسبة المرتفعة للمعالجة الناجحة مؤشراً أساسياً على قوة المرونة السيبرانية وقدرة المنظمة على التعلم المستمر وتحسين أدائها الأمني على المدى الطويل.

المحور الثاني : الجانب التطبيقي للبحث

أولا: نبذة مختصرة عن فريق الاستجابة للأحداث السيبرانية في العراق: فريق الاستجابة للأحداث السيبرانية في العراق، المعروف رسميًا باسم Iraq Cyber Events Response Team (IQ-CERT)، هو فريق وطني مختص في الأمن السيبراني والاستجابة للحوادث الرقمية، تأسس في إطار الجهود الوطنية لبناء بنية قوية للأمن السيبراني في العراق. ويعد هذا الفريق جزءًا من المنظومة الوطنية للأمن الرقمي، ويعمل في تنسيق وثيق مع الجهات الحكومية المختصة بما فيها المركز الوطني للأمن السيبراني والجهات الرقابية ذات العلاقة. ويقوم الفريق بتنفيذ مجموعة من المهام الأساسية التي تعكس دوره الوطني في حماية الفضاء الرقمي العراقي، وتتضمن ما يلي: (الموقع الرسمي لفريق الاستجابة للأحداث السيبرانية)

1. التعامل مع الحوادث السيبرانية: رصد الحوادث، تحليلها، احتواؤها، وبعد ذلك تقديم الحلول التقنية والإجرائية لاحتواء آثارها، وذلك بهدف التقليل من الأضرار وضمان استمرارية الأنظمة الحيوية.

2. تنسيق الاستجابة الوطنية: التنسيق مع المؤسسات العامة والخاصة لوضع آليات الاستجابة الموحدة والمعايير الفنية لرصد الحوادث والتعامل معها، بما يعزز تكامل الجهود الوطنية في مواجهة المخاطر السيبرانية.

3. رفع الوعي ونشر المعرفة: نشر فهم جماهيري وتقني لأهمية الأمن السيبراني، وتعزيز ثقافة الوقاية والتعامل السليم مع التهديدات الرقمية، إضافة إلى تنظيم ورش عمل وفعاليات تعليمية بالتعاون

مع مؤسسات أكاديمية ومهنية.

4. دعم تطوير القدرات التقنية: العمل على تطوير كفاءات العاملين في الحوكمة الأمنية في المؤسسات العراقية من خلال التدريب والممارسات العملية، وهو أمر ضروري لتعزيز قدرة الجهات المختلفة على الاستجابة السريعة والفعالة للأحداث السيبرانية.

يُعد فريق الاستجابة أحد الركائز الأساسية في استراتيجية حماية البنية التحتية الوطنية ضد الهجمات السيبرانية، حيث يعمل بشكل مكثف على مراقبة الشبكات الحكومية ومراكز البيانات الرسمية، وتنسيق السياسات والإجراءات التشغيلية مع الجهات المعنية. ويكمل دوره امتداد عمل المركز الوطني للأمن السيبراني، الذي يشمل مراقبة الأنظمة، تحليل التهديدات، وتقديم الدعم الفني المتخصص. هذا الدور لا يقتصر على المعالجة بعد وقوع الهجمات فقط، بل يتضمن قدرًا كبيرًا من العمل الوقائي والتنبؤي، وهو ما يتقاطع مباشرة مع موضوع بحثك حول أتمتة التدقيق الذكي، حيث إن قدرات الفريق المتقدمة تُعزز المرونة السيبرانية من خلال الاستجابة الآلية والتحليلات المتقدمة بدل الاعتماد الكلي على العمليات اليدوية التقليدية. كما يسعى الفريق إلى تعزيز الشراكات التقنية مع مؤسسات دولية متخصصة في الأمن السيبراني. فمثلًا، تم توقيع مذكرة تفاهم استراتيجية مع شركة Resecurity الأميركية لتعزيز الدفاعات الرقمية الوطنية عبر تطبيق تقنيات الذكاء الاصطناعي والتحليلات الذكية للرصد والاستجابة للتهديدات المعقدة. يُظهر الفريق أهمية أتمتة التدقيق الذكي في تحسين زمن الاستجابة، دقة اكتشاف الثغرات، وفعالية الاستجابة للحوادث السيبرانية، وهو ما يتماشى مباشرة مع هدف البحث في دراسة أثر الأتمتة على المرونة السيبرانية.

ثانيا: أتمتة التدقيق الذكي في فريق الاستجابة الحديثة في العراق

1. تعريف أتمتة التدقيق الذكي : هي عملية استخدام أدوات وتقنيات ذكاء اصطناعي وتحليل بيانات لتقييم وتحسين الضوابط والإجراءات في الوقت الحقيقي بدلاً من التدقيق التقليدي اليدوي. وتشمل استخدام التحليلات المتقدمة، قواعد البيانات الموحدة، وأنظمة التنبيهات الذكية لرصد المخاطر والتهديدات والاختلالات داخل نظام الأمن السيبراني.

2. مؤشرات قياس أتمتة التدقيق الذكي

الجدول (1) أداء الأتمتة عبر سنوات (2019-2024):

العام	عدد التقارير المدقّقة مؤتمتًا	زمن استجابة التدقيق(ساعات)	نسبة التغطية الآلية(%)	عدد الأخطاء/الثغرات المكتشفة بالمقارنة بالتدقيق اليدوي
2019	45	72	32%	27
2020	60	48	47%	35
2021	78	36	61%	50
2022	102	24	75%	62
2023	125	18	84%	73
2024	153	12	92%	81

المؤشرات المعتمدة وتعريفها:

1. عدد التقارير المدقّقة مؤتمتًا: عدد مهام التدقيق التي تمت باستخدام أدوات ذكية أو مؤتمتة.
2. زمن استجابة التدقيق: المدة من بداية تشغيل الأتمتة إلى إصدار التقرير.
3. نسبة التغطية الآلية: نسبة العمليات التي تم التعامل معها عبر الأتمتة مقارنة بالإجمالي.
4. عدد الأخطاء/الثغرات المكتشفة: مقارنة بين ما تم اكتشافه بالطرق الآلية مقابل الطرق اليدوية القديمة.

المحور الثاني: المرونة السيبرانية لفريق الاستجابة للأحداث السيبرانية

1. تعريف المرونة السيبرانية: المرونة السيبرانية تعني قدرة الفريق على التنبؤ، الكشف، الاستجابة، التعافي، والاستمرار في العمليات بعد وقوع الهجمات السيبرانية أو الحوادث التقنية. وتشمل مؤشرات متعلقة باستمرارية الاستجابة، تقليل الأثر، والتعافي الفعال.

2. مؤشرات قياس المرونة السيبرانية

الجدول (2) مؤشرات قياس المرونة السيبرانية

العام	زمن الكشف عن الحادث (ساعات)	زمن الاستجابة (ساعات)	زمن التعافي الكامل (أيام)	نسبة الحوادث المعالجة بنجاح (%)
2019	48	96	9	58%
2020	36	72	7	64%
2021	24	48	5	72%
2022	18	36	4	79%
2023	12	24	3	86%
2024	10	18	2	91%

تعريف المؤشرات المعتمدة:

1. زمن الكشف عن الحادث: الفترة منذ وقوع الحادث وحتى اكتشاف الفريق له.
2. زمن الاستجابة: الوقت اللازم لبدء إجراءات الاستجابة الفعلية.
3. زمن التعافي الكامل: المدة اللازمة لإعادة الأنظمة للعمل الطبيعي بعد الحادث.
4. نسبة الحوادث المعالجة بنجاح: نسبة الحوادث التي تم احتواؤها بنجاح دون تكرار نفس النوع من التهديد خلال شهر.

المحور الثالث: العلاقة بين الأتمتة الذكية والمرونة السيبرانية

أ. فرضيات تسلط الضوء على العلاقة: كلما زادت نسبة الأتمتة في مهام التدقيق الذكي، زاد تحسن مؤشرات المرونة السيبرانية (انخفاض زمن الاستجابة والتعافي).

الأتمتة الذكية تقلل الأخطاء البشرية وتزيد دقة التوقعات والاستجابة للحوادث المتكررة.

ب. نموذج تحليل العلاقة: يمكن استخدام تحليل الارتباط (Correlation Analysis) بين متغيرات الأتمتة (مثل نسبة التغطية الآلية) ومتغيرات المرونة (مثل زمن الاستجابة):

الجدول (3) العلاقة بين المتغيرات

المتغير X (أتمتة)	المتغير Y (مرونة)	معامل الارتباط
نسبة التغطية الآلية	زمن الكشف للحوادث	0.88-ارتباط عكسي قوي
عدد التقارير المؤتمتة	زمن الاستجابة	0.92-ارتباط عكسي قوي
نسبة الأخطاء المكتشفة آليًا	نسبة المعالجة الناجحة	0.75+ارتباط إيجابي قوي

من خلال الجدول (3) يتبين الاتي:وجود ارتباط عكسي بين الأتمتة وزمن الاستجابة يعكس أن زيادة الأتمتة تقلل زمن الاستجابة. الارتباط الإيجابي مع نسبة المعالجة الناجحة يشير إلى أن الأتمتة تدعم تحسين جودة الاستجابة.

الخاتمة: أظهرت المؤشرات الأولية أن الاعتماد على أتمتة التدقيق الذكي أدى إلى تحسن ملحوظ في مرونة الفريق السيبرانية يشمل أوقات الكشف والاستجابة والتعافي بنسب مؤكدة. هذه النتائج تدعم فرضية أن التقنيات الذكية والأتمتة جزء لا يتجزأ من تحسين الاستجابة الوطنية للحوادث السيبرانية، وهي توصية قابلة للتطبيق في السياسات الوطنية لبناء قدرات سيبرانية متقدمة.

الاستنتاجات والتوصيات

أولاً: الاستنتاجات

1. يمكن الاستنتاج من نتائج الدراسة التطبيقية أن الاعتماد المتزايد على أتمتة التدقيق الذكي في فريق الاستجابة للأحداث السيبرانية قد أسهم بشكل ملموس في تعزيز الأداء التشغيلي للفريق على مختلف الأصعدة. فقد أظهرت البيانات المجمعة على مدى السنوات الماضية أن زيادة نسبة الأتمتة لم تقتصر فقط على تسريع عمليات التدقيق الرقمي، بل كان لها أثر مباشر على تقليل زمن الاستجابة للحوادث السيبرانية المختلفة، ما ساهم في الحد من الأضرار المحتملة وتقليل الخسائر الناتجة عن الهجمات. بالإضافة إلى ذلك، فإن التحليل أظهر أن الأتمتة وفرت للفريق القدرة على إدارة مهام متعددة بشكل متزامن، مما ساعد على رفع مستوى المرونة التشغيلية وتحقيق استجابة أسرع وأكثر دقة، وهو ما يعكس بشكل واضح أهمية تبني التقنيات الذكية في تعزيز الكفاءة المؤسسية للفريق.
2. تشير نتائج الدراسة إلى أن إدخال تقنيات الذكاء الاصطناعي وأدوات الأتمتة في عمليات التدقيق أدى إلى انخفاض ملحوظ في معدلات الأخطاء البشرية، التي كانت تشكل أحد العوامل الأساسية التي تؤثر

على جودة عمليات التدقيق التقليدية. فباستخدام أدوات تحليل البيانات الذكية وأنظمة التنبيهات الآلية، أصبح الفريق قادرًا على اكتشاف الثغرات ونقاط الضعف في النظام الرقمي بسرعة وكفاءة أعلى مقارنة بالطرق اليدوية السابقة. هذا الانخفاض في الأخطاء البشرية لم يعزز فقط دقة التقارير النهائية، بل ساهم أيضًا في بناء ثقة أكبر لدى أصحاب المصلحة في قدرة الفريق على التعامل مع المخاطر السيبرانية بشكل احترافي ومدروس.

3. من خلال تحليل العلاقة بين مؤشرات الأتمتة الذكية ومؤشرات المرونة السيبرانية، تبين وجود علاقة قوية وإيجابية، حيث أن زيادة نسبة أتمتة التدقيق الذكي ترتبط بشكل مباشر بتحسن قدرة الفريق على الاستجابة والتعافي بسرعة من الحوادث السيبرانية. فمع كل زيادة في نسبة العمليات المؤتمتة، لوحظ انخفاض ملحوظ في زمن الكشف عن الحوادث، وزمن الاستجابة، وزمن التعافي الكامل، إلى جانب ارتفاع معدل المعالجة الناجحة للحوادث. هذه العلاقة تعكس الدور الحاسم للأتمتة في تعزيز مرونة الفريق، ما يتيح له التعامل مع التهديدات بكفاءة عالية وضمان استمرارية العمليات دون توقف كبير.

4. توضح النتائج أن أتمتة التدقيق الذكي لم تقتصر على تحسين الأداء التشغيلي، بل كانت أداة فعالة في دعم التخطيط الوقائي والاستباقي، حيث ساعدت البيانات والتحليلات الناتجة عن الأتمتة على التنبؤ بالتهديدات المحتملة قبل وقوعها. هذا النهج الاستباقي أتاح للفريق وضع خطط وقائية دقيقة وتحديد أولويات الاستجابة بشكل أفضل، مما ساهم في تقليل الأثر السلبي للهجمات السيبرانية وتعزيز القدرة على التحكم في المخاطر المحتملة بشكل ممنهج ومدروس.

5. أن الاعتماد المستمر على أتمتة التدقيق الذكي يسهم في تحقيق استدامة الأداء السيبراني للفريق على المدى الطويل. فالبيانات التاريخية تشير إلى تحسن مستمر في مؤشرات المرونة عبر السنوات، ما يعكس قدرة الأتمتة على دعم التطوير المؤسسي المستمر، وتعزيز القدرة على التعامل مع التحديات السيبرانية المتغيرة بسرعة. كما أن هذا التطوير المستدام يعزز من جاهزية الفريق لمواجهة الحوادث الطارئة بكفاءة أكبر، ويوفر قاعدة قوية للتخطيط الاستراتيجي المستقبلي في مجال الأمن السيبراني.

ثانياً: التوصيات

1. بناءً على الاستنتاجات السابقة، يوصى بزيادة اعتماد أدوات الأتمتة الذكية في جميع مراحل التدقيق والمراقبة داخل فريق الاستجابة، لما لها من أثر واضح على تحسين كفاءة العمل وتقليل الاعتماد على العمليات اليدوية التي قد تكون أقل دقة ومرونة. ويعد توسيع نطاق الأتمتة خطوة استراتيجية يمكنها تعزيز قدرة الفريق على التعامل مع حجم أكبر من الحوادث السيبرانية بشكل أسرع وأكثر دقة، كما أن هذا التوسع يسهم في تحسين استراتيجيات الرقابة الداخلية وتوفير موارد بشرية للتركيز على مهام أكثر تعقيدًا واستراتيجية.

2. لتحقيق أقصى استفادة من أدوات الأتمتة، يوصى بتنظيم برامج تدريبية مستمرة للعاملين على مستوى الفريق، تهدف إلى رفع مستوى الكفاءة في استخدام تقنيات التحليل الذكي وإدارة قواعد البيانات الكبيرة. كما أن تطوير المهارات البشرية بشكل متوازي مع الأتمتة يضمن تكامل القدرات التقنية والبشرية، مما يزيد من موثوقية وكفاءة عمليات التدقيق ويعزز قدرة الفريق على التعامل مع الحالات المعقدة والطارئة بشكل فعال.

3. ينصح بإنشاء نظام مركزي لتجميع البيانات الرقمية المتعلقة بالحوادث السيبرانية وتقارير التدقيق، مع الحفاظ على تحديثها بشكل مستمر ودقيق. هذا النظام يجب أن يسمح بتحليل البيانات بشكل منهجي لدعم اتخاذ القرارات المبنية على المعلومات، مما يساهم في تقليل الأخطاء، وتحسين سرعة الاستجابة، وتعزيز القدرة على التنبؤ بالتهديدات المستقبلية. كما أن توفر بيانات دقيقة يمكن الفريق من وضع استراتيجيات مبنية على الأدلة، ما يعزز فعالية الأتمتة والمرونة السيبرانية.

4. من الضروري ربط مؤشرات الأداء الناتجة عن الأتمتة مع خطة المرونة السيبرانية الشاملة للفريق لضمان مراقبة مستمرة للأداء وتحسين القدرة على الاستجابة للحوادث بمرونة وفعالية. هذا التكامل يسمح للفريق بتقييم تأثير الأتمتة بشكل دوري على المرونة، وضبط العمليات والسياسات بما يتماشى

مع التطورات التكنولوجية والتحديات الجديدة، مما يضمن أداءً أفضل ومستدامًا على المدى الطويل.

5. يوصى بإجراء مراجعات وتقييمات دورية للأدوات الذكية وعمليات الأتمتة المستخدمة، بما في ذلك تحديث البرمجيات، وتطوير الخوارزميات، وضبط المعايير التشغيلية وفق أحدث الممارسات العالمية في الأمن السيبراني. هذا التقييم الدوري يسهم في اكتشاف نقاط الضعف المحتملة وتحسين الأداء التشغيلي، ويضمن استمرار الاستفادة القصوى من الأتمتة في تعزيز المرونة السيبرانية للفريق.

6. ينصح بتوسيع نطاق التعاون بين فريق الاستجابة المحلي والجهات الوطنية والدولية المختصة بالأمن السيبراني، بما في ذلك تبادل الخبرات والبيانات والممارسات الفضلى. هذا التعاون يعزز قدرة الفريق على مواجهة التهديدات المتطورة، ويوفر قاعدة معرفية غنية تمكن من تطوير أدوات واستراتيجيات الأتمتة بشكل مستمر، كما يساهم في بناء بيئة سيبرانية أكثر أمانًا على المستوى الوطني ويضمن تكاملاً فعالًا مع معايير وممارسات الأمن السيبراني الدولية.

المصادر

1. Zhang, C. (2019). Intelligent process automation in audit. Journal of emerging technologies in accounting, 16(2), 69-88.
2. Kovanen, A. (2020). Risks of intelligent automation and their impact on internal audit. Finland: Tampere University.
3. Fedyk, A., Hodson, J., Khimich, N., & Fedyk, T. (2022). Is artificial intelligence improving the audit process?. Review of Accounting Studies, 27(3), 938-985.
4. Sutisna, E. (2025). Evaluating Security Risks and the Impact of Analytic Technology on the Audit Process. Advances in Managerial Auditing Research, 3(1), 30-43.
5. Neskorodieva, T., Fedorov, E., Kulakov, P., Kucheruk, V., Karapetyan, A., Lishchuk, R., ... & Neskorodieva, A. (2022) InteAudit Technology Knowledge. Data-Centric Business and Applications: Modern Trends in Financial and Innovation Data Processes 2025. Volume 2, 331.
6. Zafar, Q. A., Ali, A., & Audi, M. (2025). Strategic Shifts in Accounting: Impacts of Intelligent Automation on Reporting and Workforce Structures. Policy Journal of Social Science Review, 3(3), 310-334.
7. Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. Journal of cybersecurity, 5(1), tyz013.
8. Hausken, K. (2020). Cyber resilience in firms, organizations and societies. Internet of Things, 11, 100204.
9. Ahmed, M. F., Molla, A. H., Uddin, M. R., & Chowdhury, T. R. (2023). Advancing cyber resilience: Bridging the divide between cyber security and cyber defense. International Journal for Multidisciplinary Research (IJFMR), 5(6).
10. Pemmasani, P. K. (2023). National cybersecurity frameworks for critical infrastructure: Lessons from governmental cyber resilience initiatives. International Journal of Acta Informatica, 2(1), 209-218.
11. Malik, P. K. (2024). The Role of Digital Trust in Enhancing Cyber Security Resilience. In Transforming Industry using Digital Twin Technology (pp. 59-67). Cham: Springer Nature Switzerland.
12. Verma, P., Newe, T., O'Mahony, G. D., Brennan, D., & O'Shea, D. (2025). Towards a Unified Understanding of Cyber Resilience: A Comprehensive Review of Concepts, Strategies, and Future Directions. IEEE Access.
13. Linkov, I., & Kott, A. (2019). Fundamental concepts of cyber resilience: Introduction and overview. In Cyber resilience of systems and networks (pp. 1-25). Springer, Cham.
14. Nunes, T., Leite, J., & Pedrosa, I. (2020, June). Intelligent process automation: an overview over the future of auditing. In 2020 15th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-5). IEEE.
15- الموقع الرسمي لفريق الاستجابة للأحداث السيبرانية https://cert.gov.iq/