Comprehensive Journal of Humanities and Educational Studies
المجلة الشاملة للدراسات الإنسانية التربوية
Volume 1, Issue 2, 2025, Pages: 758-777
Journal homepage :http://cjhes.com.ly/index.php/cjhes/en/index

Assessing The Readiness of Digital Infrastructure Against Advanced Cyberattacks

Abdulrezag Farag Benhalim *
College of Engineering Technology - Janzour, Libya

تقييم مستوى جاهزية البنية التحتية الرقمية في مواجهة الهجمات السيبرانية المتقدمة

د. عبد الرزاق فرج بن حليم *
كلية التقنية الهندسية - جنزور، ليبيا

*Corresponding author: benhalim2001@gmail.com

Received: November 17, 2025	Accepted: December 23, 2025	Published: December 31, 2025

Abstract

This research aims to assess the level of readiness of digital infrastructure in organizations to confront advanced cyberattacks, which are continually evolving in terms of tools, technologies, and hacking methods. The research focuses on analyzing the resilience of digital systems, early detection, rapid response, and recovery after attacks. The research also addresses the most prominent vulnerabilities that attackers can exploit, and works to formulate an analytical framework to measure the readiness of institutions in light of international information security standards. The researcher used the descriptive analytical approach, relying on a questionnaire directed to workers in the field of information technology and cybersecurity, in addition to reviewing recent scientific literature. The results show a disparity in the level of readiness between institutions, in addition to a lack of protection measures and continuous updating of systems. The research recommends the need to enhance cyber defense capabilities and develop integrated strategies for managing digital risks.

Keywords: Digital Infrastructure, Digital Readiness, Cybersecurity, Advanced Cyber Attacks, APTs (Advanced Persistent Threats), Cyber Risk Management.

الملخص:

يهدف هذا البحث إلى تقييم مستوى جاهزية البنية التحتية الرقمية في المؤسسات لمواجهة الهجمات السيبرانية المتقدمة التي تشهد تطورًا مستمرًا على مستوى الأدوات والتقنيات وأساليب الاختراق. ويركز البحث على تحليل قدرة الأنظمة الرقمية على الصمود والكشف المبكر، والاستجابة السريعة، والتعافي بعد الهجمات. كما يتناول البحث أبرز نقاط الضعف التي يمكن للمهاجمين استغلالها، ويعمل على صياغة إطار تحليلي لقياس جاهزية المؤسسات في ضوء المعايير الدولية لأمن المعلومات. استخدم الباحث المنهج الوصفي التحليلي، بالاعتماد على استبيان موجه للعاملين في مجال تقنية المعلومات والأمن السيبراني، إضافة إلى مراجعة الأدبيات العلمية الحديثة. وتظهر النتائج وجود تفاوت في مستوى الجاهزية بين المؤسسات، إضافة إلى نقص في إجراءات الحماية والتحديث المستمر للأنظمة. ويوصي البحث بضرورة تعزيز قدرات الدفاع السيبراني، وتطوير استراتيجيات متكاملة لإدارة المخاطر الرقمية.

الكلمات المفتاحية: البنية التحتية الرقمية، الجاهزية الرقمية، الأمن السيبراني، الهجمات السيبرانية المتقدمة، التهديدات المستمرة المتقدمة (APTs)، إدارة المخاطر السيبرانية.

مقدمة:

تشهد البيئة الرقمية في العصر الحديث تطورات متسارعة جعلت البنية التحتية الرقمية عنصرًا محوريًا في استمرارية المؤسسات ونجاحها. وبالتوازي مع هذا التطور، ازدادت الهجمات السيبرانية تعقيدًا وحدّة، حيث أصبحت تعتمد على أساليب متقدمة تتجاوز الدفاعات التقليدية وتعتمد الذكاء الاصطناعي، والهجمات المستهدفة، واستغلال الثغرات في الأنظمة. وأمام هذه المخاطر، تبرز الحاجة الملحّة إلى تقييم مستوى جاهزية البنية التحتية الرقمية للمؤسسات بهدف حماية البيانات، وضمان استمرارية الأعمال، وتعزيز المرونة السيبرانية.

ويأتي هذا البحث استجابة لهذا التحدي، حيث يسعى إلى تحليل مدى قدرة المؤسسات على مواجهة الهجمات السيبرانية المتقدمة، ودراسة واقع الأنظمة الأمنية، وكفاءة قدرات الكشف والاستجابة، ومدى تطبيق أفضل الممارسات والمعايير الدولية للأمن السيبراني.

أولاً: مشكلة البحث

تتمثل مشكلة البحث في عدم وضوح مستوى جاهزية البنية التحتية الرقمية في العديد من المؤسسات وقدرتها الحقيقية على مواجهة الهجمات السيبرانية المتقدمة، نظرًا لسرعة تطور هذه الهجمات مقارنة ببطء تحديث الأنظمة الدفاعية في المؤسسات.

ويمكن صياغة المشكلة في السؤال الرئيس التالي:

ما مدى جاهزية البنية التحتية الرقمية في المؤسسات لمواجهة الهجمات السيبرانية المتقدمة؟

ويتفرع منه عدة أسئلة فرعية:

1. ما نقاط الضعف الأكثر شيوعًا في البنية التحتية الرقمية للمؤسسات؟
2. ما مدى قدرة المؤسسات على الكشف المبكر عن التهديدات؟
3. هل تمتلك المؤسسات خططًا فعالة للاستجابة للحوادث السيبرانية؟
4. إلى أي مدى تطبق المؤسسات المعايير الدولية للأمن السيبراني؟
5. ما الإجراءات المطلوبة لتعزيز الجاهزية والمرونة الرقمية؟

ثانياً: أهمية البحث

تنبع أهمية هذا البحث من عدة جوانب رئيسية، من أهمها:

1. أهمية الأمن السيبراني لكونه يمثل أحد أعمدة حماية المؤسسات في العالم الرقمي الحديث.
2. تزايد الهجمات السيبرانية من حيث التعقيد وشدة التأثير، مما يجعل تقييم الجاهزية ضرورة استراتيجية.
3. سد الفجوة البحثية في مجال تقييم جاهزية البنية التحتية الرقمية في المؤسسات المحلية والعربية.
4. مساعدة صناع القرار على تحديد نقاط الضعف وتعزيز قدرات الدفاع السيبراني.
5. توفير إطار قياس يمكن للمؤسسات استخدامه لتقييم مستوى الحماية لديها مقارنة بالمعايير العالمية.
6. تعزيز استمرارية الأعمال وتقليل الخسائر الناجمة عن الهجمات الرقمية.

ثالثاً: أهداف البحث

يهدف البحث إلى تحقيق مجموعة من الأهداف، أبرزها:

1. تقييم مستوى جاهزية البنية التحتية الرقمية في المؤسسات لمواجهة الهجمات السيبرانية المتقدمة.
2. تحليل نقاط الضعف والثغرات الأمنية في الأنظمة الرقمية.
3. قياس قدرات الكشف المبكر والاستجابة للحوادث السيبرانية.
4. تحديد مدى تطبيق المؤسسات للمعايير والممارسات الدولية الخاصة بالأمن السيبراني.

5. اقتراح حلول وتوصيات لتعزيز الجاهزية الرقمية ورفع مستوى الحماية.
6. تصميم نموذج تقييمي يمكن استخدامه مستقبلًا لتحسين الأمن السيبراني.

رابعاً: منهجية البحث

يعتمد هذا البحث على المنهج الوصفي التحليلي، باعتباره المنهج الأكثر ملاءمة لدراسة الظواهر المعقدة مثل جاهزية البنية التحتية الرقمية في مواجهة الهجمات السيبرانية. ويقوم المنهج على وصف الواقع الفعلي للأنظمة الرقمية وتحليل مستوى الحماية المتوفر, إضافة إلى تحديد نقاط الضعف والقدرات الدفاعية لدى المؤسسات.

وتشمل منهجية البحث ما يلي:

1. مجتمع البحث

يتمثل مجتمع البحث في العاملين في مجال تقنية المعلومات والأمن السيبراني بإدارة مكافحة جرائم تقنية المعلومات بجهاز المباحث الجنائية بوزارة الداخلية التي تعتمد على بنية تحتية رقمية أساسية في تنفيذ أعمالها.

2. عينة البحث

تم اختيار عينة طبقية عشوائية لعدد 21 موظف من أجمالي 43 موظف أي بنسبة 48.8% وتضم:

مسؤولي الأمن السيبراني
مهندسي الشبكات
محللي نظم المعلومات
الفنيين والمختصين في التهيئة والصيانة

3. أدوات جمع البيانات

يعتمد البحث على:

1. استبيان علمي مكوّن من عدة محاور لقياس مستوى الجاهزية السيبرانية.
2. مقابلات شبه مهيكلة مع خبراء الأمن السيبراني للحصول على رؤية معمقة.
3. تحليل وثائق وتقارير تقنية ذات صلة بالبنية التحتية الرقمية.
4. أساليب التحليل

يتم تحليل البيانات باستخدام:

الإحصاء الوصفي (الوسيط، الانحراف المعياري، المتوسط)
اختبارات الصدق والثبات
تحليل الفجوة بين الوضع الحالي والمستوى المعياري للأمن السيبراني

خامساً: حدود ونطاق البحث

1. الحدود الموضوعية

يتناول البحث تقييم:

حماية الشبكات
جاهزية الأنظمة
قدرات الكشف والاستجابة
تطبيق معايير الأمن السيبراني

ولا يشمل تحليل الجانب المالي أو القانوني إلا بقدر ارتباطه بالجاهزية.

2. الحدود الزمانية

يغطي البحث الفترة الزمنية من 2025.01.01م إلى 2025.06.30م

3. الحدود المكانية

يطبق البحث على إدارة مكافحة جرائم تقنية المعلومات بجهاز المباحث الجنائية بوزارة الداخلية.

3. الحدود البشرية:
التي تعتمد بدرجة كبيرة على البنية الرقمية يقتصر البحث على:
مدير الإدارة قيد البحث والاقسام التابعة لها.
موظفي تقنية المعلومات.
موظفي الأمن السيبراني.
الفنيين والمختصين بالشبكات.

سادساً: متطلبات البحث
1. متطلبات معرفية
الإلمام بمفاهيم الأمن السيبراني.
معرفة آليات الهجمات المتقدمة مثل:
Zero-day attacks
APT (التهديدات المتقدمة المستمرة)
AI-driven cyber attacks
2. متطلبات تقنية
الحصول على بيانات عن الأنظمة المستخدمة في المؤسسات.
توفر أدوات تحليل مثل:
نظم كشف التسلل IDS
أنظمة إدارة الأحداث الأمنية SIEM
3. متطلبات منهجية
تصميم استبيان محكم وموثوق.
تحديد معايير الجاهزية المعتمدة دوليًا مثل:
NIST ,ISO 27001,Cyber Resilience Framework
4. متطلبات إدارية
الحصول على موافقات المؤسسات لجمع البيانات.
التنسيق مع مسؤولي تقنية المعلومات.

سابعاً: فروض البحث
في ضوء المشكلة وعناصر الدراسة، يقترح الباحث الفروض التالية:
الفرض الرئيسي:
هناك قصور في جاهزية البنية التحتية الرقمية بالمؤسسات لمواجهة الهجمات السيبرانية المتقدمة.
فروض فرعية:
1. يوجد مستوى منخفض من إجراءات الحماية الأساسية في البنية التحتية الرقمية.
2. قدرات الكشف المبكر لدى المؤسسات غير كافية لمواجهة الهجمات السيبرانية المتقدمة.
3. خطط الاستجابة للحوادث الرقمية ضعيفة أو غير مفعّلة بالشكل المطلوب.
4. لا تطبق المؤسسات المعايير والممارسات الدولية للأمن السيبراني بشكل كامل.
5. هناك علاقة إيجابية بين تحديث البنية التحتية وارتفاع الجاهزية السيبرانية.

ثامناً: مصطلحات البحث
1. البنية التحتية الرقمية (Digital Infrastructure)

تشير إلى الأنظمة التقنية والشبكات والأجهزة والبرمجيات وقواعد البيانات والمنصات الرقمية التي تعتمد عليها المؤسسات في تقديم خدماتها وتشغيل عملياتها اليومية.

2. الجاهزية الرقمية (Digital Readiness)
هي مدى قدرة المؤسسة على مواجهة التحديات الرقمية، بما في ذلك الاستعداد التقني، وكفاءة الموارد البشرية، وتوفر الإجراءات والسياسات الأمنية اللازمة.

3. الهجمات السيبرانية المتقدمة (Advanced Cyber Attacks / APTs)
هي هجمات إلكترونية ذات مستوى عالٍ من التعقيد والتخطيط، غالباً ما تنفّذها مجموعات متخصصة وتمتاز بالدقة والاستمرارية واستغلال ثغرات غير معروفة.

4. الأمن السيبراني (Cybersecurity)
مجموعة التقنيات والعمليات والممارسات المصممة لحماية الأنظمة الرقمية والشبكات والبيانات من الهجمات أو الاختراق أو التدمير أو الوصول غير المصرح به.

5. إدارة المخاطر السيبرانية (Cyber Risk Management)
العمليات التي تعتمد عليها المؤسسات لتحديد المخاطر الرقمية وتقييمها ومعالجتها ووضع خطط للتخفيف من آثارها المحتملة.

6. الاستجابة للحوادث السيبرانية (Cyber Incident Response)
مجموعة الإجراءات المتخذة للتعامل مع الاختراقات والهجمات الرقمية، بما في ذلك الكشف، التحليل، الاحتواء، الاسترجاع، ومنع التكرار.

7. التهديدات المتقدمة المستمرة (Advanced Persistent Threats – APTs)
نوع من الهجمات الرقمية التي تعتمد على التسلل المستمر والطويل الأمد بهدف سرقة البيانات أو تعطيل الأنظمة، وغالباً ما تقف وراءها جهات عالية القدرة.

8. المرونة الرقمية (Digital Resilience)
قدرة البنية التحتية الرقمية على مواصلة العمل واستعادة وظائفها بسرعة بعد التعرض لهجوم سيبراني.

تاسعاً: الدراسات السابقة

الدراسات العربية:

1. دراسة الحربي (2020)
العنوان: تقييم جاهزية المؤسسات الحكومية للأمن السيبراني.
النتائج: ضعف في تطبيق الممارسات الدولية، نقص في تدريب الموظفين.

2. دراسة القحطاني (2021)
العنوان: تحليل البنية الرقمية في مواجهة الهجمات الإلكترونية.
النتائج: وجود فجوة بين مستوى التهديدات ومستوى الحماية الفعلية، الحاجة إلى تحديث معدات الشبكات.

3. دراسة العوضي (2022)
العنوان: الأمن السيبراني والاستجابة للحوادث الرقمية.
النتائج: تأخر المؤسسات في اكتشاف الهجمات المتقدمة، غياب خطط الاستجابة والتعافي.

الدراسات الأجنبية:

1. (2019,Smith et AI)
الموضوع: Cyber Infrastructure Readiness
النتائج: ضعف كبير في قدرات الكشف المبكر عالميًا، الاعتماد على الدفاعات التقليدية لم يعد كافيًا.

2. (2021,NIST Report)
الموضوع: Cyber Resilience Framework
النتائج: المؤسسات ذات الأنظمة المحدثة تتعرض لأقل خسائر، الجاهزية تعتمد على ثلاث ركائز: الحماية، الكشف، الاستجابة.

3. (Chen & Zhao، 2023)
الموضوع: Advanced Cyber Attacks
النتائج: الهجمات المتقدمة تعتمد على الذكاء الاصطناعي والتعلم الآلي، الحاجة إلى تحديث البنية الرقمية أصبحت ضرورة ملحة.
التعليق على الدراسات السابقة:
تشير الدراسات العربية والأجنبية إلى وجود فجوة واضحة بين متطلبات الأمن السيبراني وممارساته الفعلية في المؤسسات، خاصة في:
ضعف الجاهزية
تأخر الاستجابة
نقص التحديث
غياب خطط التعافي
ويأتي البحث الحالي لتعزيز هذا الاتجاه عبر تقييم أكثر شمولية يربط بين البنية التحتية – الهجمات المتقدمة – الجاهزية المؤسسية.

تاسعاً: الإطار النظري للبحث
المبحث الأول: البنية التحتية الرقمية – المفهوم والمكونات
المطلب الأول: مفهوم البنية التحتية الرقمية
تشير البنية التحتية الرقمية إلى مجموعة الأنظمة التقنية المتكاملة التي تُمكّن المؤسسة من تنفيذ عملياتها الإدارية والتشغيلية والتعليمية والخدمية. وتشمل:
- الأجهزة والمعدات التقنية (الخوادم، الحواسيب، نقاط الوصول).
- شبكة الاتصالات الداخلية والخارجية.
- برمجيات التشغيل والتطبيقات.
- قواعد البيانات ومراكز البيانات.
- تقنيات الأمن السيبراني والحماية.

وتُعد البنية التحتية الرقمية أساس التحول الرقمي، وشرطًا جوهريًا لضمان استمرارية المؤسسات وقدرتها على مواجهة التهديدات والهجمات الإلكترونية المتقدمة.
المطلب الثاني: أهمية البنية التحتية الرقمية
تبرز أهمية البنية التحتية الرقمية في النقاط التالية:
1. دعم العمليات المؤسسية اليومية.
2. تسريع اتخاذ القرار الإداري.
3. تعزيز أمن المعلومات وحماية البيانات.
4. تمكين العمل عن بُعد ومنصات التعلم الرقمي.
5. تقليل الاعتماد على الإجراءات الورقية.
6. تسهيل الرقمنة والتحول المؤسسي.

المطلب الثالث: مكونات البنية التحتية الرقمية
1. مكونات الأجهزة
- الخوادم (Servers)
- أجهزة التخزين
- الموجهات (Routers)
- الموزّعات (Switches)

2. مكونات البرمجيات
- نظم التشغيل.
- أنظمة إدارة قواعد البيانات.

- تطبيقات السيرفرات والتطبيقات المؤسسية.

3. مراكز البيانات

تشمل غرف السيرفرات، نظم التبريد، UPS، مراقبة بيئية.

4. شبكات الاتصالات:

- شبكة LAN
- شبكة WAN
- الشبكات اللاسلكية (Wi-Fi)

5. الأمن السيبراني

- جدران الحماية.
- أنظمة كشف التسلل.
- سياسات الأمن.
- التشفير.

المبحث الثاني: الهجمات السيبرانية المتقدمة APT

المطلب الأول: مفهوم الهجمات السيبرانية المتقدمة

الهجمات السيبرانية المتقدمة (Advanced Persistent Threats) هي:

- هجمات منهجية متطورة تنفذها جهات خبيرة.
- تستهدف اختراق الأنظمة لمدة طويلة دون اكتشافها.
- تعتمد على الهندسة الاجتماعية، الثغرات البرمجية، البرمجيات الخبيثة.

المطلب الثاني: خصائص الهجمات المتقدمة

1. الاستمرارية طويلة المدى.
2. السرية والتخفي.
3. التخطيط المسبق المبني على جمع معلومات.
4. التطوير المستمر لأدوات الاختراق.
5. استهداف مؤسسات ذات قيمة اقتصادية وسياسية وتعليمية.

المطلب الثالث: مراحل الهجمات المتقدمة

1. جمع المعلومات حول المؤسسة.
2. اختراق أولي باستخدام ثغرة أو هندسة اجتماعية.
3. زرع برمجيات تجسس.
4. الحركة الأفقية داخل الشبكة.
5. التحكم والسيطرة.
6. استخراج البيانات أو تدميرها.

المبحث الثالث: جاهزية البنية التحتية الرقمية

المطلب الأول: مفهوم الجاهزية الرقمية

تشير الجاهزية الرقمية إلى قدرة المؤسسة على:

- منع الهجوم السيبراني.
- اكتشافه مبكرًا.
- الاستجابة له.
- التعافي بعد وقوعه.

المطلب الثاني: أبعاد الجاهزية الرقمية

1. الجاهزية التقنية:

- توفر الأجهزة الحديثة.
- تحديث الأنظمة.

- إدارة الثغرات.

2. الجاهزية الأمنية:

- جدران الحماية.
- الأنظمة المضادة للبرمجيات الخبيثة.
- الكشف المبكر عن الهجمات.

3. الجاهزية البشرية:

- تدريب الموظفين.
- الوعي الأمني.
- التعامل مع رسائل التصيّد.

4. الجاهزية الإدارية:

- خطط الاستجابة للحوادث.
- السياسات الأمنية.
- إدارة المخاطر.

المطلب الثالث: مؤشرات قياس الجاهزية

1. تقنيات الدفاع السيبراني.
2. سرعة اكتشاف الاختراق.
3. إدارة التهديدات الأمنية.
4. قوة أنظمة النسخ الاحتياطي.
5. إجراءات الأمن الفيزيائي.
6. جاهزية فريق الأمن السيبراني.

المبحث الرابع: العلاقة بين البنية التحتية الرقمية والهجمات المتقدمة

المطلب الأول: العلاقة المباشرة

كلما كانت البنية التحتية الرقمية:

- أقدم، وحمايتها ضعيفة ← ارتفع نجاح الهجمات المتقدمة
- حديثة ومحمية ومتكاملة ← انخفض احتمال نجاح الهجمات

المطلب الثاني: تأثير البنية التحتية على قدرة الاستجابة

تُمكن البنية الرقمية القوية المؤسسة من:

- اكتشاف الهجمات خلال دقائق بدلًا من أيام.
- عزل الأجهزة المصابة دون انهيار الشبكة.
- استعادة البيانات بسرعة.

المبحث الخامس: الإطار النظري للنماذج والدراسات العالمية

المطلب الأول: نموذج NIST للأمن السيبراني

يُعد إطار الأمن السيبراني الصادر عن المعهد الوطني للمعايير والتقنية (NIST Cybersecurity Framework – CSF) أحد أهم الأطر العالمية وأكثرها اعتماداً لتقييم وتحسين قدرات الأمن السيبراني داخل المؤسسات الحكومية والخاصة. تم تطوير الإطار في الولايات المتحدة عام 2014، وتم تحديثه لاحقاً في إصدار 1.1، ثم في الإصدار الأحدث NIST CSF 2.0، الذي عزز مرونة الإطار ووسّع نطاقه ليشمل جميع أنواع المؤسسات دون استثناء.

ويهدف النموذج إلى وضع منهج موحّد يساعد المؤسسات على إدارة مخاطر الأمن السيبراني بطريقة منهجية واستباقية، من خلال توفير مجموعة من الإرشادات والممارسات القياسية التي تساعد في حماية الأصول الرقمية، وتحسين القدرة على الاستجابة للهجمات، وضمان استمرارية الأعمال.

أولاً: مكونات نموذج NIST CSF

يرتكز إطار NIST على ثلاثة عناصر رئيسية:

1. الوظائف الأساسية (Core Functions)

وهي خمس وظائف مترابطة تمثل دورة حياة إدارة الأمن السيبراني:

(1) التعرّف (Identify):

وتهدف إلى فهم بيئة العمل والأصول الرقمية والتهديدات المحتملة. وتشمل:

إدارة الأصول.

تحديد المخاطر.

الحوكمة.

تقييم الثغرات.

تحليل التبعية التشغيلية.

(2) الحماية (Protect):

تركّز على تطبيق إجراءات تقلل من احتمالية حدوث هجوم سيبراني. وتشمل:

التحكم في الوصول.

التوعية والتدريب.

حماية البيانات.

أمن الأنظمة والتشفير.

إدارة الهوية.

(3) الاكتشاف (Detect)

وتهدف إلى كشف الأنشطة غير الطبيعية والتهديدات فور حدوثها. وتشمل:

مراقبة الشبكات.

كشف الشذوذ.

التحليل الأمني.

الكشف المبكر للهجمات.

(4) الاستجابة (Respond)

وتشمل الإجراءات المتخذة لاحتواء الهجوم وتقليل تأثيره. وتشمل:

خطط الاستجابة للحوادث.

الاتصال وإدارة الأزمة.

التحليل والتحقيق.

التخفيف من الأضرار.

(5) التعافي (Recover)

تركّز على استعادة الخدمات بسرعة وتحسين إجراءات الحماية بعد الحادث. وتشمل:

استعادة العمليات.

توثيق الدروس المستفادة.

تحسين الضوابط الأمنية المستقبلية.

ثانياً: مستويات التنفيذ (Implementation Tiers)

يوفّر NIST أربعة مستويات لتحديد مدى جاهزية المؤسسة:

1. المستوى 1: ابتدائي (Partial)

استجابة غير منسقة، سياسات ضعيفة.

2. المستوى 2: تفاعلي (Risk Informed)

الوعي بالمخاطر موجود لكن غير مؤسسي.

3. المستوى 3: متكرر (Repeatable)

عمليات مؤسسية واضحة وقابلة للتكرار.

4. المستوى 4: متكيف (Adaptive)
قدرة عالية على التكيّف والتحسين المستمر.

ثالثاً: ملف المؤسسة (Profiles)

يمكّن الإطار المؤسسات من إنشاء ملف "بروفايل" يوضح:
الوضع الحالي للأمن السيبراني (Current Profile)
الوضع المستهدف (Target Profile)
ويساعد هذا البروفايل في سد فجوة readiness gap وإعداد خطة تطوير واضحة.

رابعاً: أهمية نموذج NIST CSF

1. مرونة عالية: يمكن تطبيقه على جميع المؤسسات بغض النظر عن الحجم أو القطاع.
2. لغة مشتركة بين الإدارات الفنية والإدارية.
3. تحسين اتخاذ القرار من خلال تحليل المخاطر.
4. تعزيز الحماية والاستجابة والتعافي.
5. الامتثال للمعايير الدولية مثل ISO 27001.
6. تقليل تكاليف الهجمات السيبرانية عبر الكشف المبكر.
7. تحقيق استمرارية الأعمال والمرونة الرقمية.

خامساً: استخدامات إطار NIST في المؤسسات

تقييم الثغرات في البنية التحتية الرقمية.
بناء سياسات الأمن السيبراني.
تصميم خطط الاستجابة للحوادث.
تطوير نظم الحوكمة وإدارة الهوية.
رفع مستوى تدريب الموظفين.
تعزيز الأمن في التحول الرقمي والحوسبة السحابية.

إن نموذج NIST للأمن السيبراني يمثل إطاراً مرجعياً متكاملاً يساعد المؤسسات على إدارة المخاطر الرقمية بشكل استباقي ومنهجي، من خلال رؤية شاملة تمتد من التعرف على التهديدات إلى التعافي وتحسين الأداء الأمني. وقد أصبح هذا النموذج معياراً عالمياً بفضل مرونته وسهولة تطبيقه وارتباطه الوثيق بمفاهيم الحوكمة الرقمية والجاهزية السيبرانية.

المطلب الثاني: نموذج Zero Trust

- لا ثقة في أي مستخدم أو جهاز.
- التحقق المستمر.
- مراقبة جميع الأنشطة.

يُعد نموذج الثقة الصفرية (Zero Trust Model) أحد أهم النماذج الحديثة والمتقدمة في مجال الأمن السيبراني. تم تطوير المفهوم لأول مرة عام 2010 من قبل المحلل جون كيندرڤاغ (John Kindervag) في مؤسسة Forrester Research، ليصبح لاحقاً أحد الركائز الأساسية في استراتيجيات حماية الأنظمة الرقمية على مستوى الحكومات والمؤسسات الكبرى.

ويعتمد هذا النموذج على مبدأ رئيسي يتمثل في:
"عدم الثقة بأي مستخدم أو جهاز أو تطبيق... سواء كان داخل الشبكة أو خارجها" " Never Trust, Always Verify" فهو يلغي الافتراض التقليدي بأن المستخدم الداخلي موثوق أو أن الشبكة الداخلية آمنة، ويستبدله بنظام تحقق مستمر ودقيق عبر جميع نقاط الوصول. ويقوم نموذج الثقة الصفرية على فكرة أن التهديدات يمكن أن تأتي من داخل المؤسسة كما من خارجها، وأن الاعتماد على الحماية المحيطية (Perimeter Security) لم يعد كافياً في ظل التطور الكبير للهجمات السيبرانية، وتوزع الأصول بين السحابة والإنترنت وأجهزة المستخدمين المتنقلة.

وبالتالي، يُلزم النموذج المؤسسات بتطبيق سياسات أمنية قائمة على:

التحقق المستمر (Continuous Authentication)
تحديد أقل قدر من الامتياز (Least Privilege)
تجزئة الشبكة (Micro-Segmentation)
مراقبة السلوك والأنشطة (Behavior Monitoring)

المبادئ الأساسية لنموذج Zero Trust:

1. التحقق المستمر للهويات (Verify Explicitly)

لا يسمح لأي مستخدم أو جهاز بالوصول إلا بعد التأكد من:
الهوية
صلاحيات الوصول
موقع الجهاز
مستوى الأمان
سياق العملية
ويتم ذلك باستخدام تقنيات مثل:
المصادقة متعددة العوامل (MFA)
التحقق البيومتري
إدارة الهوية والوصول (IAM / IGA)

2. مبدأ الحد الأدنى من الامتيازات (Least Privilege Access)

يُمنح المستخدم فقط الحد الأدنى من الصلاحيات اللازمة لإنجاز المهام، ويُمنع من الوصول إلى أي بيانات أو تطبيقات لا يحتاجها فعلياً.
ويتم ذلك من خلال:
سياسة الوصول الديناميكي (Dynamic Access Control)
إدارة جلسات الوصول
اعتماد مبدأ Zero Standing Privileges

3. افتراض حدوث اختراق (Assume Breach)

يعتمد Zero Trust على فرضية أن الهجوم قد وقع بالفعل، وأن على النظام:
احتواء الهجوم.
منع انتشاره.
مراقبة كل الأنشطة المشبوهة.
لذلك يستخدم تقنيات:
تجزئة الشبكة الدقيقة (Micro-Segmentation)
تحليل السلوك (UEBA)
مراقبة حركة البيانات (DPI)

مكونات: Zero Trust Architecture (ZTA)

1. إدارة الهوية والوصول (IAM)

التحقق من المستخدمين والأجهزة بشكل متكرر باستخدام MFA.

2. أمان الأجهزة (Device Security)

التأكد من:
تحديث النظام
خلوه من البرمجيات الخبيثة
توافقه مع سياسات المؤسسة

3. تجزئة الشبكة (Network Micro-Segmentation)

تقسيم الشبكة إلى أجزاء صغيرة لمنع المهاجم من التحرك بحرية في حال اخترق جزءاً منها.

4. أمان التطبيقات (Application Security)
تطبيق مبادئ Zero Trust على مستوى التطبيقات باستخدام:
Web Application Firewalls
API Security
Continuous Monitoring
5. حماية البيانات (Data Security)
استخدام تقنيات:
تصنيف البيانات
تشفير البيانات في السكون والحركة
منع التسرب (DLP)

فوائد نموذج Zero Trust للأمن السيبراني:

1. تقليل مخاطر الاختراق عبر التحقق الدائم من الهويات.
2. منع انتشار الهجمات داخل الشبكة من خلال التجزئة الدقيقة.
3. تحسين حماية البيانات الحساسة.
4. دعم بيئات العمل الهجينة والسحابية.
5. رفع مستوى مراقبة الشبكة عبر التحليلات الأمنية المستمرة.
6. تطبيق حوكمة وضوابط صارمة على جميع نقاط الوصول.
7. الاستجابة السريعة للحوادث نتيجة الرؤية الشاملة للأنشطة.

تحديات تطبيق نموذج Zero Trust:

رغم فوائده المتقدمة، يواجه النموذج بعض التحديات مثل:
التكلفة العالية للتحول من الأنظمة التقليدية.
تعقيد البيئات التكنولوجية الكبيرة.
الحاجة إلى إدارة دقيقة للهوية والصلاحيات.
مقاومة التغيير داخل المؤسسات.
ضرورة التكامل بين أنظمة متعددة.

لذا يُعد نموذج Zero Trust نموذجاً ثورياً في الأمن السيبراني، يعمل على تحقيق حماية شاملة للبنية التحتية الرقمية من خلال إلغاء الثقة في أي مكوّن من مكوّنات الشبكة، واعتماد التحقق المستمر، والحد الأدنى من الامتيازات، وتجزئة الشبكات، والمراقبة الاستباقية. وقد أصبح هذا النموذج خياراً استراتيجياً للجهات الحكومية والمؤسسات التي تسعى لرفع جاهزيتها في مواجهة الهجمات المتقدمة، خاصة في ظل التحول الرقمي واعتماد الحوسبة السحابية.

المطلب الثالث: نموذج Defense in Depth

تعدد طبقات الحماية:

- الشبكة.
- الأجهزة.
- التطبيقات.
- المستخدم.

يُعد نموذج الدفاع المتعدد الطبقات (Defense in Depth) أحد أشهر وأقدم النماذج المعتمدة في مجال الأمن السيبراني، ويهدف إلى توفير حماية شاملة للأنظمة الرقمية من خلال تطبيق عدة طبقات متكاملة من الدفاع بدلاً من الاعتماد على آلية حماية واحدة. ظهر هذا النموذج في الأصل من الاستراتيجيات العسكرية الدفاعية، قبل أن يُعتمد على نطاق واسع في أمن المعلومات لحماية الشبكات، والبيانات، والبنى التحتية التقنية.

ويقوم هذا النموذج على فكرة أساسية مفادها أن المهاجم سيواجه سلسلة من الدفاعات المتراكبة والمتتالية، بحيث يؤدي اختراق طبقة منها إلى مواجهته طبقة أخرى، ما يقلل من احتمالات النجاح ويزيد الوقت اللازم لاختراق المؤسسة، مما يمنح فرق الأمن السيبراني فرصة كشف التهديد واحتوائه.

أولاً: مفهوم Defense in Depth

يعني "الدفاع في العمق" تطبيق عدة طبقات مستقلة ولكن مترابطة من الحماية تشمل:
ضوابط تقنية، ضوابط إدارية، ضوابط فيزيائية.
والهدف من هذه الطبقات هو منع الهجمات، واكتشافها في حال حدوثها، والاستجابة لها بكفاءة.
ويُستخدم هذا النموذج بكثرة في المؤسسات الضخمة التي تتعامل مع بيانات حساسة أو تعمل في بيئات معقدة، بما في ذلك:
الحكومات، المؤسسات المالية، شركات الاتصالات، البنية التحتية الحيوية (المياه، الطاقة، الصحة)

ثانياً: المبادئ الأساسية لنموذج الدفاع المتعدد الطبقات:

1. الطبقات المتتابعة من الحماية (Layered Security)

يعتمد النموذج على وضع عدة مستويات من الدفاع تشمل:
الشبكات
الخوادم
التطبيقات
قواعد البيانات
الأجهزة
المستخدمين
بحيث تعمل كل طبقة كحاجز مستقل.

2. عدم الاعتماد على طبقة واحدة (No Single Point of Failure)

وجود بدائل متعددة يقلل من احتمالية انهيار النظام الأمني بالكامل في حال اختراق طبقة معينة.

3. التكامل والتعاضد بين الطبقات (Integrated Defense)

تتكامل طبقات الدفاع معاً عبر:
مشاركة البيانات الأمنية.
التحليلات الموحدة.
سياسات موحّدة لإدارة التهديدات.

ثالثاً: الطبقات الأساسية في نموذج Defense in Depth

يختلف عدد الطبقات بحسب المؤسسة، لكن غالباً ما يشمل النموذج ما يلي:

1. الطبقة الفيزيائية (Physical Security)

تشمل حماية مراكز البيانات والمكاتب باستخدام:
كاميرات المراقبة.
أنظمة الدخول البيومتري.
أقفال إلكترونية.
حراسة أمنية.

2. طبقة حماية الشبكات (Network Security) تشمل:
الجدران النارية (Firewalls).
أنظمة كشف التسلل ومنعه IDS/IPS.
تقسيم الشبكة (Segmentation).
VPN

مراقبة حركة المرور
3. طبقة حماية الأجهزة (Endpoint Security) تشمل:
برامج مكافحة الفيروسات.
أدوات EDR (Endpoint Detection and Response).
إدارة التحديثات Patch Management.
4. طبقة حماية التطبيقات (Application Security) تشمل:
اختبار الاختراق للتطبيقات.
جدران حماية تطبيقات الويب WAF.
فحص الأكواد Static & Dynamic Analysis.
5. طبقة حماية البيانات (Data Security) تشمل:
تشفير البيانات أثناء النقل والسكون.
إدارة الحقوق الرقمية DRM.
منع التسرب DLP.
تصنيف البيانات.
6. طبقة المستخدمين (User Security) تشمل:
سياسات كلمات المرور.
المصادقة متعددة العوامل MFA.
التوعية الأمنية.
منع الوصول غير المصرح به.
7. طبقة المراقبة والاستجابة للحوادث (Monitoring & Incident Response) تشمل:
أنظمة SIEM.
فرق الاستجابة للحوادث (CSIRT).
تحليل السلوك (UEBA).
التحقيق الرقمي Digital Forensics.

رابعاً: فوائد نموذج Defense in Depth:

1. تعزيز الحماية الشاملة من خلال طبقات متعددة.
2. زيادة صعوبة الهجوم وإطالة مدة الاختراق مما يزيد فرص اكتشافه.
3. تقليل التأثير الناتج عن الاختراق عبر احتواء الهجمات.
4. حماية البيانات الحساسة من التسرب أو التشويه.
5. المرونة في مواجهة التهديدات المتقدمة (APTs).
6. تقليل نقطة الفشل الواحدة داخل النظام الأمني.

خامساً: التحديات التي تواجه نموذج Defense in Depth:

1. التكلفة المرتفعة لتطبيق جميع الطبقات.
2. صعوبة الإدارة خاصة في بيئات المؤسسات الضخمة.
3. احتمال وجود تعارض بين الأنظمة الأمنية.
4. الحاجة إلى خبرات متقدمة لإدارة التنسيق بين الطبقات.

ويعد نموذج Defense in Depth من أهم النماذج الاستراتيجية للأمن السيبراني، حيث يهدف إلى توفير حماية شاملة للمؤسسات عبر طبقات متعددة من الدفاع المتكامل.
وهو فعّال بشـــكل خاص في مواجهة الهجمات المتقدمة وتوفير اســـتجابة مرنة وســـريعة عند وقوع الاختراقات، مما يجعله خياراً أساسياً للمؤسسات التي تسعى لتعزيز جاهزية بنيتها الرقمية وحماية بياناتها الحيوية.

عاشراً: الأطار العملي

الأساليب الإحصائية: يستخدم البحث الأساليب التالية:

1. الإحصاء الوصفي:
   - المتوسط الحسابي
   - الانحراف المعياري
   - التكرارات والنسب المئوية
2. اختبار الثبات Reliability
   معامل كرونباخ ألفا (Cronbach Alpha)
3. تحليل الارتباط Correlation
4. تحليل الفجوة Gap Analysis

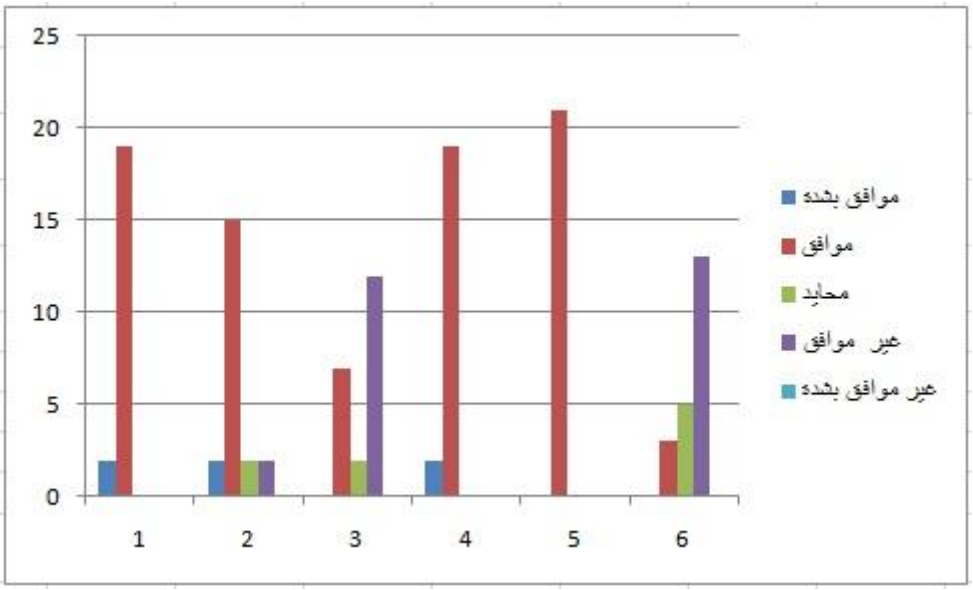
لتحديد الفرق بين الوضع الحالي والمستوى المعياري للأمن السيبراني.

النتائج العملية

عنوان البحث: تقييم مستوى جاهزية البنية التحتية الرقمية في مواجهة الهجمات السيبرانية المتقدمة

جدول رقم (1): محور جاهزية البنية التحتية الرقمية

الرقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	**تمتلك المؤسسة بنية تحتية تقنية حديثة ومحدّثة بشكل دوري.**	**2**	**19**	**0**	**0**	**0**
2	**تتوفر أنظمة حماية قوية على مستوى الشبكة والخوادم.**	**2**	**15**	**2**	**2**	**0**
3	**يتم إجراء صيانة دورية لمكونات البنية التحتية.**	**0**	**7**	**2**	**12**	**0**
4	**توجد خطط واضحة لتحديث الأجهزة والبرمجيات.**	**2**	**19**	**0**	**0**	**0**
5	**أنظمة التشغيل المستخدمة محدثة وآمنة.**	**0**	**21**	**0**	**0**	**0**
6	**تتوفر أجهزة كشف التسلل (IDS/IPS) في الشبكة.**	**0**	**3**	**5**	**13**	**0**

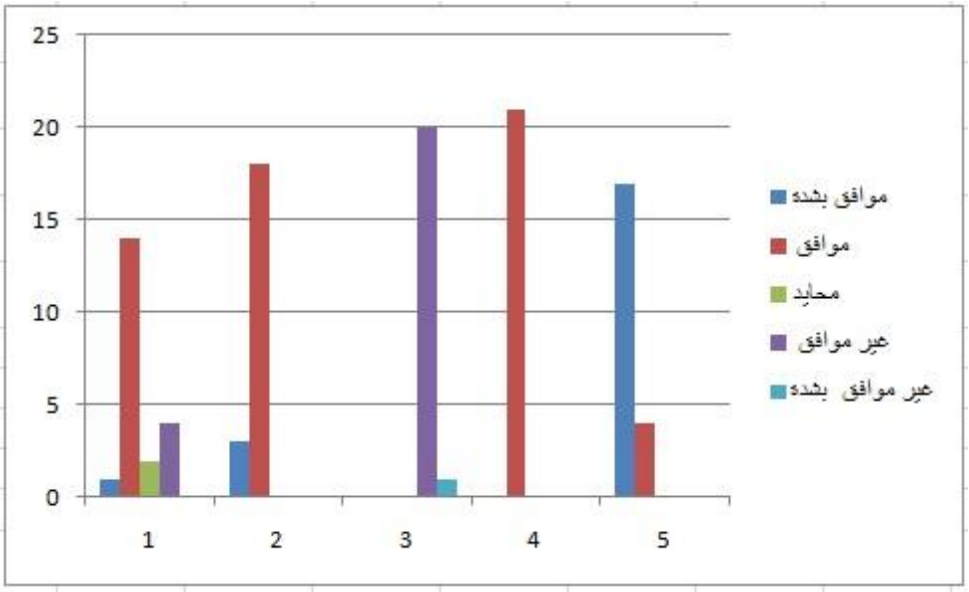


شكل رقم (1): محور جاهزية البنية التحتية الرقمية

من خلال الجدول السابق نجد أن المؤسسة تمتلك بنية تحتية تقنية حديثة ومحدّثة بشكل دوري موافقين بنسبة 90.4%، تتوفر أنظمة حماية قوية على مستوى الشبكة والخوادم موافقين بنسبة 71.4%، يتم إجراء صيانة دورية لمكونات البنية التحتية. غير موافقين بنسبة 57.14%، أنظمة التشغيل المستخدمة محدثة وآمنة. موافقين بنسبة 100%، تتوفر أجهزة كشف التسلل (IDS/IPS) في الشبكة غير موافقين بنسبة 61.9%.

جدول رقم (2) قدرات الكشف المبكر عن الهجمات المتقدمة

الرقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	تستخدم المؤسسة أنظمة SIEM لمراقبة الأحداث الأمنية.	1	14	2	4	0
2	يتم تحليل السجلات (Logs) بشكل يومي للكشف عن أي نشاط غير طبيعي.	3	18	0	0	0
3	تعتمد المؤسسة على أدوات الذكاء الاصطناعي في الكشف عن التهديدات.	0	0	0	20	1
4	يتم تدريب الموظفين على اكتشاف الهجمات المتقدمة مثل APT.	0	21	0	0	0
5	توجد آلية لتحديد نقاط الضعف بشكل مستمر.	17	4	0	0	0

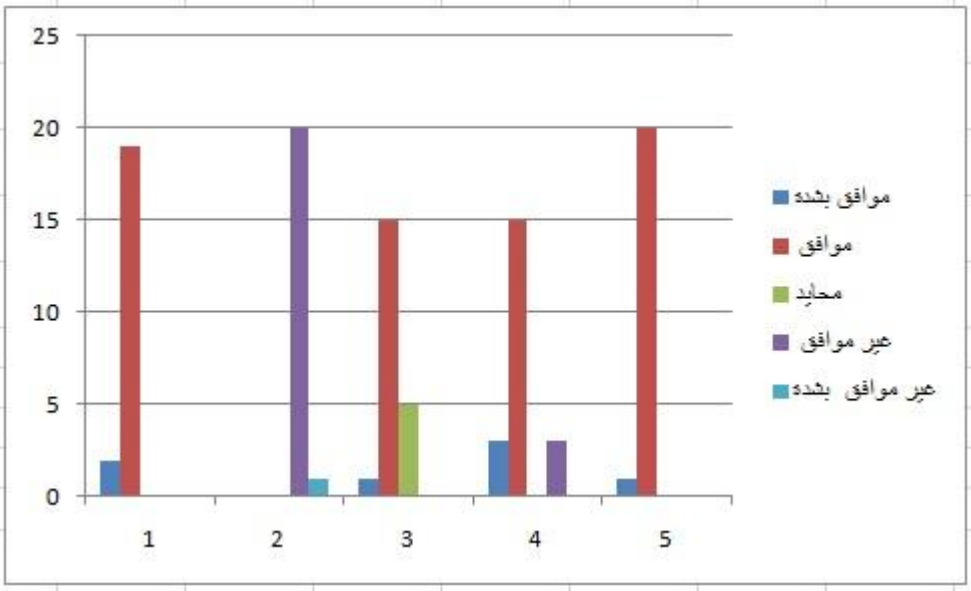


شكل رقم (2) قدرات الكشف المبكر عن الهجمات المتقدمة.

يتضح من الجدول والشكل البياني السابقين أن المؤسسة تستخدم أنظمة SIEM لمراقبة الأحداث الأمنية موافقين بنسبة 66.6%، يتم تحليل السجلات (Logs) بشكل يومي بنسبة للكشف عن أي نشاط غير طبيعي موافقين بنسبة 85.7%، تعتمد المؤسسة على أدوات الذكاء الاصطناعي في الكشف عن التهديدات غير موافقين بنسبة 95.2%، يتم تدريب الموظفين على اكتشاف بنسبة الهجمات المتقدمة مثل APT موافقين بنسبة 100%، توجد آلية لتحديد نقاط الضعف بشكل مستمر موافقين بشدة بنسبة 80.9%.

جدول رقم (3) الاستجابة للحوادث الرقمية.

الرقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	توجد خطة واضحة للاستجابة للحوادث الأمنية (Incident Response Plan)	2	19	0	0	0
2	يتم إجراء محاكاة دورية للهجمات الرقمية لاختبار الجاهزية.	0	0	0	20	1
3	لدى المؤسسة فريق متخصص بإدارة الحوادث.	1	15	5	0	0
4	يتم توثيق الحوادث الرقمية وتحليل أسبابها.	3	15	0	3	0
5	تتوفر آلية لإعادة الأنظمة إلى العمل بسرعة بعد الهجوم.	1	20	0	0	0

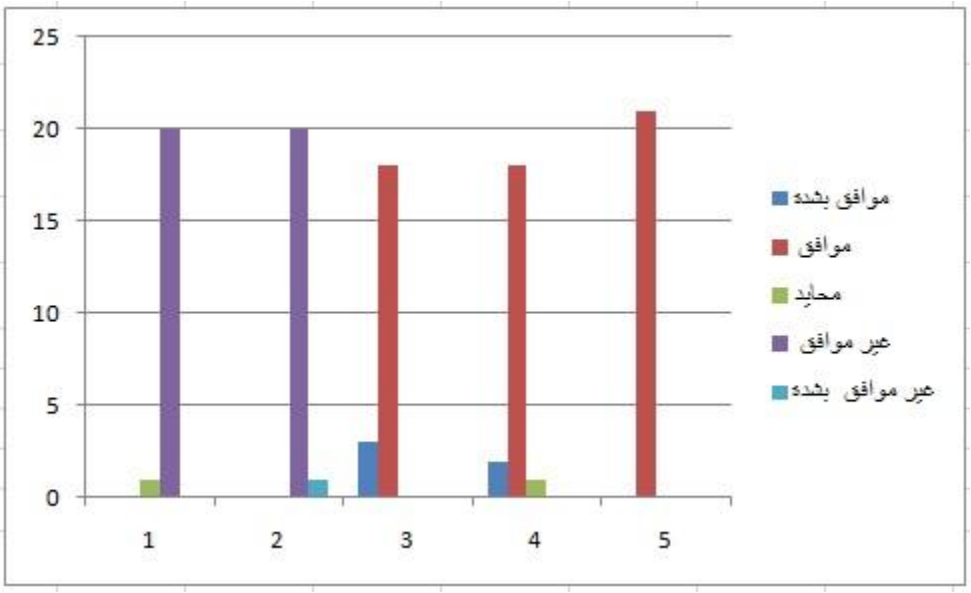


جدول رقم (3) الاستجابة للحوادث الرقمية.

يتضح من الجدول والشكل البياني السابقين أنه توجد خطة واضحة للاستجابة للحوادث الأمنية (Incident Response Plan) موافقين بنسبة 90.4%، يتم إجراء محاكاة دورية للهجمات الرقمية لاختبار الجاهزية غير موافقين بنسبة 95.2%، لدى المؤسسة فريق متخصص بإدارة الحوادث موافقين بنسبة 71.4%، يتم توثيق الحوادث الرقمية وتحليل أسبابها. موافقين بنسبة 71.4%، تتوفر آلية لإعادة الأنظمة إلى العمل بسرعة بعد الهجوم. موافقين بنسبة 95.2%.

جدول رقم (4): تطبيق المعايير الدولية للأمن السيبراني.

الرقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
1	تطبق المؤسسة معايير ISO 27001.	0	0	1	20	0
2	تتبع المؤسسة إطار NIST للتحكم في التهديدات.	0	0	0	20	1
3	يتم إجراء تدقيق أمني دوري على جميع الأنظمة.	3	18	0	0	0
4	لدى المؤسسة سياسة لإدارة الهوية والصلاحيات IAM.	2	18	1	0	0
5	يوجد نظام فعال للنسخ الاحتياطي واسترجاع البيانات.	0	21	0	0	0



شكل رقم (4): تطبيق المعايير الدولية للأمن السيبراني.

يتضح من الجدول والشكل البياني السابقين أن المؤسسة تطبق معايير ISO 27001 غير موافقين بنسبة 95.2%، تتبع المؤسسة إطار NIST للتحكم في التهديدات غير موافقين بنسبة 95.2%، يتم إجراء تدقيق أمني دوري على جميع الأنظمة موافقين بنسبة 85.7%، لدى المؤسسة سياسة لإدارة الهوية والصلاحيات IAM موافقين بنسبة 85.7%، يوجد نظام فعال للنسخ الاحتياطي واسترجاع البيانات. موافقين بنسبة 100%.

النتائج:

1. وجود فجوة بين الوضع الحالي والمستوى المعياري للأمن السيبراني.
2. جاهزية متوسطة للبنية التحتية الرقمية لكنها غير كافية لمواجهة الهجمات المتقدمة.
3. ضعف في قدرات الكشف المبكر بسبب عدم وجود أدوات ذكاء اصطناعي.
4. قصور في خطط الاستجابة للحوادث وغياب محاكاة دورية للهجمات.
5. اعتماد جزئي وغير كامل للمعايير الدولية.
6. تمتلك المؤسسة بنية تحتية تقنية حديثة ومحدّثة بشكل دوري.
7. تتوفر أنظمة حماية قوية على مستوى الشبكة والخوادم.
8. لايتم إجراء صيانة دورية لمكونات البنية التحتية.
9. أنظمة التشغيل المستخدمة محدثة وآمنة.
10. لا تتوفر أجهزة كشف التسلل (IDS/IPS) في الشبكة.
11. تستخدم المؤسسة أنظمة SIEM لمراقبة الأحداث الأمنية.
12. يتم تحليل السجلات (Logs) بشكل يومي بنسبة للكشف عن أي نشاط غير طبيعي.
13. لا تعتمد المؤسسة على أدوات الذكاء الاصطناعي في الكشف عن التهديدات.
14. يتم تدريب الموظفين على اكتشاف بنسبة الهجمات المتقدمة مثل APT.
15. توجد آلية لتحديد نقاط الضعف بشكل مستمر.
16. توجد خطة واضحة للاستجابة للحوادث الأمنية (Incident Response Plan).
17. لا يتم إجراء محاكاة دورية للهجمات الرقمية لاختبار الجاهزية.
18. لدى المؤسسة فريق متخصص بإدارة الحوادث.
19. يتم توثيق الحوادث الرقمية وتحليل أسبابها.

20. تتوفر آلية لإعادة الأنظمة إلى العمل بسرعة بعد الهجوم.
21. تطبق المؤسسة معايير ISO 27001.
22. تتبع المؤسسة إطار NIST للتحكم في التهديدات.
23. يتم إجراء تدقيق أمني دوري على جميع الأنظمة.
24. لدى المؤسسة سياسة لإدارة الهوية والصلاحيات IAM.
25. يوجد نظام فعال للنسخ الاحتياطي واسترجاع البيانات.

التوصيات:

1. تحديث البنية التحتية الرقمية وتوفير أجهزة أكثر مقاومة للهجمات المتقدمة.
2. اعتماد أنظمة SIEM + SOAR لرفع القدرة على الكشف والاستجابة.
3. تفعيل التدريب المستمر للموظفين على الهجمات المتقدمة (APT – Zero-day).
4. تطوير سياسة أمنية تتوافق تمامًا مع معايير NIST و ISO 27001.
5. إجراء اختبارات اختراق دورية وسنوية لتقييم مستوى الحماية.
6. إنشاء مركز عمليات أمنية SOC متكامل.
7. يجب أن يتم إجراء صيانة دورية لمكونات البنية التحتية.
8. يجب أن تتوفر أجهزة كشف التسلل (IDS/IPS) في الشبكة.
9. يجب أن تعتمد المؤسسة على أدوات الذكاء الاصطناعي في الكشف عن التهديدات.
10. يجب أن تطبق المؤسسة معايير ISO 27001.
11. يجب أن تتبع المؤسسة إطار NIST للتحكم في التهديدات.

قائمة المراجع:

المراجع العربية:

1. الحربي، أحمد. (2020). جاهزية المؤسسات الحكومية للأمن السيبراني. الرياض: مجلة تقنية المعلومات.
2. القحطاني، بدر. (2021). تحليل البنية الرقمية في مواجهة الهجمات الإلكترونية. جامعة الملك سعود.
3. العوضي، محمد. (2022). الاستجابة للحوادث الرقمية وأثرها على الأمن السيبراني. مجلة الأمن المعلوماتي.

المراجع الأجنبية:

1. Smith, J., & Walker, A. (2019). Cyber Infrastructure Readiness Assessment. Journal of Cybersecurity.
2. NIST. (2021). Cybersecurity Framework. National Institute of Standards and Technology.
3. Chen, L., & Zhao, H. (2023). Advanced Persistent Threats and Digital Defense Strategies. Cyber Defense Review.
4. ISO. (2022). ISO/IEC 27001 Information Security Management Systems. International Organization for Standardization.