الجمهورية العربية السورية
وزارة التعليم العالي
الجامعة الافتراضية السورية
ماجستير إدارة تقانة

Syrian Arab Republic
Ministry of Higher Education
Syrian Virtual University
PMTM

بحث مقدم لنيل درجة الماجستير في إدارة التقانة التخصّصي PMTM

بعنوان:

تقييم تأثير تطبيق برنامج SIEM في تعزيز دور أمن المعلومات في المصارف العاملة في الجمهورية العربية السورية

Evaluating the effect of implementing SIEM solution in enhancing the role of information security in banks operating in Syrian Arab Republic

إعداد الطالبة:

دولت جرجس العلي

الرقم الجامعي: 215885

الفصل الدراسي F23

إشراف:

د. باسم السهوة

الإهداء

إلى اليدين النظيفتين اللتين جعدتهما السنين كفاحاً وأبتا إلا سلوك الطريق المستقيم، إلى من أفخر بنسبي له، أهديك هذا النجاح بابا حبيبي.

والدي جرجس العلي

إلى التي وجهت بوصلتي إلى طريق العلم والمعرفة منذ نعومة أظافري، دوناً عن كل أفضالك عليّ، بفضلك ماما أنا أعدُّ اليوم هذا البحث وأنال هذه الشهادة، ياوجودي وصلاتي.

والدتي سلوى عدره

مهدت لي هذا الطريق بعبورك له أولاً علماً ومعرفةً وحكمةً، فكنت معلمتي قبل أختي وسندي وقوتي، أهديك كل ثمار جهودي ولا تكفيني اعترافاً بفضلك.

أختي عصمت

أماني واطمئناني، الروح الحرة والفكر المتقظ، دعمتني كثيراً في مسيرتي لإعداد هذا البحث، أسأل الله أن يعوضك كل مافي الدنيا من خير وجمال.

أختي جورجينا

بيتي الثاني وعائلتي الداعمة، آمنتم بي دائماً وغمرتني محبتكم، أتمنى لكم النجاح والتفوق الدائم.

عائلتي في بنك سورية والخليج

أنت من شجعني منذ البداية وآمن بي، كم كان كبيراً حظي حين عثرت عليك يا صديقة دربي وأختي، أهديك ثمار جهودي.

أريج أورفلي

أحطتوني بكل الدعم والمساندة وما أحسست يوماً غير أنكم أخوتي، أهديكم هذا النجاح الذي هو نجاحنا جميعاً.

فريق إدارة المخاطر في بنك سورية والخليج

أخوات وصديقات وداعمات، جميلاتٌ شكلاً وصلبات وقويات من الداخل، شكراً لكل يوم دعمتوني به واحتملتم معي مصاعبه.

غيد فرح ولمى ملحم

أستاذي ومرجعي في أمن المعلومات، من لم يبخل علي بمعلومة أو نصيحة، الأخ والصديق اللطيف، شكراً لك دائماً وأبداً.

علاء الحمد

شُكرٌ وتقدير

أَحمُدُ الله الذي يسر لي إعداد هذا البحث، ثم أشكر أساتذتي الأفاضل في الجامعة الافتراضية السوريّة الذين لم يبخلوا عليَّ وعلى زملائي بالعلم والمعرفة خلال سنوات الدراسة، وأخصّ بالشكر الدكتور باسم السهوة على ماقدَّمه من جهد ووقت ومتابعة في الإشراف على إعداد هذا البحث، كما أشكر كل من شاركني خبرة وعلماً خلال مسيرتي الدراسية والمهنية.

ملخص مشروع البحث

يهدف هذا البحث إلى تناول أهمية وجود برنامج مركزي لإدارة الأحداث والمعلومات الأمنية (SIEM) في المؤسسات عامةً وفي البنوك العاملة في الجمهورية العربية السورية خاصةً ودوره في تعزيز دور فرق أمن المعلومات فيها ومساعدتها في أداء واجباتها ومهامها في حماية أصول المعلومات في البنك من مختلف التهديدات الداخلية والخارجية التي قد تتعرض لها.

تم طرح استبيان الكتروني مؤلف من 103 سؤال مصمم على منصة Google Forms على مختصي ومسؤولي أمن المعلومات وتقانة المعلومات، وتم جمع 38 استبيان وتم تحليل البيانات اعتماداً على عدد الإجابات الأعظمي لكل سؤال (Use Case)، وتوصّل البحث إلى تحديد أهم السيناريوهات الأمنية Use cases التي يحتاج فريق أمن المعلومات لضبطها وكشفها عن طريق برنامج SIEM بما يحقق أمن معلومات فعال وبيئة عمل مصرفية آمنة ومحمية قدر الإمكان، بالإضافة إلى تثقيل هذه السيناريوهات الأمنية Use cases بأوزان تبعاً لأهميتها وحراجيتها ودورها في حماية أصول المعلومات في المصرف.

انتهى البحث بتقديم مجموعة من التوصيات والمقترحات المستقبلية لتعزيز كفاءة وفعالية دور أمن المعلومات في المصارف.

الكلمات المفتاحية:

أمن المعلومات – بنك – برنامج SIEM – سيناريوهات أمنية – أصول المعلومات – أحداث أمنية – ملفات سجلات الأحداث.

Abstract

This research aims to clarify the importance of having a centralized system for managing security incidents and information in organizations in general, and in banks operating in Syrian Arab Republic particularly. And the effect of this system in reinforcement the role of information security teams in these banks and helping them doing their tasks and duties in protecting information assets from external and internal threats that may be exposed to.

An electronic survey has been designed using Google Forms platform and published to be answered by information security specialists and people operating in information technology field. 38 answers were collected and then analyzed using the "maximum number of answers" criteria. The research led to determine the most important use cases that information security teams need to detect and monitor using SIEM system which helps providing a secure banking environment as possible. Besides giving each of these use cases a weight based on its criticality and importance in protecting information assets.

The research has been finished by introducing a number or recommendations and proposals to reinforce the role of information security teams in banks.

Key words:

Information security – Bank – SIEM system – Use Cases – Information Assets – Security Incidents – Log Files.

فهرس المحتويات

قائمة الأشكال:

قائمة الجداول:

مصطلحات البحث:

الرمز	إنكليزي	عربي
SIEM	Security Information and Event Management	نظام إدارة الأحداث والمعلومات الأمنية
Logs	Log Files	ملفات السجلات
Vu	Vulnerabilities	نقاط ضعف
RA	Risk Assessment	تقييم مخاطر
	Correlation Rule	قواعد ارتباط
	Raw Data	بيانات خام
	Normalized Data	بيانات معالجة
	Use Cases	سيناريوهات أمنية
	Information Assets	أصول المعلومات
C	Information Confidentiality	سرية المعلومات
I	Information Integrity	أصالة المعلومات
A	Information Availability	توافرية المعلومات
	Threats	التهديدات
	CIA Triad	مثلث أمن المعلومات
	Incident	حدث

الفصل الأول:

الإطار العام للدراسة

1. مقدمة:

يواجه فريق أمن المعلومات في المصارف العديد من التحديات والصعوبات في معرض أدائه للواجبات والمهام المنوطة به في حماية أصول المعلومات في المصرف من مختلف التهديدات الداخلية والخارجية، ولذلك لا بُد من أن يُوفر لهذا الفريق أولاً الدعم الكافي من مجلس الإدارة والإدارة التنفيذية في المصرف انطلاقاً من إدراكهم لأهمية دور أمن المعلومات في خلق بيئة آمنة للعمل المصرفي، وثانياً الأدوات والبرامج اللازمة التي تساعد هذا الفريق في خلق هذه البيئة.

يهدف هذا البحث إلى دراسة أهمية وجود برنامج "إدارة الأحداث والمعلومات الأمنية" المركزي SIEM (Security Information and Event Management) Solution كأحد حلول أمن المعلومات الرئيسية والذي يمكن تقسيم وظائفه الأساسية إلى أولاً: إدارة المعلومات الأمنية وذلك كونه مصب لجميع ملفات السجلات log files الصادرة عن جميع تجهيزات المنظومة المعلوماتية والبنية التحتية في المصرف من مخدمات وقواعد بيانات وموجهات ومبدلات وجدران نار ومضاد فيروسات وغيرها، وتوليد تقارير بالمعلومات المستخرجة من هذه الملفات، وثانياً: إدارة الأحداث الأمنية حيث يقوم بتحليل وإدارة الأحداث في الزمن الحقيقي، وكل ذلك لغاية استصدار التنبيهات التي تحدد مواطن الضعف في المنظومة المعلوماتية لفريق أمن المعلومات وتقييمها من حيث الأثر الذي ينتج عن استغلالها وتطبيق الإجراءات العلاجية المناسبة بما يحقق بيئة آمنة تحمي أصول المعلومات في المصرف.

إن تطبيق نظام برنامج SIEM في المصارف يحقق أيضاً تطبيق الضوابط الرقابية اللازمة الصادرة عن توصيات إدارة المخاطر، إدارة التدقيق الداخلي والخارجي وإدارة الالتزام في المصرف، كما يحقق الامتثال لمتطلبات القرارات الصادرة عن الجهات الإشرافية والوصائية في الجمهورية العربية السورية مثل مصرف سورية المركزي والهيئة الوطنية لخدمات التقانة، بالإضافة لتحقيق متطلبات تطبيق بعض معايير الجودة العالمية مثل ISO 27001 الخاص بأمن المعلومات وغيرها.

2. مشكلة البحث:

نشأت مشكلة البحث من حقيقة أن:

1. المهام والمسؤوليات المطلوبة من فريق أمن المعلومات في المصارف تحتاج لوجود نظام مركزي SIEM وذلك لكون ملفات السجلات والأحداث log files الصادرة عن المنظومة المعلوماتية والبنية التحتية في المصرف عددها ضخم جداً وبصيغة خام غير معالجة وكل منها يحتوي على الآلاف من السطور ومن الغير ممكن لفريق أمن المعلومات أن يقوم بشكل يدوي بما يلي:

- ✓ مراقبة وتحليل هذه الملفات بشكلها الخام من دون معالجة وتصفية.
- ✓ استخراج وربط الأحداث الهامة مع بعضها والتي تدل على وجود ثغرات في المنظومة.
- ✓ كشف الهجمات ومحاولات الاختراق الداخلية والخارجية التي تتعرض لها المنظومة المعلوماتية في المصرف وإجراء التحقيقات اللازمة لغرض اتخاذ الإجراءات العلاجية المناسبة.

2. ضرورة ضبط معايير عمل هذا البرنامج عند تطبيقه بالقيم الصحيحة بما يساعد فريق أمن المعلومات في كشف السيناريوهات الأمنية المحتملة التي تشكل خطراً على أصول المعلومات في البنك لغاية الوقاية منها وعلاجها.

3. أهداف البحث:

تتحدد أهداف البحث من خلال البنود الأساسية التالية:

- تحديد أهم السيناريوهات الأمنية Use cases التي يحتاج فريق أمن المعلومات لضبطها وكشفها عن طريق برنامج SIEM بما يحقق أمن معلومات فعال وبيئة عمل مصرفية آمنة محمية قدر الإمكان من التهديدات الداخلية والخارجية التي تهدف إلى اختراق أصول المعلومات في المصرف.
- تثقيل هذه السيناريوهات الأمنية Use cases بأوزان تبعاً لأهميتها وحراجيتها ودورها في حماية أصول المعلومات في المصرف.
- مساعدة فرق أمن المعلومات في المصارف من خلال هذا البحث على أداء مهامها ومسؤولياتها بشكل أفضل نتيجة إضائته على العديد من النقاط الهامة.

4. أهمية البحث:

تبرز أهمية هذا البحث في الجوانب التالية:

- الحاجة الحقيقة له في بيئة العمل الواقعية المصرفية، وهو ناجم عن معاناة الباحثة وزملاؤها في فرق أمن المعلومات في المصارف العاملة في سورية والتحديات اليومية التي يواجهونها في معرض أداء مهامهم.
- تسليط الضوء على أهم السيناريوهات الأمنية التي يحتاج فريق أمن المعلومات في المصارف لضبطها ومراقبتها وكشفها عن طريق برنامج SIEM، وذلك لما تتمتع به بيئة العمل المصرفية من طبيعة حساسة وخاصة في ظل وجود خدمات مصرفية متاحة للزبائن عبر تطبيقات الموبايل البنكي والإنترنت مثل فتح الحسابات أون لاين وتحويل الأموال والدفع الالكتروني وغيرها.
- افتقار المكتبات الأكاديمية المحلية للأبحاث والدراسات التي تتناول تأثير وأهمية برنامج SIEM في تحديد وتقييم ومعالجة مخاطر أمن المعلومات في المصارف.

5. فرضية البحث:

يستند البحث على فرضية رئيسية تقول إن وجود نظام SIEM لإدارة ملفات السجلات والأحداث في المنظومة المعلوماتية للبنك يساعد فرق أمن المعلومات فيها في مراقبة السيناريوهات الأمنية التي تحدث على مصادر البيانات فيها مما يلعب دوراً هاماً في تعزيز ممارسة هذه الفرق لمهامها ومسؤولياتها.

6. منهجية البحث:

اعتمدت الدراسة المنهج الوصفي التحليلي بوصفه المنهج الذي يعتمد على دراسة المشكلات والظواهر كما توجد في الواقع ويهتم بوصفها وصفاً دقيقاً ويعبر عنها كيفياً أو كمياً.

7. الدراسات السابقة:

7.1. الدراسات العربية:

- **<u>دراسة الدكتور حسين علي قاسم الشمالي 2016 بعنوان (أمن وسرية المعلومات وأثرها في الأداء المصرفي دراسة تطبيقية على البنوك العاملة في الأردن) – أستاذ مساعد/ إدارة أعمال/ كلية توليدو الأهلية/ إربد/ الأردن:</u>**

تناولت الدراسة التعريف بأهمية وأثر أمن المعلومات وسريتها في الأداء المصرفي في البنوك العاملة في الأردن وطبقت الدراسة على عينة عشوائية تكونت من 13 بنك أي بنسبة 50% من مجتمع الدراسة المؤلف من 26 بنك عامل في الأردن.

أظهرت نتائج الدراسة أن مستوى ممارسة أمن المعلومات وسريتها في البنوك الأردنية يعتبر مرتفع من حيث الأهمية النسبية، كما بينت وجود أثر ذي دلالة إحصائية عند مستوى الدلالة (P<=0.05) لأمن وسرية المعلومات بأبعادها في الأداء المصرفي في البنوك العاملة في الأردن، إذ كان معامل الارتباط (R=0.755) وهذا يشير إلى العلاقة الموجبة.

أوصت هذه الدراسة إلى ضرورة تبني وتطبيق إدارات البنوك في الأردن للممارسات اللازمة لنشر ثقافة أمن المعلومات في مختلف المستويات الإدارية عن البرامج التدريبية، بالإضافة لتخصيص المزيد في خطة الإنفاق على برامج وحلول أمن المعلومات، والسعي للحصول على الشهادات العالمية المطابقة لأنظمة المعلومات الدولية.

- **<u>دراسة الأستاذ المهندس الدكتور نزار كاظم الكيخاني 2017 بعنوان (حماية أمن المعلومات المصرفية وفق المواصفات العالمية ISO 17799 ومدى تطبيقه في المصارف – دراسة تحليلية مقارنة بين بعض المصارف الخاصة في العراق ولبنان) – جامعة القادسية – كلية الإدارة والاقتصاد:</u>**

تقصت الدراسة عن مدى تطبيق المواصفات العالمية لأمن المعلومات ISO 17799 كأداة فاعلة في حماية أمن المعلومات وسريتها في المصارف العراقية واللبنانية، اختارت الدراسة 5 مصارف عراقية خاصة و5 مصارف لبنانية خاصة كعينة للبحث، امتازت هذه المصارف بأهميتها في التعامل داخل اقتصاد كل بلد إضافة إلى قدم تأسيس كل مصرف وفاعليته في الحركة المصرفية.

ولجمع البيانات استخدم الباحث استبانة تكونت من 30 فقرة تشير إلى مدى فهم وتطبيق المواصفة ISO 17799 وتم توزيع 160 استمارة (80 لكل بلد) شملت مديري الفروع ومعاونيهم وبعض الموظفين وبنتيجة الدراسة أن المصارف العراقية لا تطبق المواصفة العالمية ISO 17999 لحماية أمن معلوماتها المصرفية بينما تطبق المصارف اللبنانية هذه المواصفة.

أوصت الدراسة بضرورة اعتماد جميع بنود ومضامين المواصفات العالمية ISO 17799 في القطاعات المصرفية لزيادة كفاءة النظم الحامية للعمل المصرفي، بالإضافة لزج العاملين وإدارات المصارف في دورات ترفع من قدراتهم في أمن المعلومات وتبويب وأرشفة الخطوات التي تتخذها المصارف العاملة في العراق في جانب تطبيق المواصفة.

- **دراسة نبيلة قرزيز ومحمد زيدان 2021 بعنوان (دور أمن المعلومات في تحقيق جودة الخدمات المصرفية – دراسة حالة القرض الشعبي الجزائري بالشلف) – جامعة الشلف – الجزائر:**

سلطت الدراسة الضوء على مدى تأثير أمن المعلومات على تحقيق جودة الخدمات المصرفية بالقرض الشعبي الجزائري لولاية الشلف، وتكونت العينة التي اختارها الباحثون من 55 موظف في المصرف تم انتقائهم من ذوي الاطلاع على أمن المعلومات وكانت نتيجة الدراسة وجود علاقة ذات دلالة إحصائية عند مستوى الدلالة ($P<=0.05$) بين أمن المعلومات بأبعاده الثلاثة (السرية والسلامة والتوافرية) وجودة الخدمات المصرفية.

أوصت الدراسة بضرورة الاهتمام أكثر بتوظيف مختصين في أمن المعلومات في البنك وتوفير برامج الحماية اللازمة من عمليات القرصنة والاحتيال، بالإضافة لضرورة قيام البنك بشكل دوري بتقييم المخاطر الناتجة عن ممارسته لأنشطته المختلفة لغرض وضع الإجراءات العلاجية اللازمة لحمايتها.

- **دراسة شيرين عبد الملك عبد القوي المخلافي 2018 بعنوان (دور نظام أمن المعلومات في تطوير الخدمات المصرفية – دراسة ميدانية بالتطبيق على البنوك اليمنية) – المجلة العلمية للدراسات التجارية والبيئية (العدد الثاني – الجزء الثاني – المجلد التاسع):**

تناولت الدراسة العلاقة بين نظام أمن المعلومات وتطوير الخدمات المصرفية، استخدمت الباحثة المنهج الوصفي لإنجاز الدراسة، حيث تألف مجتمع البحث من 204 فرد من سبع بنوك تجارية يمنية وعينة البحث من 133 فرد من العاملين في إدارة وأقسام تكنولوجيا المعلومات والتسويق وخدمة العملاء في البنوك اليمنية، واستفسرت الأسئلة المطروحة في الاستبيانات الموزعة عن مدى تطبيق

البنك للسرية والخصوصية والاعتمادية والتوافرية للمعلومات والخدمات المصرفية بالإضافة لمدى دعم الإدارة العليا لتطوير الخدمات.

خلصت الدراسة إلى وجود علاقة إيجابية بدلالة إحصائية بين السرية والخصوصية وجميع أبعاد تطوير الخدمات المصرفية، بينما توجد علاقة ضعيفة بين الاعتمادية وخدمة المعلومات الالكترونية ولكن بشكل عام توجد علاقة إيجابية بدلالة إحصائية بين الاعتمادية وباقي أبعاد تطوير الخدمات المصرفية.

أوصت الدراسة بقيام البنوك اليمنية ببناء سياسات تتعلق بأمن المعلومات والعمل على نشرها وتطبيقها لما لها من أثر في تحسين الإجراءات الأمنية، بالإضافة لوضع برامج ومصفوفات خاصة بالأدوار والصلاحيات على نظم المعلومات[1]، وضرورة توجيه الجهود التسويقية في البنوك نحو تغيير العادات المصرفية لدى العملاء مما يزيد من اطمئنانهم الأمني تجاه الخدمات المصرفية.

7.2. الدراسات الأجنبية:

- **Remus, M. S. H., Akter, S., & Ferdous, K. (2023) بعنوان (تقييم مدى تطبيق أمن تكنولوجيا المعلومات والاتصالات في البنوك – دراسة حالة البنوك البنغلادية) المجلة الأوروبية لعلوم الحاسب وتكنولوجيا المعلومات:**

تناولت الدراسة مدى تطبيق معايير أمن تكنولوجيا المعلومات والاتصالات في بنوك بنغلاديش بما يلتزم مع التوجيهات الصادرة عن البنك المركزي البنغلادي، وخصصت الدراسة أربعة معايير للسؤال عن مدى تطبيقها في الاستبيان وهي (**PAM** وهو برنامج لإدارة وحماية ومراقبة الحسابات ذات الصلاحيات العالية في منظومة المعلومات والاتصالات، **PCI DSS** وهو معيار خاص بأنظمة الدفع الالكتروني والبطاقات الائتمانية مصمم لحماية بيانات البطاقات من السرقة واستغلالها في عمليات الاحتيال، **SIEM** برنامج يلعب دور هام في تحليل الأحداث الأمنية الصادرة عن التطبيقات والمخدمات والتجهيزات الشبكية وقواعد البيانات وجدران النار وغيرها، **تقييم مخاطر نظم المعلومات والاتصالات** عن طريق تحديد وقياس وتصنيف المخاطر المتعلقة باستخدام أصول المعلومات وتحديد الإجراءات اللازمة للاستجابة والعلاج وهي عملية مستمرة).

[1] مصفوفة توضح الأدوار والمهام والمسؤوليات والصلاحيات الممنوحة لموظفي تقانة المعلومات على الأنظمة بحيث تحقق مبدأي فصل المهام والرقابة الثنائية ويجب أن تكون مُصادقة من قبل مجلس إدارة المؤسسة.

تألفت عينة البحث من 10 بنوك بنغلادية قامت بالإجابة عن الأسئلة المطروحة في الاستبيان لقياس مدى تطبيق المعايير الأربعة المذكورة أعلاه، خلصت الدراسة إلى أن البنوك عينة البحث تطبق بالترتيب وبشكل تناقصي كما يلي (المعيار الرابع بنسبة جيد جداً– ثم الأول بنسبة مرضي–ثم الثالث بنسبة مرضي–ثم الثاني بنسبة مرضي) من مقياس (ممتاز–جيد جداً–جيد–مرضي–قريب من الحد الأدنى)، أوصت الدراسة ببذل المزيد الجهود من قبل البنوك لرفع مستوى النسب إلى ممتاز.

- **Jangampeta S. (2022) بعنوان (أمن البيانات المالية وبرنامج SIEM–حماية المعلومات المالية الحساسة في الأنظمة البنكية والمالية) المجلة التركية لتعليم الحاسب والرياضيات:**

تحدثت الدراسة عن أهمية حماية بيانات العملاء المالية والشخصية الحساسة في المؤسسات المالية ودور برنامج SIEM في صد هجمات تصيد البيانات Phishing Attacks والحرمان من الخدمة DDos وتسرب البيانات والاحتيال وغيرها، وذلك لما يتميز به من القدرة على كشف هذه الهجمات في الوقت الحقيقي لحدوثها و القدرة على الاستجابة لها والتخفيف من أثرها.

أوصت الدراسة بضرورة تطبيق المؤسسات المالية لبرنامج SIEM في بيئاتها للاستفادة من ميزاته ولما له من دور في تحسين واقع أمن المعلومات فيها والحماية من التهديدات الأمنية المحتملة على معلوماتها الحساسة.

- **Cugnasco F. (2023) بعنوان (تحليل منصة مكافحة الاحتيال متعددة القنوات في العمليات المصرفية) – جامعة تورينو إيطاليا – دراسة أعدت لنيل الماجستير في هندسة الحاسوب:**

ركز البحث على دراسة كيفية تقديم تحسينات في هيكلية منظومة كشف الاحتيال في البنوك وبما يبقيها على اطلاع دائم على أحدث التحديات والتكنولوجيا لتكون دائماً متطورة وجاهزة للوقوف في وجه الأنواع المتعددة والحديثة من الهجمات، وبين البحث دور برنامج SIEM كجزء في هذه المنظومة كونه أداة مركزية لتجميع كل ملفات الأحداث logs للأنظمة التي تعالج البيانات في البنك وتحليلها بناءً على القواعد المبنية من فريق أمن المعلومات (correlation rules) ومن ثم توليد

التنبيهات alerts للشخص المنشئ لهذه القواعد بناءً على نتائج التحليل والتي تنذر بحدوث حالة احتيال في البنك.

- **Urien P ، Pasguet M., ،Achemlal, M., Gharout, S., & Gaber, C. (2012) بعنوان (التحديات الأمنية لبرنامج SIEM في خدمات نقل الأموال عبر الهواتف الجوالة) جامعة كان – فرنسا:**

الغرض من هذا البحث هو طرح التحديات التي تواجه برنامج SIEM في كشف حالات الاحتيال وغسل الأموال في أنظمة الدفع ونقل الأموال عبر الموبايل وذلك في ظل ازدياد انتشار هذه الأنظمة، وتتراوح هذه التحديات بحسب البحث بين السيناريوهات المعقدة التي يحتاج البرنامج لتحليلها وذلك باستخراج المعلومات اللازمة من الأحداث المختلفة التي جمعها، مرونة البرنامج في بناء قواعد متعددة البارمترات والوسائط وذلك من مصادر مختلفة للأحداث، قدرة البرنامج على كشف حالات الاحتيال في الوقت الحقيقي، قدرة البرنامج على التوسع في ظل توسع أنظمة الدفع والنقل عبر الموبايل، وأخيراً قدرة البرنامج على ربط أحداث صادرة من طبقات مختلفة من الشبكة مثلاً من طبقتي Network و Application.

7.3. التعقيب على الدراسات السابقة:

تزخر الدراسات الأجنبية بالعديد من الأبحاث التي تتناول الدور الهام والاستراتيجي لنظام SIEM في المصارف في حماية البيانات الحساسة وأمن أنظمة الدفع الالكتروني والتطبيقات البنكية وكشف الاحتيال، بالإضافة للتحديات التي يواجهها البرنامج في هذه البيئات، وفي ذات الوقت تكاد أن تكون الدراسات العربية التي تناولت الموضوع نادرة، وتقتصر فقط على الإضاءة على دور أمن المعلومات بشكل عام في حماية بيانات المصارف الحساسة وأثره في تحقيق جودة الخدمات المصرفية.

فيما يلي تلخيص نتائج الدراسات السابقة وفق الجدول التالي:

م	الدراسات السابقة	العنوان	نتائج الدراسة
1	دراسة الدكتور حسين علي قاسم الشمالي 2016 – كلية توليدو الأهلية – الأردن	أمن وسرية المعلومات وأثرها في الأداء المصرفي دراسة تطبيقية على البنوك العاملة في الأردن	* جاء اهتمام البنوك العاملة في الأردن لمستوى أمن وسرية المعلومات بأهمية نسبية مرتفعة، وقد جاء في المرتبة الأولى بعد (الحماية المادية)، بينما جاء حماية الأفراد بالمرتبة الثانية وفي المرتبة الأخيرة الحماية البرمجية، مايشير إلى أن ممارسة أمن وسرية المعلومات في البنوك العاملة في الأردن مرتفعة. * أما مستوى الأداء المصرفي من حيث الأهمية النسبية مرتفعة، إذ بلغ المتوسط الحسابي لهذا المتغير (4.07). * لقد تبين أن أمن وسرية المعلومات بأبعادها (الحماية المادية وحماية الأفراد والحماية البرمجية) لها أثر في الأداء المصرفي في البنوك العاملة في الأردن.
2	دراسة الأستاذ المهندس الدكتور نزار كاظم الكيخاني 2017 – جامعة القادسية–كلية الإدارة والاقتصاد	حماية أمن المعلومات المصرفية وفق المواصفات العالمية ISO 17799 ومدى تطبيقه في المصارف – دراسة تحليلية مقارنة بين بعض المصارف الخاصة في العراق ولبنان	* تعد متضمنات المواصفات العالمية ISO 17799 من أهم الوثائق التوجيهية للمنظمات بشكل عام وللمصارف بشكل خاص لبناء هيكلية متينة لإدارة أمن المعلومات المصرفية. * لا تطبق المصارف العراقية المواصفات العالمية ISO 17799 باختلاف أبعادها العشرة. * تطبق المصارف اللبنانية المواصفات العالمية ISO 17799 لحماية أمن معلوماتها المصرفية وبأبعادها العشرة. * تتباين المصارف العراقية واللبنانية في تطبيقها للمواصفات العالمية ISO 17799 لحماية أمن معلوماتها المصرفية.

3	دراسة نبيلة قرزيز ومحمد زيدان 2021 – جامعة الشلف – الجزائر	دور أمن المعلومات في تحقيق جودة الخدمات المصرفية – دراسة حالة القرض الشعبي الجزائري بالشلف	* احتل بعد حماية سرية البيانات في محور أمن المعلومات الدرجة الأولى ليليه في المركز الثاني بعد الحفاظ على سلامة البيانات، وفي المركز الثالث. بعد توافر البيانات للمخولين، مما يدل على اهتمام إدارة القرض الشعبي الجزائري بالشلف بخصوصية أمن المعلومات مع التوعية المستمرة للموظفين. * يولي البنك أهمية بالغة لمعلومات العملاء السرية. * يوجد أثر ذو دلالة احصائية أمن المعلومات بأبعاده الثلاثة وجودة الخدمات المصرفية. * لا توجد فروق ذات دلالة احصائية لمتوسطات جودة الخدمات المصرفية تعزى لمتغيرات (العمر ،المستوى التعليمي، الخبرة المهنية).
4	دراسة شيرين عبد الملك عبد القوى المخلافي 2018 ضمن المجلة العلمية للدراسات التجارية والبيئية	دور نظام أمن المعلومات في تطوير الخدمات المصرفية – دراسة ميدانية بالتطبيق على البنوك اليمنية)	* وجود علاقة ارتباط إحصائية بين أبعاد نظام أمن المعلومات (السرية والخصوصية والاعتمادية) وبين أبعاد تطوير الخدمات المصرفية في البنوك اليمنية (خدمة المعلومات الالكترونية، خدمة البطاقات الذكية، دعم الإدارة العليا) على مستوى الأبعاد مجتمعة.
5	دراسةSaddam Hossain Remus وSanzida Akter و Khaleda و Ferdous – المجلة الأوروبية لعلوم الحاسب وتكنولوجيا المعلومات 2023	تقييم مدى تطبيق أمن تكنولوجيا المعلومات والاتصالات في البنوك – دراسة حالة البنوك البنغلادية	تتبنى البنوك البنغلادية حلول تكتولوجيا المعلومات في عملها، كما أنها تستثمر في حلول أمن المعلومات بشكل كبير أيضاً لتحقيق الأهداف الأمنية اللازمة في القطاع الاقتصادي والمالي، ومع ذلك لازال هناك الكثير من العمل في الطريق الطويل لتحقيق متطليات ومعايير أمن المعلومات بحسب الهيئات الناظمة البنغلادية، مما يحتم ضرورة القيام بالعديد من الدراسات التي تهدف إلى تطوير فعالية أمن المعلومات بما يحمي البنوك البنغلادية.

6	دراسة ShivaDutt – Jangampeta المجلة التركية لتعليم الحاسب والرياضيات 2022	أمن البيانات المالية وبرنامج SIEM– حماية المعلومات المالية الحساسة في الأنظمة البنكية والمالية	إن تطبيق أدوات وميزات برنامج SIEM في شركات ومؤسسات القطاع المالي تساهم بشكل كبير في تحسين ضوابط وواقع أمن المعلومات فيها لجهة الدور الذي تلعبه في تحديد وتقييم الهجمات الأمنية المحتملة على المؤسسة المالية ووضع الإجراءات اللازمة للاستجابة لها وعلاجها وبالتالي حماية المعلومات الحساسة.
7	دراسة Federica Cugnasco جامعة تورينو إيطاليا – دراسة أعدت لنيل الماجستير في هندسة الحاسوب 2023	تحليل منصة مكافحة الاحتيال متعددة القنوات في العمليات المصرفية	يلعب برنامج SIEM دور هام كجزء في منصة مكافحة الاحتيال في البنوك كونه أداة مركزية لتجميع كل ملفات الأحداث logs للأنظمة التي تعالج البيانات في البنك وتحليلها بناءً على القواعد المبنية من فريق أمن المعلومات (correlation rules) ومن ثم توليد التنبيهات alerts للشحص المنشئ لهذه القواعد بناءً على نتائج التحليل والتي تنذر بحدوث حالة احتيال في البنك.
8	دراسة Achemlal, M., Gharout, S.، & Gaber, C., Pasguet M., , 2012 جامعة Urien P كان – فرنسا	التحديات الأمنية لبرنامج SIEM في خدمات نقل الأموال عبر الهواتف الجوالة	هناك الكثير من التحديات التي تواجه برنامج SIEM في كشف حالات الاحتيال وغسل الأموال في أنظمة الدفع ونقل الأموال عبر الموبايل، مثل السيناريوهات المعقدة التي يحتاج البرنامج لتحليلها، مرونة البرنامج في بناء قواعد متعددة البارمترات والوسائط وذلك من مصادر مختلفة للأحداث، قدرة البرنامج على كشف حالات الاحتيال في الوقت الحقيقي، قدرة البرنامج على التوسع في ظل توسع أنظمة الدفع والنقل عبر الموبايل، وأخيراً قدرة البرنامج على ربط أحداث صادرة من طبقات مختلفة منى الشبكة مثلاً من طبقتي Network و Application.

وعليه، فإن الإضافة العلمية للدراسة الحالية هي البحث عن أهم السيناريوهات الأمنية التي يحتاج فريق أمن المعلومات في المصارف لضبطها ومراقبتها وكشفها عن طريق برنامج SIEM، وذلك لما تتمتع به بيئة العمل المصرفية من طبيعة حساسة وخاصة في ظل وجود خدمات مصرفية متاحة للزبائن عبر تطبيقات الموبايل البنكي والإنترنت مثل فتح الحسابات أون لاين وتحويل الأموال والدفع الالكتروني وغيرها.

الفصل الثاني:

أمن المعلومات وأهمية تطبيقه في المؤسسات

1. المبحث الأول: مفهوم أمن المعلومات ومرتكزاته

1.1. تعريف المعلومات وأمن المعلومات:

المعلومات هي العلامات أو الإشارات أو النصوص أو الرسائل أو الأصوات أو الصور الثابتة أو المتحركة التي تحمل معنى قابل للإدراك ومرتبط بسياق محدد، في حين أن **أصول المعلومات** هي البيانات والمعلومات والبنية التحتية والبيئة المحيطة بها من تجهيزات أو برمجيات أو خدمات أو مستخدمين أو مرافق وغيرها.

وبالتالي فإن **أمن المعلومات** هو الوسائل والتدابير الخاصة بالحفاظ على سرية وتوافرية وسلامة المعلومات وحمايتها من الأنشطة غير المشروعة التي تستهدفها.[2]

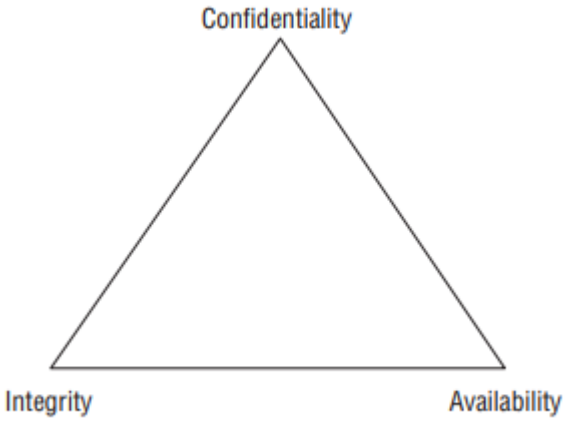
1.2. مرتكزات أمن المعلومات :

يقوم أمن المعلومات على مرتكزات ثلاثة وهي: سرية المعلومات Confidentiality، أصالة المعلومات Integrity وتوافرية المعلومات Availability. إن مرتكزات أمن المعلومات الثلاثة هذه تحدد البارامترات الأساسية التي تحتاجها أي مؤسسة لتحقيق بيئة آمنة، كما أنها تعرّف الأهداف والأغراض التي يجب تحقيقها من خلال تطبيق أمن معلومات فعال يخلق بيئة آمنة، حيث تُقاس كفاية الضوابط الناتجة عن عملية تقييم المخاطر ونقاط الضعف في بيئة البنك بمدى قدرتها على تغطية أو عنونة هذه المرتكزات الثلاثة، فين حين أن المخاطر ونقاط الضعف بحد ذاتها يتم تقييمها بناءً على مدى تعريضها هذه المرتكزات الثلاث للكشف أو الاختراق، يُشار إلى هذه المرتكزات الثلاثة باسم مثلث أمن المعلومات أو CIA Triad وهي:[3]

---

[2] السياسة الوطنية لأمن المعلومات، الجمهورية العربية السورية، الهيئة الوطنية لخدمات التقانة، ص3

[3] Chapple, M., Stewart, J. M., & Gibson, D. (2018). (ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide. John Wiley & Sons.



الشكل رقم (1) مثلث أمن المعلومات CIA Triad

- **سرية المعلومات Confidentiality:**

وهي أولى مرتكزات أمن المعلومات، تُعنى سرية المعلومات بضمان عدم قدرة أي أحد بالوصول والاطلاع على مصادر المعلومات باستثناء الأشخاص المخولين بذلك، من الهجمات التي تستهدف سرية المعلومات (التقاط المعلومات المُتبادلة عبر الشبكة – سرقة كلمات المرور – الهندسة الاجتماعية – التنصت وغيرها). إن خرق سرية المعلومات قد لا يكون ناتجاً فقط عن الهجمات المباشرة، بل قد يكون نتيجة خطأ بشري أو عدم كفاءة الشخص المسؤول عن إدارة المعلومات أو عدم كفاية الضوابط الرقابية اللازمة والسياسات الأمنية لحماية سرية المعلومات.

من الأحداث التي تؤدي إلى خرق سرية المعلومات نذكر (الإخفاق في تشفير المعلومات – إرسال فاكس أو بريد الكتروني إلى غير وجهته الصحيحة – ترك المستند المطبوع على الطابعة بحيث يكون متاحاً للجميع – وأيضاً مغادرة الحاسب الشخصي من دول إقفال الشاشة).

من الضوابط الأمنية المُستخدمة لحماية مرتكز سرية المعلومات نذكر (استخدام التشفير – ضبط صلاحيات الأشخاص بالوصول لأصول المعلومات – استخدام تقنيات التعمية لإخفاء المعلومات السرية ضمن المعلومات العادية الغير سرية).

- **أصالة المعلومات Integrity:**

وهي ثاني مرتكزات أمن المعلومات، تُعنى أصالة المعلومات بحماية صحة ووثوقية المعلومات عن طريق منع التعديل الغير المخول لها الذي يستهدفها من قبل أشخاص غير مخولين سواءً بشكل عرضي أو مقصود وأيضاً من قبل البرامج الخبيثة مثل الفيروسات وغيرها، وبالمقابل فهو يعمل على

منح صلاحية التعديل للأشخاص المخولين فقط، وبذلك فإنه يضمن أن تبقى المعلومات صحيحة، موثوقة، دقيقة، ومحفوظة بشكل جيد.

من الهجمات التي تستهدف أصالة المعلومات (الفيروسات والبرامج الخبيثة – الوصول غير المخول للمعلومات – الأخطاء في برمجة التطبيقات – التعديل الخبيث المقصود على البيانات وغيرها). إن خرق أصالة المعلومات كما في ورد معنا في سريتها قد لا يكون ناتجاً فقط عن الهجمات المقصودة، بل قد يكون نتيجة خطأ بشري أو عدم كفاءة مهارات وقدرات الشخص المسؤول عن إدارة المعلومات أو عدم كفاية الضوابط الرقابية اللازمة والسياسات الأمنية لحماية أصالة المعلومات.

من الأحداث التي تؤدي إلى خرق أصالة المعلومات نذكر (حذف ملفات – إدخال معلومات غير صحيحة – تغيير إعدادت نظام – أخطاء في إدخال الأوامر على محرر الأوامر – تفشي برنامج خبيث مثل حصان طروادة Trojan Horse على الشبكة).

من الضوابط الأمنية المُستخدمة لحماية مرتكز أصالة المعلومات نذكر (ضبط الوصول لأصول المعلومات – ضبط صلاحيات الأشخاص بالتعديل على المعلومات – تفعيل خاصية تقفي الأثر Audit Trail لمراقبة التعديلات المنفذة على المعلومات وعدم الإنكار – استخدام تقنيات hashing للتأكد من سلامة البيانات من التعديل – التدريب المناسب للأشخاص المخولين بالتعديل على المعلومات).

- **توافرية المعلومات Availability:**

وهي ثالث مرتكزات أمن المعلومات والتي تُعنى بضمان إتاحة الوصول لأصول المعلومات من قبل الأشخاص المخولين في الوقت الحقيقي ومن دون مقاطعة، وبأن البنية التحتية في المؤسسة التي تتضمن الاتصالات والخدمات وغيرها تعمل وظيفياً بشكل سليم مما يسمح للموظفين المخولين بالوصول لمصادر المعلومات.

من الهجمات التي تستهدف توافرية المعلومات (فشل الأجهزة والأنظمة – أخطاء البرمجيات والتطبيقات – العوامل الطبيعية والبيئية مثل الفيضانات والبراكين وغيرها – هجمات الحرمان من الخدمة DoS – قطع الاتصالات وغيرها)، إن خرق توافرية المعلومات كما في ورد معنا في سريتها وأصالتها قد لا يكون ناتجاً فقط عن الهجمات المقصودة، بل قد يكون نتيجة خطأ بشري أو عدم كفاءة مهارات وقدرات الشخص المسؤول عن إدارة المعلومات أو عدم كفاية الضوابط الرقابية اللازمة والسياسات الأمنية لحماية توافرية المعلومات.

من الأحداث التي تؤدي إلى خرق توافرية المعلومات نذكر (حذف ملفات – استخدام عتاد برمجي أو صلب بشكل مبالغ فيه مما يؤدي إلى تعطله – تعطل مصدر التغذية الكهربائية وغيرها).
من الضوابط الأمنية المُستخدمة لحماية مرتكز توافرية المعلومات نذكر (مراقبة أداء الشبكة والمنظومة المعلوماتية – استخدام جدران النار Firewalls للحماية من هجمات الحرمان من الخدمة DoS – تطبيق مبدأ النظام الموازي Redundant System للأنظمة الحرجة في المؤسسة – التأكد من سلامة النسخ الاحتياطية المأخوذة بشكل دوري).

1.3. أهمية وهدف أمن المعلومات في المؤسسات:

يهدف تطبيق أمن معلومات فعال في أي مؤسسة إلى حماية مرتكزات أصول المعلومات فيها عن طريق إجراء عملية مستمرة لتقييم المخاطر التي تهدد هذه الأصول كما يلي:

- ✓ تحديد التهديدات التي تتعرض لها أصول المعلومات في المؤسسة والتي يمكن أن تؤثر على أحد مرتكزات أمن المعلومات وعلى استمرارية العمل في المؤسسة.
- ✓ تقييم المخاطر الناجمة عن هذه التهديدات وتصنيف درجة خطورتها على مقياس (عالية–متوسطة–منخفضة) وذلك بناءً على أثرها الفعلي واحتمال تكرارها.
- ✓ وضع خطة تتضمن الإجراءات والضوابط العلاجية والتصحيحة والوقائية لمعالجة هذه المخاطر.
- ✓ قياس مدى كفاية الضوابط والإجراءات المحدّدة في الخطة العلاجية في تخفيف المخاطر وذلك بعد تطبيقها على أرض الواقع، ليُصار إلى إعادة تقييم فعّاليتها بناءً على التغييرات الحاصلة في المؤسسة في بنيتها التحتية ومنظومتها المعلوماتية ونشاطها.

وبالتالي تتجلى أهمية تطبيق خطة أمن معلومات فعالة في ضمان عمل كافة نشاطات المؤسسة الداخلية والخارجية بشكل آمن ومستمر وموثوق وبما يتماشى مع أهداف المؤسسة الاستراتيجية ورؤيتها ومهمتها.

2. المبحث الثاني: التعريف بمهام ودور فريق أمن المعلومات في المصارف

2.1. الغاية والهدف من وجود فريق أمن المعلومات في المصرف:

يتلخص الهدف الأساسي من وجود وحدة وفريق أمن المعلومات في المصارف هو المساهمة في تطوير منظومة عمل أمن وخصوصية المعلومات في المصرف بما يضمن حماية أصول معلوماته، بالإضافة لعملية التقييم المستمر للمخاطر الناجمة عن وجود خلل ونقاط ضعف في الأنظمة والعمليات التي تعالج معلوماته والإبلاغ عنها مشفوعةً بالتوصيات اللازمة للإجراءات العلاجية التصحيحية لمجلس إدارة البنك والإدارة العليا والجهات ذات العلاقة فيه، ويقصد هنا بنطاق معلومات البنك هو كافة الأشكال الالكترونية والمطبوعة وأي تنسيقات أخرى للبيانات وآليات التعامل معها وعلاجها وتخزينها.

2.2. المهام والواجبات المُسندة إلى فريق أمن المعلومات في المصرف:

يُسند إلى فريق أمن المعلومات مجموعة من المهام والواجبات، نذكر أهمها:

1. المشاركة في إعداد وتحديث سياسات وإجراءات أمن تكنولوجيا المعلومات، الاتصالات، العمليات والإجراءات، بما يتناسب مع أهداف واستراتيجيات ورؤية البنك.
2. مراقبة أنشطة المصرف وجمع المعلومات اللازمة لتحديد المخاطر المرتبطة بتكنولوجيا المعلومات وأمنها.
3. تقييم مخاطر أمن المعلومات في المصرف وتقديم الرأي بخصوصها للتخفيف منها، إدارتها واقتراح التعديلات والتطوير.
4. مراقبة الالتزام بسياسة وإجراءات أمن المعلومات والتقرير عن حالات المخالفات لمجلس إدارة البنك والإدارة العليا.
5. المشاركة في تطوير خطة استمرارية الأعمال، واختبارها.
6. نشر الوعي وثقافة أمن المعلومات في المؤسسة وبين الموظفين عن طريق الدورات التدريبية وبطاقات التوعية.
7. المشاركة في وضع الضوابط والصلاحيات للموظفين للوصول إلى المعلومات.
8. تقييم أنظمة حماية وتشفير البيانات ومعالجة الثغرات واقتراح تطويرها.

9. المشاركة في وضع الخطط الأمنية المناسبة للبنك، بما في ذلك اختبارات الاختراق ونقاط الضعف الداخلية والخارجية التي يجب أن تتم بصورة دورية.
10. المشاركة في إعداد وتطوير الاتفاقيات المتعلقة بأمن المعلومات وعدم الإفصاح (NDA Non-Disclosure Agreement) والتي يتم توقيعها مع كافة الجهات التي يتم التعاقد معها سواء كانت خارجية أو داخلية (موظفين، موردي خدمات، موردي أنظمة، الخ...).
11. إعداد تقرير دوري عن واقع أمن المعلومات في البنك ورفعه لمجلس إدارة البنك.
12. أي مهام أخرى ذات علاقة بمراقبة ومتابعة وتحسين أمن المعلومات يتم تكليفه بها من قبل مجلس إدارة البنك وإدارته العليا.

2.3. القرارات والتشريعات التي تحدد مهام أمن المعلومات في المصارف العاملة في سورية:

نورد فيما يلي أهم القرارات والتشريعات الصادرة عن الجهات الإشرافية والوصائية في الجمهورية العربية السورية والتي تتناول دور أمن المعلومات والواجبات والمهام الموكلة إليه:

ر.ت	القرار	الجهة	دور أمن المعلومات
1	القرار رقم 71 / م ن تاريخ 2018/6/4 (المعايير المطلوب توفرها بالبنية التقنية لدى المصارف العاملة في الجمهورية العربية السورية)	مصرف سورية المركزي	* إدارة وضبط التحكم بالوصول للتطبيقات والأنظمة في البنك (منح الموافقات على طلبات الوصول والصلاحيات وتعديلاتها وحذفها). * فرض تطبيق سياسة كلمات المرور في البنك (تحديد معايير كلمات المرور القوية – إجبار التغييرات الدورية عليها – تشفير كلمات المرور). * فرض تطبيق سياسة التشفير المعتمدة في البنك(اعتماد تقنيات التشفير عند نقل المعلومات الحساسة عبر الشبكات التشاركية لضمان سريتها – تأمين حماية البيانات وتشفيرها عند حفظها أو نقلها – إدارة وحماية مفاتيح التشفير (مفاتيح عامة و خاصة و مشتركة) والشهادات الرقمية وتخزينها).

			* حماية الهواتف المحمولة والأجهزة المتنقلة. * إدارة أصول المعلومات في البنك (ملكيتها – مخزونها – تصنيفها – نقلها). * أمن الموارد البشرية (الأدوار والمسؤوليات والتحري عن المرشحين للتوظيف – الإجراءات الجزائية وإجراءات إنهاء الخدمات بحيث تغطي إرجاع الأصول وإلغاء الصلاحيات الممنوحة – التوعية والتدريب فيما يتعلق بأمن المعلومات – الأحكام والشروط عند التوظيف). * الأمن الفيزيائي والبيئي (حماية نقاط الدخول الفيزيائية – حماية المكاتب والمرافق والكابلات وغرف البيانات – إتلاف المعدات بطريقة آمنة). * الحماية من البرمجيات الخبيثة (التأكد من تنصيب وتحديث وضبط برامج الحماية من البرمجيات الخبيثة). * التأكد من النسخ الاحتياطي للبيانات. * إدارة وأمن الشبكات (مراقبة المعدات الشبكية – حماية وتشفير المعلومات التي تمر عبر الشبكات). * الرقابة وسجلات الضبط (حماية سجلات الضبط – ضبط الوصول إليها – تسجيل الأحداث والأخطاء ومراجعة سجلات الضبط). * المشاركة في وضع خطة استمرارية الأعمال بالتنسيق مع المخاطر التشغيلية. * حماية البنية التحتية للبنك (وجود إجراء للمراجعة الدورية لاعدادات التجهيزات الشبكية – وجود سجلات وتقارير للتجهيزات الشبكية الأمنية).

2	القرار رقم 15 م ن تاريخ 2024/1/31 (إجراءات إدارة الأمن السيبراني[4] في المؤسسات المالية المصرفية وغير المصرفية)	مصرف سورية المركزي	* الإشراف المباشر على سياسة وبرنامج الأمن السيبراني ومتابعة تنفيذهما وتحديثهما في البنك. * تقييم مدى كفاءة وكفاية سياسة وبرنامج الأمن السيبراني * قياس مدى فعالية ضوابط وتعليمات الحماية المحددة في سياسة الأمن السيبراني في البنك بصورة مستمرة. * تحديد وتحليل وتقييم المخاطر السيبرانية باستخدام نماذج عالمية مثل COBIT، FAIR, COSO.... * إعداد وعرض تقارير ربع سنوية لمجلس إدارة البنك حول الأمن السيبراني وسياسته وبرنامجه ومدى كفايته وكفاءته وعن الانحرافات في تطبيق السياسة والإجراءات ونتائج تقييم المخاطر السيبرانية مشفوعة بالتوصيات والمقترحات الواجب تنفيذها مع عرض ملخص حول أهم الأحداث والتهديدات والاختراقات التي تعرضت لها البنك خلال فترة التقرير.
3	السياسة الوطنية لأمن المعلومات واللوائح التنظيمية الخاصة بها تاريخ 2014/10/12	وزارة الاتصالات والتقانة (الهيئة الوطنية لخدمات الشبكة) وحالياً تسمى	* تحديد وتنفيذ خطة وسياسة أو سياسات أمن المعلومات في البنك (التحكم بالنفاذ – أمن الموارد البشرية – أمن الشبكات – الأمن الفيزيائي – الحماية من البرامج الخبيثة – استخدام التشفير...). * إجراء عملية تقييم دورية للمخاطر والتهديدات الداخلية والخارجية التي تهدد البنك. * إعداد تقارير عن حسن الالتزام للإدارة العليا مع

[4] مجموعة من الأدوات والسياسات ومفاهيم الأمان وإجراءات ضمانها وتعليماته وإجراءات إدارة المخاطر والتهديدات والأدوات والتقنيات التي يمكن استخدامها لحماية أصول معلومات المؤسسة الالكترونية والمادية والبرمجيات والخدمات وقواعد البيانات والبنى التحتية من التهديدات الداخلية والخارجية.

		الهيئة الوطنية لخدمات التقانة وتتبع لرئاسة مجلس الوزراء	المدد الزمنية للتنفيذ. * تحديد آلية واضحة لإبلاغ المعنيين داخل وخارج البنك بأي حدث أو انتهاك يخص أمن المعلومات.

الفصل الثالث:

برنامج SIEM (Security Information and Event Management)
وميزاته وأهميته في تعزيز دور أمن المعلومات في المصارف

1. المبحث الأول: التعريف بنظام (Security Information and Event Management) SIEM

1.1. التعريف بالبرنامج ونشأته التاريخية:

تم طرح مصطلح نظام SIEM لأول مرة من قبل شركة Gartner عام 2005 وهي شركة تقدم خدمات واستشارات في مجال تكنولوجيا المعلومات والاتصالات، حيث جاء هذا المصطلح ليستبدل نوعين من الأنظمة:

- SIM (Security Information Management): يقوم بإدارة سجلات logs التي يجمعها من عدد من المصادر في المنظومة المعلوماتية والبنية التحتية للمؤسسة مثل التجهيزات الشبكية والمخدمات وقواعد البيانات وغيرها ويولد تقارير بالمعلومات الموجودة فيها، وهو بذلك يدير عملية تخزين هذه المعلومات وتحليلها.
- SEM (Security Event Management): يقوم بتحليل وإدارة الأحداث events والحوادث incidents في الزمن الحقيقي.

وبالتالي يمكن تقسيم مراحل عمل البرنامج إلى خمس خطوات رئيسية هي[5]:

1. جمع البيانات من عدة مصادر في المنظومة المعلوماتية والبنية التحتية (مخدمات–موجهات–مبدلات–جدران نار–قواعد بيانات وغيرها).
2. معالجة البيانات المُجمعة، فحيث أن هذه البيانات قادمة من مصادر عديدة ومختلفة عن بعضها البعض من حيث الصيغة مما يجعل عملية مقارنتها صعبة، فلا بد من إجراء عملية المعالجة اللازمة والتي تسمى normalization حيث تقوم بترجمة أي تحويل صيغ كل البيانات المُجمعة إلى صيغة واحدة مما يسهل عملية إدارتها وتحليلها.
3. تجميع البيانات المُعالجة في الخطوة السابقة واستخراج المعلومات منها.
4. ربط المعلومات المستخرجة ببعضها عن طريق استخدام قواعد الارتباط correlation rules المبنية مسبقاً من قبل فريق أمن المعلومات وذلك لغرض لاكتشاف وتقييم المخاطر.

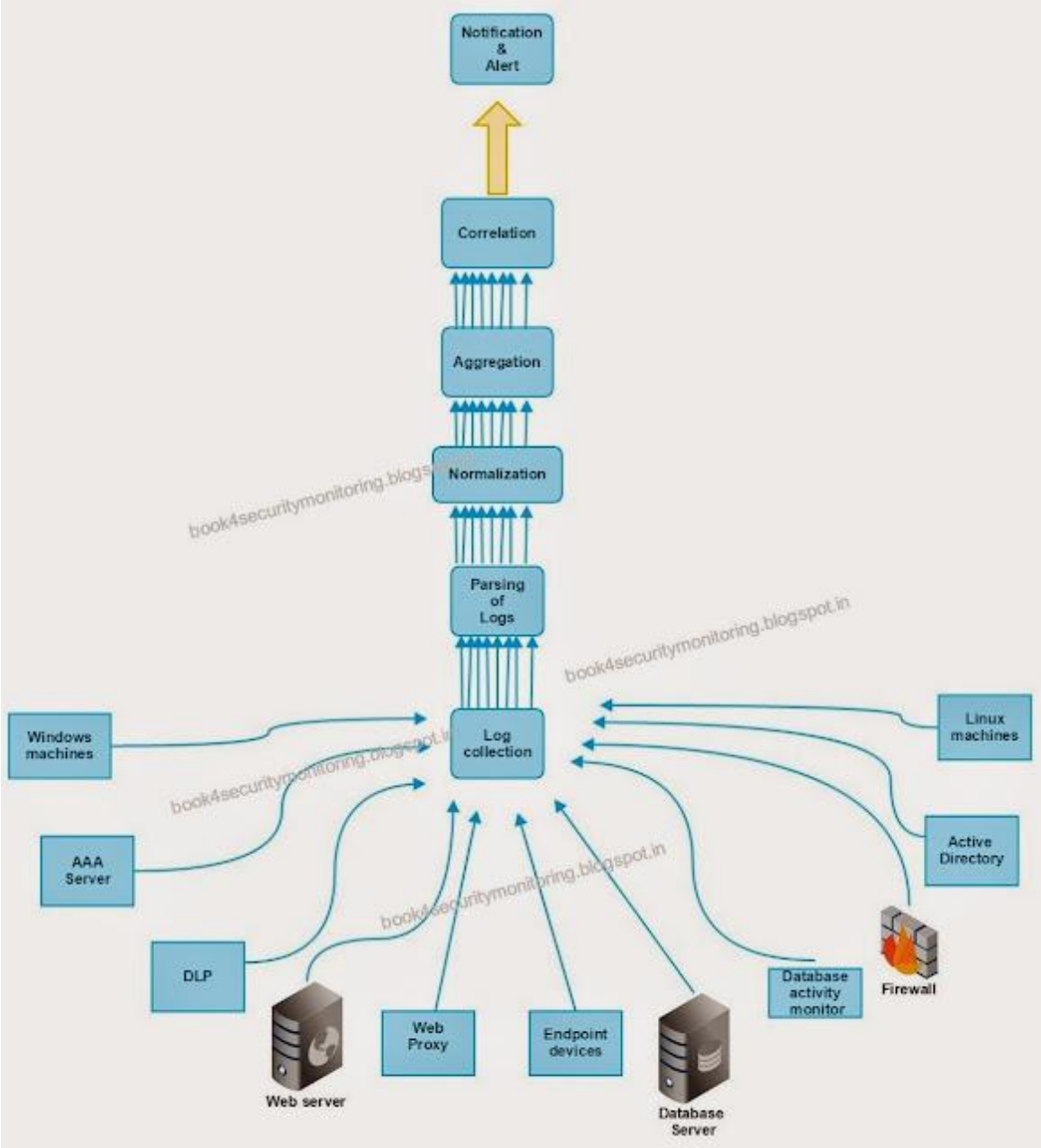
[5] Gaber, C., Gharout, S., Achemlal, M., Pasquet, M., & Urien, P. (2012). Security challenges for security information and event management systems in mobile money transfer services.

5. توليد التنبيهات الناتجة عن التقييم في الخطوة السابقة لفريق أمن المعلومات واتخاذ الإجراءات العلاجية اللازمة.

1.2. هيكلية بناء أو هندسة النظام SIEM Architecture:

يتألف التصميم الهندسي للبرنامج من مجموعة من المكونات أو الوحدات الأساسية المتكاملة مع بعضها البعض[6] وهي كما تظهر في الشكل أدناه:

[6] Chikonga, M. (2014). *Exploring the applicability of SIEM technology in IT security* (Doctoral dissertation, Auckland University of Technology).



الشكل رقم (2) هيكلية نظام SIEM

1. وحدة تجميع ملفات سجلات الأحداث logs من مصادر البيانات:

من دون هذه الوحدة لن يكون هناك قيمة وفائدة لعمل SIEM، حيث أن أول خطوة في عملية تطوير البرنامج هي تحديد المصادر التي ستقوم بإرسال ملفات logs له وهي متنوعة ومختلفة بحسب طبيعة عمل المؤسسة وماتحتويه في منظومتها المعلوماتية من تجهيزات شبكية ومخدمات وقواعد بيانات وجدران نار وغيرها، إن أغلب الشركات المصنعة للتجهيزات

والأنظمة والتطبيقات في أيامنا هذه تُطبق في تصنيعها إمكانية توليد هذه الأنظمة والتجهيزات لملفات logs، تختلف طرق جمع البرنامج لملفات logs من مصادرها بين طريقة السحب pull أو طريقة الدفع push، فبينما في طريقة السحب تقوم وحدة تجميع الأحداث في البرنامج بسحب الملفات من مصادرها، تقوم طريقة الدفع بطلب إرسال هذه الملفات للبرنامج من مصادرها.

أيضاً يرتبط مصطلحي "جمع ملفات الأحداث مع وجود وكيل Agent-based log collection" و "جمع ملفات الأحداث من دون وجود وكيل Agent-less based log collection" بمفهوم تجميع ملفات الأحداث في البرنامج، فبطريقة من دون وجود وكيل ليس هناك حاجة لتنصيب برمجية على الجهاز أو النظام المصدر لملفات logs وفي هذه الحالة فإن وحدة تجميع ملفات الأحداث logs تقوم إما بسحبها من مصادرها أو تقوم المصادر من تلقاء نفسها بدفعها وإرسالها إلى الوحدة، بينما في طريقة مع وجود وكيل لا بد من تنصيب برمجية على الجهاز أو النظام المصدر حيث يقوم الوكيل بتجميع الملفات وإعادة توجيهها نحو SIEM في الزمن الحقيقي أو أقرب مايمكن للزمن الحقيقي.

2. **وحدة الفلترة Filtering:**

توصف الفلترة بأنها عملية استبعاد بعض البيانات الموجودة في ملفات logs من عمليات التحليل والصياغة في تقارير والتخزين وغيرها، وذلك لأن صفات أو ميزات هذه البيانات تشير إلى أنها غالباً لا تحوي معلومات هامة أو مفيدة، حيث أنه كلما ازداد عدد الأجهزة التي تقوم بإرسال ملفات logs للبرنامج كلما ازداد بالمقابل حجم هذه الملفات لأن أغلب مصادر البيانات قد تم ضبطها لتقوم بإرسال كل ملفات logs التي تتولد عنها لوحدة التجميع في النظام سواءً كانت هذه الملفات ذات صلة بسياق الأحداث والثغرات الأمنية المطلوب من البرنامج اكتشافها أم لم تكن، مما يزيد من طول الوقت اللازم لتحليلها.

وبالتالي فإن عملية الفلترة أو استبعاد البيانات هنا تقوم بعلاج هذا العبء وضمان عدم ضياع البيانات الهامة بسبب خلطها مع غيرها من البيانات الغير الهامة، وذلك عن طريق استخلاص البيانات المهمة ذات الصلة واستبعاد تلك الغير ذات صلة.

3. **وحدة التطبيع Normalization:**

إن صيغ الأحداث التي تتولد عن مختلف المصادر في البنية التحتية تختلف فيما بينها بسبب عدم توحيد صيغ الأحداث بين التطبيقات والأجهزة من قبل الشركات المصنعة لها، وإن غياب هذا التوحيد في الصيغ يقود إلى تحديات في عمليات التحليل والربط بينها، وبالتالي فإن الغرض الأساسي من عملية تطبيع ملفات الأحداث هو تحويلها إلى صيغة عامة مشتركة وبذلك فهو يمكّن إجراء عملية مقارنتها وتحليلها والربط بينها وتوليد التقارير.

من الأمثلة عن البيانات التي تخضع لعملية التطبيع حقول (التاريخ–الوقت–عنوان IP–اسم المستخدم–أرقام المنافذ). كما يجب أن تتم عملية التطبيع بوسائل وطرق وتقنيات لا تنتهك فيها مرتكز أصالة البيانات ودقتها وصحتها.

4. **وحدة القواعد Rules:**

صُممت القواعد في برنامج SIEM للتمييز مابين الأحداث العادية التي تحدث ضمن منظومة المؤسسة مثل (تسجيل دخول ناجح لاسم مستخدم)، وبين الأحداث الغير العادية التي تدل على وجود خلل أمني أو اشتباه في انتهاك أحد مرتكزات أمن المعلومات في منظومة المؤسسة مثل (فشل تسجيل دخول للمحاولة الخامسة في دقيقة واحدة لأحد الحسابات ذات الصلاحيات العالية كحساب root في نظام Linux مما قد يدل على وجود محاولة اختراق لهذا الحساب)، وذلك عندما تتطابق قيم الحقول المرتبطة بهذه الأحداث مع قواعد مصممة ومعرفة مسبقاً على النظام. تكون بعض هذه القواعد مبنية بشكل ضمني مع البرنامج وبعضها الآخر يقوم فريق أمن المعلومات بتعريفها وتصميمها بما يناسب تطبيق سياسة أمن المعلومات في المؤسسة وضمان الامتثال لها.

تتجه برامج SIEM الحديثة الآن نحو استخدام أدوات الذكاء الصنعي في جعل هذه القواعد أكثر مرونة وصلادة (robust) في اكتشاف أي سلوك مثير للريبة في المنظومة.

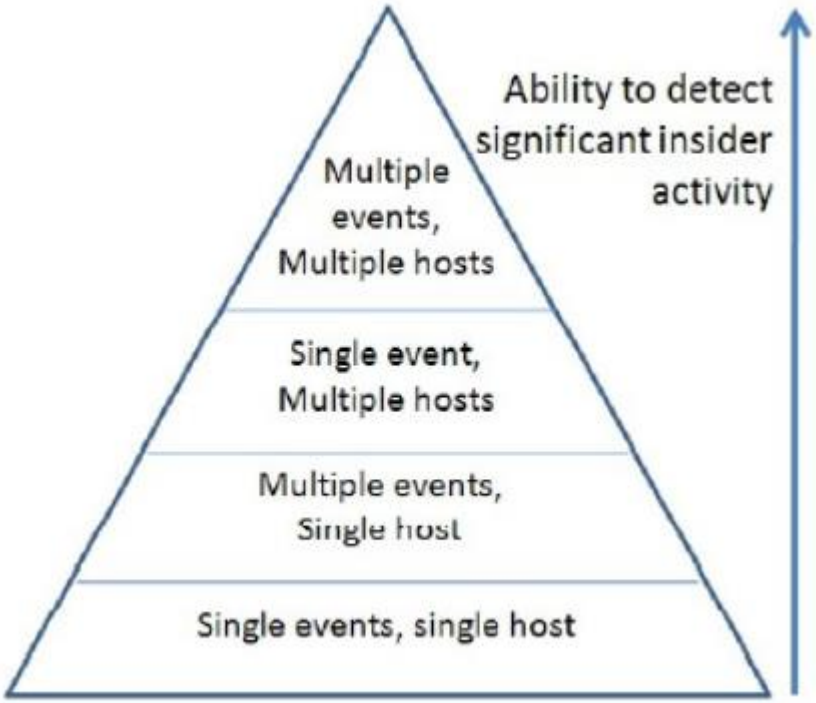
5. **وحدة إغناء البيانات وتسييقها Data Enrichment and Contextualization:**

يهدف وجود هذه الوحدة إلى تزويد بيانات ملفات الأحداث التي تم جمعها من المصادر بسياق يُمكِّن من القيام بعملية تحليل أغنى ورؤية الصورة الشاملة والأكبر عند التحقيق في حادث ما، وذلك عن طريق تأمين أحداث أخرى ذات صلة بها تحوي معلومات إضافية مفيدة لعملية التحليل مثل: (نجاح عملية تسجيل الدخول لمخدم أو نظام ما من عنوان معين

وذلك بعدة عدة عمليات حجب له عن الدخول من قبل جدار النار)، حيث أن الأحداث بشكلها العام لا تحوي سياق بشكل افتراضي مما قد ينتج عن ذلك ضعف في عملية ترجمة وتفسير الحدث وجعله غير مفهوم أو إسناد عدة ترجمات أو تفسيرات للحدث نفسه.

6. وحدة ارتباط الأحداث Event Correlation:

لعلّ مفهوم الارتباط هو واحد من أهم الإمكانيات التي يقدمها برنامج SIEM، حيث أن الارتباط بين الأحداث الواردة من عدة مصادر في المنظومة المعلوماتية للمؤسسة ودراسة العلاقات فيما بينها يمكّن المؤسسة من اكتشاف مصادر التهديدات والهجمات الأمنية المحتملة عليها وتوليد التنبيهات اللازمة لفريق أمن المعلومات والتي لن يكون من الممكن اكتشافها من دون وجود هذا الارتباط وفي حال الأخذ بعين الاعتبار الأحداث الواردة من مصدر واحد فقط. يبين الشكل أدناه كيف تزداد إمكانية البرنامج على اكتشاف الثغرات والهجمات ونقاط الضعف كلما زادت قدرته على ربط الأحداث الواردة من مصادر متعددة.



الشكل رقم (3) الارتباط بين الأحداث

يحتاج تطبيق الارتباط في SIEM إلى فهم عميق لبنية الشبكة والمنظومة والأحداث التي تتولد عنها وإلى فهم العلاقات المؤقتة والسببية بين الأحداث، حيث يتم تطبيق الارتباط على حقول وعناصر البيانات التي جرى مسبقاً تطبيعها ومعالجتها في مراحل سابقة.

هناك عدة طرق لتحقيق الارتباط بين الأحداث ولعل أكثرها استخداماً هو الارتباط بناءً على القواعد Rule based correlation، ولكن هناك طرق أخرى نذكر منها (Model based correlation–Finite state machine based correlation–Graph based correlation–Codebook based correlation–Case based reasoning correlation) ولكل طريقة منها ميزاتها وجوانب قصورها، وإن اختيار طريقة ما دوناً عن غيرها يعتمد بشكل أساسي على طبيعة وخصوصية المنظومة المعلوماتية والبنية التحتية للمؤسسة.

7. **وحدة تجميع الأحداث Event Aggregation:**

تشير عملية تجميع الأحداث إلى توحيد وتدعيم الأحداث التي حدثت ضمن مجال زمني واحد إلى حدث واحد مما يحسن من أداء النظام.

8. **وحدة تخزين ملفات الأحداث Log Storage:**

إن تحديد فترة تخزين ملفات الأحداث logs وسياسات الاحتفاظ الخاصة بها ضمن المؤسسة يتبع لمتطلبات التدقيق والالتزام ضمن المؤسسة وبما يمتثل للتشريعات والقرارات الصادرة عن الجهات الإشرافية والوصائية، لطالما كان تخزين ملفات logs يعتمد بشكل أساسي على صيغ مختلفة من الملفات مثل الملفات النصية أو الثنائية أو المضغوطة وخصوصاً صيغ الملفات النصية التي كانت تستخدم في أنظمة إدارة ملفات الأحداث log management، لكن أنظمة SIEM في وقتنا الحالي تستخدم قواعد البيانات لتخزين ملفات الأحداث مثل Oracle و Microsoft SQL و My SQL.

1.3. ميزات البرنامج الفنية:

يمتلك نظام SIEM مجموعة من الميزات الفنية والوظائف الأساسية التي يجب على المؤسسة وفي حالة هذا البحث (البنك) التأكد منها قبل قيامها بعملية شراء المنتج وهي[7]:

1. **قواعد الارتباط Correlation Rules:**

يعتمد نجاح برنامج SIEM في قدرته على اكتشاف الأحداث بناءً على قواعد الارتباط، وفي ظل امتلاك أغلب برامج SIEM لقواعد ارتباط أساسية فإن القليل منها فقط يمتلك إمكانيات بحث قوية ومرنة وتدعم اللغات المُستخدمة لكتابة أوامر بحث معقدة لاستخدامها في البحث ضمن بيانات البرنامج.

2. **مصادر البيانات Data Sources:**

واحد من أهم الميزات الأساسية في برنامج SIEM هو قدرته على جمع البيانات من مختلف مصادرها في البنية التحتية للبنك أو أي مؤسسة على اختلاف الشركات المصنعة وأنظمة التشغيل وأنواع قواعد البيانات وغيرها.

3. **المعالجة في الزمن الحقيقي Real Time Processing:**

تأخذ هذه الميزة بعين الاعتبار قدرة البرنامج على معالجة البيانات في الزمن الحقيقي، فنقيم هنا قدرته على القيام بعمليات المراقبة وتحليل الملايين من الأحداث والاكتشاف في الزمن الحقيقي لما له من دور هام في اكتشاف الهجمات والحوادث السيبرانية من دون هامش تأخير.

4. **حجم البيانات Data volume:**

إن تحليل الأحجام الكبيرة من البيانات القادمة من مصادر مختلفة هو أمر ضروري جداً لتحقيق مراقبة أفضل للبنية التحتية، ولكن الاحتفاظ بهذه الأحجام الكبيرة من البيانات المُجمعة في البرنامج هو غالباً مكلف جداً وغير عملي وهو يتبع لسياسة الاحتفاظ المُطبقة في المؤسسة (البنك)، وبالتالي فإن هذه الميزة تقيم قدرة البرنامج على التعامل مع أحجام كبيرة من البيانات وتخزينها من دون أخطاء أو مشاكل.

---

[7] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759.

5. **العرض Visualization:**

إن واحداً من أهم العوامل الأساسية التي تعيق عملية تحليل الأحداث الأمنية هو وجود قصور في الطرق المناسبة لعرض البيانات المُجمعة وإظهارها وتصفحها بطريقة تفاعلية، ولذلك فإنه من المهم جداً التأكد من قدرة النظام على منح مستخدميه إمكانية خلق طرق عرض جديدة للبيانات ولوحة قيادة Dashboard مرنة.

6. **تحليل البيانات Data Analysis:**

تدعم النسخ الحديثة من نظام SIEM إمكانية التكامل مع أدوات تحليل سلوك المستخدمين (الموظفين) والأطراف الثالثة التي تتعامل مع المؤسسة وذلك بالاعتماد على أدوات الذكاء الصنعي وتعلّم الآلة.

7. **الأداء Performance:**

تقيم هذه الميزة أداء نظام SIEM من حيث قدرته الحسابية وتخزين البيانات ومعالجتها وقواعد الارتباط، بالإضافة لإمكانيات البحث في البيانات والفهرسة والمراقبة.

8. **التحليلات الجنائية Forensics:**

بالإضافة لميزة معالجة الأحداث تقدم بعض أنظمة SIEM شبكة مبنية ضمنياً بداخلها تستطيع التقاط كافة الرزم packets المتبادلة ضمن الجلسة المفتوحة التي يشتبه بها على أنها تحوي مكونات خبيثة مثل فيروسات أو كود خبيث.

9. **التعقيد Complexity:**

من المتعارف عليه في مجال أمن المعلومات أن أنظمة SIEM هي أنظمة معقدة ويصعب إدارتها، ولذلك من المهم جداً اختبار مدى إمكانية تنصيب وإدارة البرنامج في مرحلة اختباره بجهد مقبول وعادي وذلك قبل أخذ قرار الشراء.

10. **إمكانية التوسع Scalability:**

وهي قدرة البرنامج على التوسع في المستقبل ليس فقط من ناحية التجهيزات والعتاد الصلب، بل أيضاً بعدد الأحداث الأمنية التي يستطيع جمعها ومعالجتها وتحليلها وذلك في ظل التحول الرقمي الجديد الذي يؤدي إلى إضافة المزيد من التجهيزات والمخدمات وقواعد البيانات وغيرها إلى نطاق عمل النظام.

11. تحليل المخاطر Risk Analysis:

تقيّم هذه الميزة قدرة برنامج SIEM على القيام بعملية تحليل مخاطر للأصول المرتبطة به أم يحتاج البنك أو المؤسسة إلى تطبيق نظام خارجي ليقوم بهذه المهمة، علماً أن أغلب أنظمة SIEM الحديثة توفر هذه الميزة.

12. التخزين Storage:

على اعتبار أن نظام SIEM يخزن المعلومات لمدة 90 يوم فقط بشكل افتراضي، تقيّم هذه الميزة طول الفترة التي يخزن فيها البرنامج البيانات لغايات المعالجة والتحقيق الجنائي الرقمي.

13. المرونة Resilience:

المرونة أو التسامح بالأخطاء هي ميزة هامة جداً لأي نظام مراقبة حرج، فمن الضروري جداً فهم وتقييم إمكانيات التسامح مع الأخطاء الموجودة في النظام، على سبيل المثال (هل يوفر البرنامج إتاحية عالية في قدرته على جمع البيانات من مصادرها؟ (High Availability) كأن يكون هناك اتصال بديل بين مصادر البيانات وSIEM في حال تعرض الاتصال الأساسي لخلل ما–هل بالإمكان استعادة الأحداث المحذوفة من قاعدة بيانات البرنامج في حال تم حذفها بشكل عرضي أو مقصود؟).

14. تحليل سلوك المستخدمين UEBA User and Entity Behavior Analysis:

تقّيم هذه الميزة وجود وحدة خاصة بتحليل سلوك المستخدمين والتطبيقات والأجهزة عن طريق أدوات الذكاء الصنعي وتعلم الآلة في نظام SIEM، أم في حال عدم وجودها فهل يدعم نظام SIEM إمكانية تكامله مع حلول وبرامج وأدوات أخرى تقوم بذلك؟. حيث يهدف تحليل السلوك هذا إلى كشف أي خروقات يقوم بها المستخدم أو التطبيق عن سلوكه المُعتاد والذي يكون فيه ملتزماً فيه بسياسة المؤسسة الأمنية مثل (كشف تسريب البيانات عن طريق لحظ تدفق غير عادي للبيانات من داخل شبكة المؤسسة إلى خارجها أو استخدام كثيف وغير عادي للإنترنت من قبل مستخدم أو تطبيق ما).

15. الأمن Security:

تقيّم هذه الميزة قدرة البرنامج على تطبيق تقنيات التشفير للبيانات المتبادلة بين الوحدات المكونة له أثناء عمليات التجميع والتحليل وغيرها.

2. المبحث الثاني: دور نظام SIEM في تعزيز دور أمن المعلومات في المصارف

2.1. التحديات التي يواجهها فريق أمن المعلومات في المصارف لتأدية مهامه:

نستعرض فيما يلي أدناه أهم التحديات التي تواجه فريق أمن المعلومات في المصرف لتأدية المهام والواجبات المُسندة إليه من دون وجود برنامج مركزي لتجميع الأحداث مثل SIEM:

- ضرورة وجود عملية مراقبة مستمرة وفي الزمن الحقيقي أو مع هامش تأخير مقبول من قبل فريق أمن المعلومات لمنظومة البنك المعلوماتية وبنيته التحتية للكشف عن التهديدات والثغرات المحتملة والقائمة.
- إن حجم بيانات الأحداث وسجلات logs التي تولدها التجهيزات والأنظمة وقواعد البيانات وغيرها كبيرة جداً ولا يمكن إدارتها بطريقة يدوية، حيث إن إدارتها ومعالجتها بشكل يدوي هي عملية صعبة ومضجرة وعرضة للخطأ.
- ضرورة التزام البنك بجمع كل ملفات logs الصادرة عن منظومته، كونها مصدر هام للمعلومات ولاحتمالية الحاجة للرجوع إليها في عمليات البحث المستقبلية والتحقيقات الجنائية الرقمية.
- قبل تطبيق مفهوم المركزية في تجميع ملفات logs والأحداث الناتجة عن مصادر البيانات في البنك كان يتم الاهتمام بجمع وتخزين الأحداث الحرجة والحساسة فقط لتحقيق بعض الضوابط المطلوبة وهو إجراء غير كافٍ لجهة تطبيق أمن معلومات فعال في البنك.

2.2. دور ميزات النظام في مساعدة فريق أمن المعلومات في تأدية مهامه:

نستعرض فيما يلي أدناه أهم النقاط التي ساهمت ميزات نظام SIEM عن طريقها في تحسين واقع أمن المعلومات في البنك وفي مساعدة فرق أمن المعلومات في المصارف في تأدية مهامها:

- إن استخدام مفهوم المركزية (Centralization) في تجميع الأحداث الصادرة عن البنية التحتية لمنظومة البنك تُتيح له إمكانية الوصول المباشر لأي حدث على أي تجهيزة من نظام أو مخدم أو قاعدة بيانات أو جدار نار أوغيره في منظومته وفي الزمن الحقيقي للحدث، وذلك قد لا يكون مُتاحاً من دون استخدام مثل هذا النظام المركزي وإن كان متاحاً فسيكون هذا بجهد وكلفة كبيرين ومن دون مراعاة عامل الزمن الحقيقي في إمكانية اكتشاف الحدث.

- يُمكّن النظام المركزي لتجميع الأحداث فريق أمن المعلومات من الاستفادة من ميزة الرؤية والمراقبة العامة لأحداث البنية التحتية في البنك والتي يوفرها هذا النظام عن طريق لوحة القيادة (dashboard) وميزة استخراج التقارير والاستجابة للحوادث والتحقيقات الجنائية الرقمية، وهو بذلك يقلل الكلفة من وقت وجهد ويساعد أيضاً في تحسين عمليات الالتزام والتدقيق الداخلي والعمليات المركزية وكشف الاحتيال، كما يخفف من درجة تعقيد إدارة البنية التحتية الضخمة.
- إن موضوع الاحتفاظ بالبيانات (Data Retention) هو أيضاً واحد من المشاكل التي حُلّت عند تطبيق نظام مركزي لتجميع الأحداث، علماً أن المدة الزمنية للاحتفاظ تُحدد من قبل البنك في "سياسة الاحتفاظ بالبيانات" مع مراعاة التزام هذا السياسة بالتعليمات والقرارات الصادرة عن الجهات الإشرافية والوصائية التي تم ذكرها في معرض هذا البحث.
- يُساعد نظام SIEM بشكل كبير في إدارة العمليات أيضاً وذلك عن طريق توفيره لإمكانية استخراج المعلومات المهمة عن كيفية حدوث خطأ في نظام أو مخدم ما، بالإضافة للمعلومات التي تشير إلى كيفية حل هذه المشكلة، كما أن توحيد صيغة ملفات سجلات LOGS ومعالجتها المعالجة المناسبة من قبل النظام يُحسّن من كفاءة عمليات البحث عن معلومات الأحداث وهو ما يساهم في تحسين إدارة العمليات التقنية في البنك.
- توفير نظام SIEM لميزة التحقيق الجنائي الرقمي (Forensic Investigation) عن طريق الاحتفاظ بجميع الأدلة العائدة لهجمة أو حدث ما في ملف واحد، مما يتيح للبنك إمكانية إجراء عمليات التحقيق اللازمة لاكتشاف السبب الحقيقي وراء الهجمة أو الحدث.

2.3. اختيار نظام SIEM يلائم طبيعة العمل في البنك وسياسته الأمنية:

إن عملية اختيار نظام SIEM مناسب للبنك من بين عدة شركات موردة لهذا النظام يخضع لعملية تقييم مسبقة من قبل البنك قبل اتخاذ قرار الشراء النهائي، حيث تتم عملية التقييم هذه ليس بناءً على المتطلبات الفنية والتقنية للنظام فقط (Technical Requirement)، بل أيضاً على احتياجات ومتطلبات البنك بحسب طبيعة بنيته التحتية وسير العمليات فيها وبما ينسجم مع سياسته الأمنية (Organizational Requirement).

إن تحديد المتطلبات بنوعيها هو أمر هام وجوهري جداً فهو يساعد البنك على تعريف وتحديد احتياجاته لتطبيق أمن معلومات فعال، حيث أن فريق أمن المعلومات وإدارة المخاطر في البنك هم

المسؤولون عن تقييم إمكانيات النظام التي يجب أن تلتزم مع السيناريوهات المطلوبة (Use Cases) والمتطلبات المُحدّدة وبحيث تنسجم مع بيئة العمل في البنك الحالية والمستقبلية القابلة للتوسع.

يمكن تقسيم هذه المتطلبات إلى:

- متطلبات إجبارية "Mandatory" مثل (قدرة النظام على جمع ملفات logs من مصادرها – أن يتمتع النظام بتصميم مرن وقابل التوسع مع توسع بنية البنك التحتية – أن يوفر النظام إتاحية عالية High Availability – أن يوفر النظام لوحة قيادة مرنة من حيث إظهار الأحداث والاستجابة لها Flexible Dashboard – أن يوفر النظام إمكانية إرسال التنبيهات في الزمن الحقيقي عبر البريد الالكتروني أو واتساب وتلغرام).
- متطلبات من الجيد وجودها "Nice to Have" مثل (إدارة المستخدمين وصلاحياتهم على النظام اعتماداً على مفهوم الأدوار Roles – قدرة البنك على القيام بتحديث النظام من دون العودة للشركة المزودة – أن يوفر النظام وحدة خاصة بإسناد متابعة المهام من قبل مدير فريق أمن المعلومات لعناصره Ticketing Module).

وهذه المتطلبات مجموعةً تعبر عن كل الميزات والخدمات التي يجب أن تكون متوفرة في النظام ويمكن تصنيفها عبر خمس قطاعات وهي (المنصة Platform – العمليات Operations – التكامل Integration – ميزات إضافية متقدمة Advanced Features – الترخيص وخدمات الدعم Licensing and Support Services).

بعد مرحلة تحديد المتطلبات تبدأ عملية اختبار النظام وتقييمه للتأكد من أن الميزات المذكورة في العرض هي فعلاً موجودة في النظام. تُقسم منهجيات التقييم إلى منهجية كمية Quantitative Methodology ومنهجية نوعية Qualitative Methodology.

تتميز المنهجية الكمية باعتمادها على الأرقام ونتائج القياسات والتحليلات الإحصائية والعمليات الحسابية وهي بالتالي تمثل عنصر الدقة في التقييم، في حين أن المنهجية النوعية تقوم بتقييم عوامل أخرى لا تُقاس بالأرقام مثل نجاح النظام وجدارته ووثوقيته في العمل في بيئة البنك بالاعتماد على المراقبة وعلى آراء الجهات المعنية وهي بذلك تمثل عنصر المرونة في التقييم.

إن هاتين المنهجيتين مكملتين لبعضهم البعض في عملية التقييم ولكل منها فوائدها في مساعدة أصحاب القرار في البنك على اتخاذ القرار الصحيح والمناسب في عملية الشراء والابتعاد عن الانحياز.

الفصل الرابع:

الجانب العملي/ استبيان عن أهم السيناريوهات الأمنية Use cases التي يحتاج فريق أمن المعلومات في المصارف لضبطها وكشفها عن طريق برنامج SIEM

1. المنهجية:

استخدمت الدراسة المنهج الوصفي التحليلي بوصفه المنهج الذي يعتمد على دراسة المشكلات والظواهر كما توجد في الواقع ويهتم بوصفها وصفاً دقيقاً ويعبر عنها كيفياً أو كمياً.

وكون المنهج الوصفي التحليلي يساعد الباحثين في جمع المعلومات والبيانات، مع إيجاد وسائل مختلفة لتفسيرها، فلذلك يستطيع الباحث الاعتماد عليه كأداة معرفية قائمة على تشخيص الحالة كما هي في الواقع لاختبار أسئلة الدراسة، وبيان نتائج وتوصيات الدراسة، والمنبثقة أساساً من آراء مختصي ومسؤولي أمن المعلومات وتقانة المعلومات.

2. أداة الدراسة:

استخدمت الدراسة الاستبيان كأداة لجمع البيانات حيث تم تطبيقها على عينة من مختصي ومسؤولي أمن المعلومات وتقانة المعلومات من كافة نواحي الجمهورية العربية السورية والوطن العربي، فالاستبيان هو أداة أساسية تستخدم في جمع بيانات من العينة المختارة أو من جميع مفردات مجتمع البحث عن طريق توجيه مجموعة من الأسئلة المحددة والمعدة مسبقاً وذلك لغاية التعرف على حقائق معينة.

تضمن الاستبيان السؤال عن أهم مصادر البيانات التي يجب ربطها مع برنامج SIEM بحيث تقوم بإرسال ملفات logs له، بالإضافة لتصنيف أهمية 103 سيناريو أمني (use case) من حيث الخطورة على مقياس من (عالي High، متوسط Medium، منخفض Low)، حيث تم اختيار هذه السيناريوهات الأمنية لإدراجها في الاستبيان بناءً على أهميتها ونتيجة لخبرة الباحثة في مجال تقانة وأمن المعلومات لمدة أربعة عشر عاماً في القطاع المصرفي، بحيث تندرج هذه السيناريوهات ضمن النطاقات التالية:

1. مخدمات بأنظمة تشغيل Windows Server
2. مخدمات بأنظمة تشغيل Linux
3. جدار النار Firewall

4. مخدم البريد الالكتروني Exchange Server
5. الاتصالات اللاسلكية والاتصالات عن بعد Wireless-VPN
6. نظام منع الاختراقات Intrusion Prevention System (IPS)
7. قواعد بيانات أوراكل Oracle Database
8. موجهات ومبدلات Routers/Switches
9. برنامج مضاد الفيروسات Anti-Virus

3. مجتمع الدراسة والعينة:

يمثل مجتمع الدراسة مختصي ومسؤولي أمن المعلومات وتقانة المعلومات في الجمهورية العربية السورية والوطن العربي، حيث تم تصميم استبيان الكتروني على منصة Google Forms لرصد الإجابات وتم نشر الرابط على المجموعات والمنتديات المختصة بأمن المعلومات على وسائل التواصل الاجتماعي (فيسبوك، تلغرام، LinkedIn) وتم جمع 38 استبيان وتم تحليل البيانات اعتماداً على عدد الإجابات الأعظمي لكل سؤال (Use Case).

نص الاستبيان:

تقوم الباحثة بإجراء دراسة حول (معايير عمل برنامج إدارة المعلومات والأحداث الأمنية SIEM وأهم السيناريوهات الأمنية Use cases التي يحتاج فريق أمن المعلومات في المصارف لضبطها وكشفها عن طريق البرنامج بما يحقق أمن معلومات فعال وبيئة عمل مصرفية آمنة تحمي أصول المعلومات فيها من التهديدات الداخلية والخارجية التي تهدف إلى اختراقها)، علماً أن إجاباتكم في هذا الاستبيان تُستخدم لأغراض البحث العلمي فقط لذلك لا حاجة لذكر الاسم، يرجى لطفاً اعتماد الدقة والموضوعية والتريّث في اختيار التثقيل الذي سيقيم أهمية السيناريو أو الـuse case (عالي High أو متوسط Medium أو منخفض Low)، آملين تعاونكم معنا ولكم جزيل الشكر والتقدير.

4. أسئلة الاستبيان مع النتائج:

ما هي أهم مصادر البيانات التي يجب ربطها مع برنامج SIEM بحيث تقوم بإرسال ملفات logs له؟

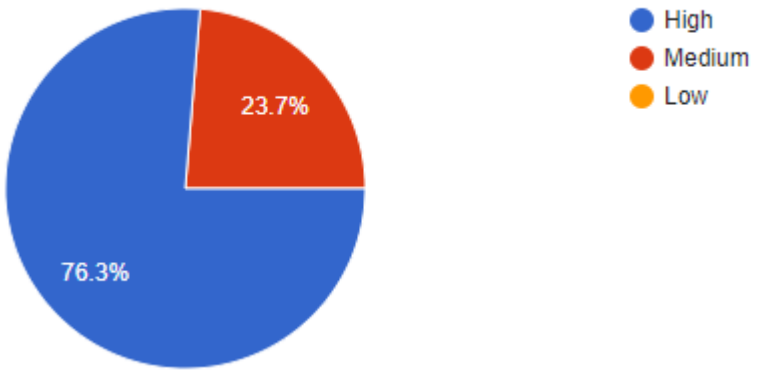
أهم مصادر البيانات التي يجب ربطها مع برنامج SIEM بحيث تقوم بإرسال ملفات logs له	النسبة المئوية
مخدمات بأنظمة تشغيل Windows Server	**76.3%**
مخدمات بأنظمة تشغيل Linux	**76.3%**
جدار النار Firewall	**84.2%**
مخدم البريد الالكتروني Exchange Server	**81.6%**
الاتصالات اللاسلكية والاتصالات عن بعد Wireless- VPN	**63.2%**
نظام منع الاختراقات Intrusion Prevention System (IPS)	**78.9%**
قواعد بيانات SQL	**68.4%**
قواعد بيانات أوراكل Oracle	**73.7%**
موجهات Routers	**55.3%**
مبدلات Switches	**50%**
برنامج مضاد الفيروسات Anti-Virus	**63.2%**
أخرى Other	**WAF (2.6%), Proxies, EDR, Honeypots (2.6%)**

النطاق الأول: السيناريوهات الأمنية الخاصة بمخدمات بأنظمة تشغيل Windows Server:

السؤال1 (Use Case1): وصل وحدة تخزين بالمخدم Removable media detected:

عدد الإجابات الكلي	High	Medium	Low
38	29	9	0

النسبة المئوية (%100)	76.3%	23.7%	0%



الشكل رقم (4) النسبة المئوية للسؤال 1 من النطاق الأول

تبين من نتيجة الاستبيان أن هذا السيناريو يُصنف عالي الأهمية من حيث الخطورة.

وهكذا وبنفس الطريقة تم التوصل إلى النتائج التالية بخصوص النطاق الأول:

مخدمات بأنظمة تشغيل Windows Server					
ر.ت	حالة استخدام أو مايسمى سيناريو أمني (Use Case)	عالي High	متوسط Medium	منخفض Low	النتيجة
1	Removable media detected وصل وحدة تخزين بالمخدم	76.3%	23.7%	0%	High
2	Server shutdown–reboot after office hours إيقاف تشغيل أو إعادة إقلاع المخدم بعد ساعات الدوام الرسمي	73.7%	18.4%	7.9%	High
3	Administrative group membership changed تغيير في أعضاء مجموعة المستخدمين المدراء	78.9%	15.8%	5.3%	High

Medium	2.6%	50%	47.4%	Remote access login – success & failure فشل أو نجاح عملية تسجيل دخول عن بعد للمخدم	4
Medium	7.9%	52.6%	39.5%	Certain windows account enabled/disabled تفعيل أو إيقاف تفعيل حساب مستخدم معين	5
High	0%	26.3%	73.7%	Logins outside normal business hours عمليات تسجيل الدخول بعد ساعات الدوام الرسمي	6
High	2.6%	2.6%	94.8%	Brute force attempt from same source with successful login التعرض لهجمة بروت فورس ونجاح تسجيل الدخول بعدها من نفس المصدر	7
High	2.6%	44.7%	52.7%	local windows account created/deleted إنشاء أو حذف مستخدم على المخدم	8
High	5.3%	26.3%	68.4%	Failed login to multiple destinations from same source فشل عملية تسجيل الدخول لعدة مخدمات من قبل نفس العنوان المصدر	9
High	5.2%	23.7%	71.1%	Administrative Account– Multiple Login failure فشل عدة محاولات تسجيل دخول لحساب بصلاحيات مدير	10

High	0%	18.4%	81.6%	Detection of user account added/removed in admin group إضافة أو حذف حساب مستخدم لمجموعة الحسابات بصلاحيات مدير	11
High	5.3%	26.3%	68.4%	Detection of use of default product vendor accounts استخدام أحد الحسابات الافتراضية على المخدم مثل حساب أدمن	12
Medium	13.2%	50%	36.8%	User deleted after 24hours of being created حذف حساب بعد 24 ساعة من إنشائه	13
High	0%	15.8%	84.2%	Critical service stopped on Windows Servers توقف خدمات حرجة على مخدمات ويندوز	14
Medium	5.3%	55.2%	39.5%	Windows log is full ملفات لوغز ممتلئة	15
High	7.9%	44.7%	47.4%	Multiple password changes in short time تغيير كلمة مرور حساب عدة مرات في وقت قصير	16
High	5.3%	39.4%	55.3%	Audit policy change تغيير في سياسة تسجيل الحركات والتدقيق على المخدم	17
High	0%	26.3%	73.7%	High number of users created/ removed within a short period of time إنشاء وحذف عدد كبير من حسابات المستخدمين في وقت قصير	18

High	2.7%	18.4%	78.9%	High outbound traffic observed from severs to Internet تدفق بيانات كبير من المخدمات إلى شبكة الإنترنت	19
High	10.6%	28.9%	60.5%	Failed logins attempt with disabled/ex-employee/expired accounts فشل عملية تسجيل دخول من حساب مقفل أو منتهي الصلاحية أو عائد لموظف مستقيل	20
High	15.8%	31.6%	52.6%	Windows file-folder delete حذف مجلد أو ملف من المخدم	21
Medium	10.5%	50%	39.5%	Windows-file folder permission changes تغيير في صلاحيات مجلد أو ملف على المخدم	22
High	5.2%	21.1%	73.7%	Monitor privileged user accounts activities مراقبة نشاطات الحسابات ذات الصلاحيات العالية	23
High	2.6%	26.3%	71.1%	Privileged accounts creation خلق حسابات بصلاحيات عالية	24
High	5.2%	21.1%	73.7%	Detect logs clearance or removal حذف ملفات لوغز خاصة بالمخدم	25
High	18.4%	31.6%	50%	Windows Hardware Failure فشل في أحد مكونات العتاد الصلب للمخدم	26

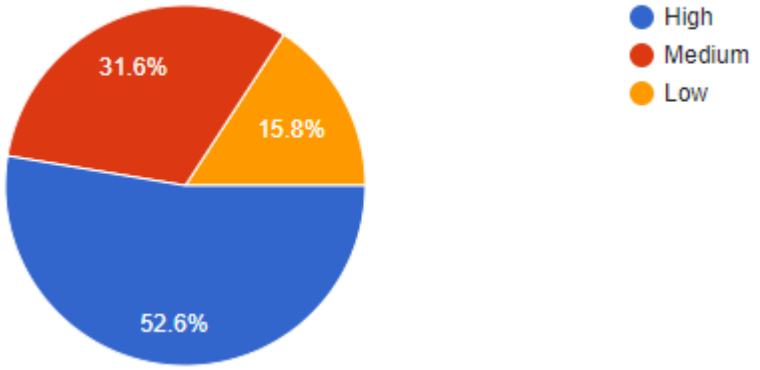
الجدول رقم (1) نتائج النطاق الأول

إذاً ومن أصل 26 سيناريو أمني في النطاق الأول تم تصنيف 21 عالي الخطورة و 5 متوسط الخطورة وصفر منخفض الخطورة.

النطاق الثاني: السيناريوهات الأمنية الخاصة بمخدمات بأنظمة تشغيل Linux:

السؤال1 (Use Case1): امتلاء نظام ملفات مخدم لينكس من حيث القدرة على التخزين Linux file system is full:

عدد الإجابات الكلي	High	Medium	Low
38	20	12	6
النسبة المئوية (%100)	52.6%	31.6%	15.8%



الشكل رقم (5) النسبة المئوية للسؤال 1 من النطاق الثاني

تبين من نتيجة الاستبيان أن هذا السيناريو يُصنف عالي الأهمية من حيث الخطورة.

وهكذا وبنفس الطريقة تم التوصل إلى النتائج التالية بخصوص النطاق الثاني:

مخدمات بأنظمة تشغيل Linux					
ر.ت	حالة استخدام أو مايسمى سيناريو أمني (Use Case)	عالي High	متوسط Medium	منخفض Low	النتيجة
1	Linux file system is full امتلاء نظام ملفات مخدم لينكس من حيث	52.6%	31.6%	15.8%	High

				القدرة على التخزين	
High	5.2%	31.6%	63.2%	Server shutdown إيقاف تشغيل المخدم	2
High	7.9%	42.1%	50%	Users created /deleted إنشاء أو حذف حسابات مستخدمين	3
High	5.3%	23.6%	71.1%	High number of users group created /removed within a short period إضافة أو حذف عدد كبير من حساب مستخدمين على مجموعة خلال فترة قصيرة	4
High	7.9%	36.8%	55.3%	Linux-Login attempts with the same account from different source desktops عدة محاولات دخول على المخدم من نفس حساب المستخدم ولكن من عناوين أجهزة مختلفة مختلفة	5
High	2.6%	15.8%	81.6%	Failed logins (Reports when an account causes an authentication failure event at least 9 times to a single Linux host within 1 minute) فشل 9 محاولات تسجيل دخول لحساب مستخدم على المخدم خلال دقيقة واحدة	6
High	15.7%	21.1%	63.2%	Failed logins with disabled accounts فشل عمليات تسجيل الدخول من خلال حساب منتهي الصلاحية	7

8	Detection of use of default product vendor accounts استخدام أحد الحسابات الافتراضية على المخدم مثل حساب رووت	76.3%	15.8%	7.9%	High
9	Failed logins from root access فشل عدة عمليات تسجيل الدخول من رووت خلال حساب	57.9%	36.8%	5.3%	High
10	Linux multiple sudo login failures فشل عدة عمليات للانتقال من حساب مستخدم ما إلى الحساب رووت من خلال تعليمة سودو	63.2%	28.9%	7.9%	High
11	Sudo access login success نجاح عملية الانتقال من حساب ما إلى الحساب رووت من خلال تعليمة سودو	55.3%	36.8%	7.9%	High
12	Critical services stopped like (oracle database listener) توقف أحد الخدمات الحرجة على المخدم مثل (خدمة الاتصال مع قواعد بيانات أوراكل)	76.3%	21.1%	2.6%	High
13	High privileged accounts password changed تغيير كلمة مرور أحد الحسابات ذات الصلاحيات العالية	50%	44.7%	5.3%	High
14	Adding, removing and modifying cron jobs إضافة أو حذف أو تعديل أحد المهام المجدولة على المخدم	36.8%	50%	13.2%	Medium

15	Detection of change in syslog configuration تغيير في إعدادات النظام المسؤول عن إدارة ملفات لوغز في المخدم	76.3%	18.4%	5.3%	High
16	Privileged accounts creation خلق حسابات مستخدمين بصلاحيات عالية	71.1%	23.7%	5.2%	High

الجدول رقم (2) نتائج النطاق الثاني

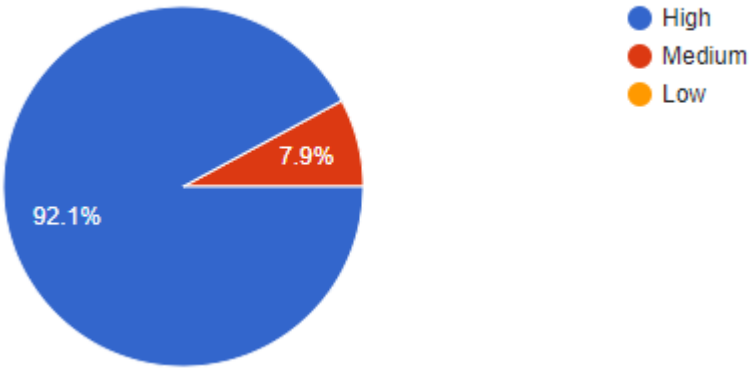
إذاً ومن أصل 16 سيناريو أمني في النطاق الثاني تم تصنيف 15 عالي الخطورة و 1 متوسط الخطورة وصفر منخفض الخطورة.

النطاق الثالث: السيناريوهات الأمنية الخاصة بجدار النار Firewall:

السؤال1 (Use Case1): فشل عدة عمليات دخول لحساب المدير (أدمن) على الفايروول (تسع محاولات خلال دقيقة واحدة)

Administrator login failure (Reports when an admin account causes an authentication failure event at least 9 times within 1 minute):

عدد الإجابات الكلي	High	Medium	Low
38	35	3	0
النسبة المئوية (%100)	92.1%	7.9%	0%



الشكل رقم (6) النسبة المئوية للسؤال 1 من النطاق الثالث

تبين من نتيجة الاستبيان أن هذا السيناريو يُصنف عالي الأهمية من حيث الخطورة.

وهكذا وبنفس الطريقة تم التوصل إلى النتائج التالية بخصوص النطاق الثالث:

جدار النار Firewall					
ر.ت	حالة استخدام أو مايسمى سيناريو أمني (Use Case)	عالي High	متوسط Medium	منخفض Low	النتيجة
1	Administrator login failure (Reports when an admin account causes an authentication failure event at least 9 times within 1 minute) فشل عدة عمليات دخول لحساب المدير (أدمن) على الفايروول (تسع محاولات خلال دقيقة واحدة)	92.1%	7.9%	0%	High
2	Brute force with successful configuration changes التعرض لهجمة بروت فروس على أحد حسابات مستخدمي جدار النار يتبعها تغيير في إعداداته	92.1%	7.9%	0%	High
3	Firewall failover فشل في عمل وظائف جدار النار	86.8%	10.5%	2.7%	High
4	Successful connection from internet IP after repetitive blocks in firewall نجاح عبور اتصال من عنوان على شبكة الإنترنت عبر جدار النار إلى الشبكة الداخلية وذلك بعدة عمليات حظر له من	92.1%	7.9%	0%	High

				قبل جدار النار	
High	0%	31.6%	68.4%	Successful logon between non-business hours نجاح تسجيل دخول حساب مستخدم إلى جدار النار خارج أوقات الدوام الرسمي	5
High	7.9%	39.5%	52.6%	Firewalls reboot إعادة إقلاع جدار النار	6
High	7.9%	36.8%	55.3%	User added/deleted to firewall إضافة أو حذف حسابات مستخدمين لجدار النار	7
High	2.6%	31.6%	65.8%	High number of denied events عدد كبير من عمليات حجب الوصول من قبل جدار النار	8
High	5.3%	26.3%	68.4%	configuration change detected on firewall تغيير في إعدادت جدار النار	9
High	5.2%	23.7%	71.1%	Network and host port scan attempts محاولات القيام بعملية مسح للشبكة أو لجهاز ما	10
Medium	7.9%	52.6%	39.5%	Detection of primary-secondary switch over اكتشاف حدوث عملية تبديل بين المبدلة الرئيسية والثانوية	11
Medium	13.2%	52.6%	34.2%	An admin has allowed/removed access to the firewall from a	12

				particular IP قيام حساب مدير لجدار النار بسماح أو منع إمكانية الوصول لجدار النار من عنوان معين	
High	2.7%	28.9%	68.4%	Detecting high CPU utilization on firewall لحظ وجود معدل عال من استخدامية وحدة المعالج على جدار النار	13
High	0%	18.4%	81.6%	Outbound traffic observed on important ports حدوث تدفق بيانات خارجة من منافذ هامة على الشبكة	14
High	0%	2.6%	97.4%	Successful outbound traffic to blacklisted threat IP address نجاح خروج تدفق بيانات لعناوين محظورة	15
High	0%	23.7%	76.3%	Adding/removing/changing in access rules إضافة أو تغيير أو حذف في قواعد الوصول على جدار النار	16
High	0%	15.8%	84.2%	Outbound connection to a foreign country اتصال خارج من الشبكة إلى بلدان أجنبية أو معادية	17
High	2.6%	21.1%	76.3%	Excessive firewall denies from single source (Reports excessive firewall denies from a single host to a single destination within 5 minutes)	18

	حجب عدة محاولات للعبور عبر جدار النار من نفس العنوان إلى نفس الهدف خلال خمس دقائق				

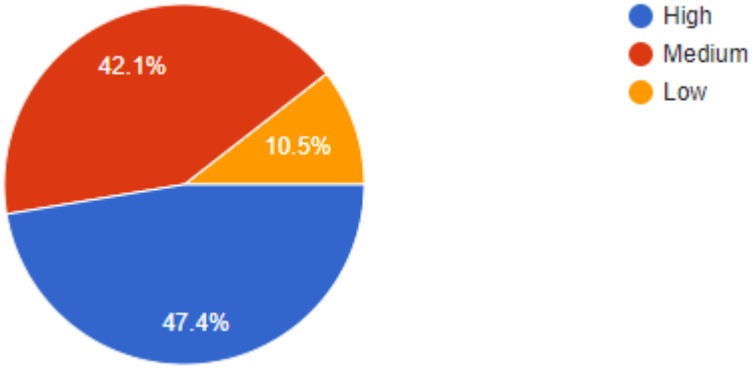
الجدول رقم (3) نتائج النطاق الثالث

إذاً ومن أصل 18 سيناريو أمني في النطاق الثالث تم تصنيف 16 عالي الخطورة و 2 متوسط الخطورة وصفر منخفض الخطورة.

النطاق الرابع: السيناريوهات الأمنية الخاصة بمخدم البريد الالكتروني Exchange Server:

السؤال1 (Use Case1): أكبر عشر مستخدمين يقومون بإرسال رسائل بريد الكتروني لنطاقات خارج الشبكة الداخلية للبنك Top 10 users sending mails to external domains:

Low	Medium	High	عدد الإجابات الكلي
4	16	18	38
10.5%	42.1%	47.4%	النسبة المئوية (%100)



الشكل رقم (7) النسبة المئوية للسؤال 1 من النطاق الرابع

تبين من نتيجة الاستبيان أن هذا السيناريو يُصنف عالي الأهمية من حيث الخطورة.

وهكذا وبنفس الطريقة تم التوصل إلى النتائج التالية بخصوص النطاق الرابع:

مخدم البريد الالكتروني Exchange Server					
ر.ت	حالة استخدام أو مايسمى سيناريو أمني (Use Case)	عالي High	متوسط Medium	منخفض Low	النتيجة
1	Top 10 users sending mails to external domains أكبر عشر مستخدمين يقومون بإرسال رسائل بريد الكتروني لنطاقات خارج الشبكة الداخلية للبنك	47.4%	42.1%	10.5%	High
2	Large files send via mail ملفات بأحجام كبيرة يتم إرسالها عبر البريد الالكتروني	55.3%	39.5%	5.2%	High
3	Malicious/Suspicious attachments identified ملفات مرفقة برسائل البريد الالكتروني مشبوهة بأنها خبيثة	78.9%	21.1%	0%	High
4	Monitoring mails going out from the bank domain to other domains after office hours مراقبة رسائل البريد الالكتروني الصادرة من البنك إلى نطاقات خارجية خارج أوقات الدوام الرسمي	65.8%	34.2%	0%	High
5	High number of rejected mails from single “from” address عدد كبير من الرسائل المرفوضة من نفس المرسل	47.4%	42.1%	10.5%	High

الجدول رقم (4) نتائج النطاق الرابع

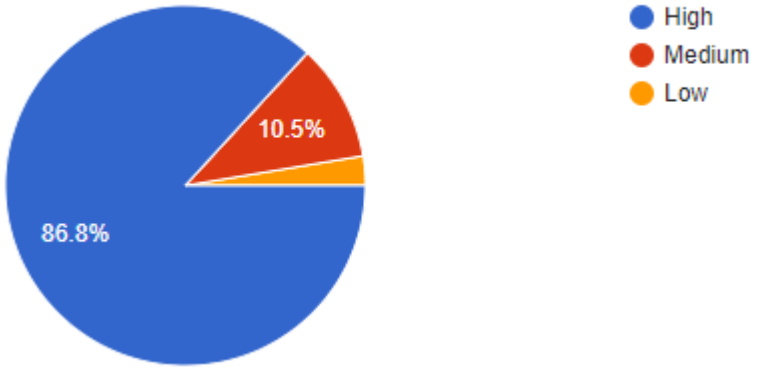
إذاً ومن أصل 5 سيناريو أمني في النطاق الرابع تم تصنيفها جميعها عالية الخطورة.

النطاق الخامس: السيناريوهات الأمنية الخاصة بالاتصالات اللاسلكية والاتصالات عن بعد Wireless-VPN:

السؤال1 (Use Case1): حسابات الدخول عن بعد التي تسجل دخول إلى الشبكة الداخلية للبنك من أكثر من مكان بعيد أو من بلدان معادية

Top VPN account logged in from multiple remote locations or from suspicious countries:

Low	Medium	High	عدد الإجابات الكلي
1	4	33	38
2.7%	10.5%	86.8%	النسبة المئوية (%100)



الشكل رقم (8) النسبة المئوية للسؤال 1 من النطاق الخامس

تبين من نتيجة الاستبيان أن هذا السيناريو يُصنف عالي الأهمية من حيث الخطورة.

وهكذا وبنفس الطريقة تم التوصل إلى النتائج التالية بخصوص النطاق الخامس:

الاتصالات اللاسلكية والاتصالات عن بعد Wireless-VPN					
ر.ت	حالة استخدام أو مايسمى سيناريو أمني (Use Case)	عالي High	متوسط Medium	منخفض Low	النتيجة
1	Top VPN account logged in from multiple remote locations or from suspicious countries حسابات الدخول عن بعد التي تسجل دخول إلى الشبكة الداخلية للبنك من أكثر من مكان بعيد أو من بلدان معادية	86.8%	10.5%	2.7%	High
2	Wireless unauthorized login attempts محاولات تسجيل الدخول الفاشلة بطريقة لاسلكية	34.2%	57.9%	7.9%	Medium
3	VPN connection beyond 24 hours اتصال عن بعد للشبكة الداخلية مستمر لأكثر من 24 ساعة	68.4%	31.6%	0%	High
4	Wireless Access Point rebooted إعادة إقلاع نقطة اتصال لاسلكية	57.9%	18.4%	23.7%	High
5	Wireless unsecure Access Point detected اكتشاف نقطة اتصال لاسلكية غير آمنة	76.3%	21.1%	2.6%	High

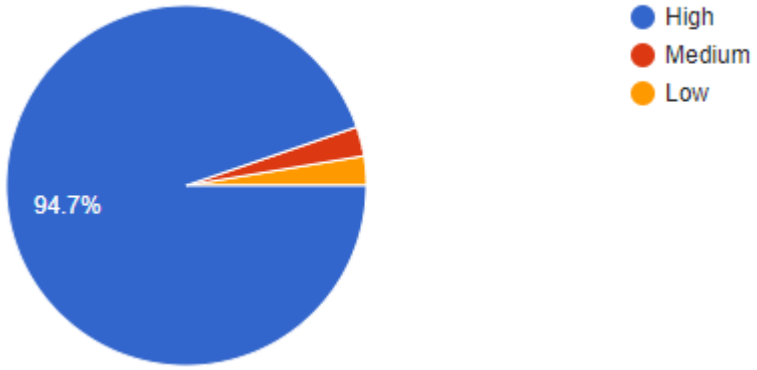
الجدول رقم (5) نتائج النطاق الخامس

إذاً ومن أصل 5 سيناريو أمني في النطاق الخامس تم تصنيف 4 عالي الخطورة و 1 متوسط الخطورة وصفر منخفض الخطورة.

النطاق السادس: السيناريوهات الأمنية الخاصة بنظام منع الاختراقات Intrusion Prevention System (IPS):

السؤال1 (Use Case1): التحذيرات الخطرة التي يطلقها النظام IPS high alerts:

Low	Medium	High	عدد الإجابات الكلي
1	1	36	38
2.7%	2.6%	94.7%	النسبة المئوية (%100)



الشكل رقم (9) النسبة المئوية للسؤال 1 من النطاق السادس

تبين من نتيجة الاستبيان أن هذا السيناريو يُصنف عالي الأهمية من حيث الخطورة.

وهكذا وبنفس الطريقة تم التوصل إلى النتائج التالية بخصوص النطاق السادس:

نظام منع الاختراقات Intrusion Prevention System (IPS)					
ر.ت	حالة استخدام أو مايسمى سيناريو أمني (Use Case)	عالي High	متوسط Medium	منخفض Low	النتيجة
1	IPS high alerts التحذيرات الخطرة التي يطلقها النظام	94.7%	2.6%	2.7%	High
2	Possible exploit of vulnerability احتمال استغلال ثغرة ما في الشبكة الداخلية	84.2%	15.8%	0%	High

3	SQL Injection attempt محاولة تنفيذ هجمة حقن اس كيو ال	89.5%	7.9%	2.6%	High
4	Virus traffic in the network كشف اتصالات في الشبكة ناجمة عن فيروس ما	89.5%	10.5%	0%	High

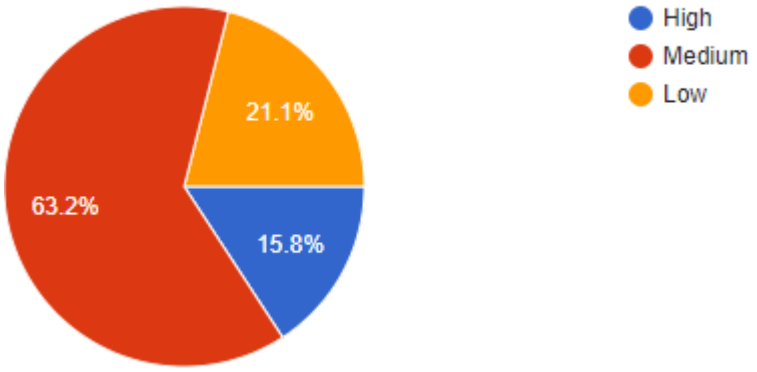
الجدول رقم (6) نتائج النطاق السادس

إذاً ومن أصل 4 سيناريو أمني في النطاق السادس تم تصنيفها جميعها عالية الخطورة.

النطاق السابع: السيناريوهات الأمنية الخاصة بقواعد بيانات أوراكل Oracle Database:

السؤال1 (Use Case1): انتهاء صلاحية كلمة مرور أحد مستخدمي قواعد البيانات Oracle password expired:

عدد الإجابات الكلي	High	Medium	Low
38	6	24	8
النسبة المئوية (%100)	15.8%	63.1%	21.1%



الشكل رقم (10) النسبة المئوية للسؤال 1 من النطاق السابع

تبين من نتيجة الاستبيان أن هذا السيناريو يُصنف متوسط الأهمية من حيث الخطورة.

وهكذا وبنفس الطريقة تم التوصل إلى النتائج التالية بخصوص النطاق السابع:

قواعد بيانات أوراكل Database Oracle					
ر.ت	حالة استخدام أو مايسمى سيناريو أمني (Use Case)	عالي High	متوسط Medium	منخفض Low	النتيجة
1	Oracle password expired انتهاء صلاحية كلمة مرور أحد مستخدمي قواعد البيانات	15.8%	63.1%	21.1%	Medium
2	Critical commands executed on the database تنفيذ تعليمات حرجة على قواعد البيانات	78.9%	21.1%	0%	High
3	Oracle user created/deleted إنشاء أو حذف مستخدم على قواعد البيانات	52.6%	44.7%	2.7%	High
4	Multiple login failures observed for database فشل عدة محاولات تسجيل دخول لقاعدة البيانات	44.7%	42.1%	13.2%	High
5	Database schema creation/modification/deletion إنشاء أو حذف أو تعديل في مخطط قاعدة البيانات	63.2%	31.6%	5.2%	High
6	Monitoring login attempts on database مراقبة محاولات تسجيل الدخول إلى قاعدة البيانات	55.3%	36.8%	7.9%	High
7	Database access during non-business hours الدخول إلى قاعدة البيانات خارج أوقات	65.8%	31.6%	2.6%	High

	الدوام الرسمي				
8	Oracle user changed privilege تغيير صلاحيات أحد مستخدمي قواعد البيانات	65.8%	28.9%	5.3%	High
9	Privileged accounts creation إنشاء مستخدم بصلاحيات عالية على قاعدة البيانات	78.9%	13.2%	7.9%	High
10	Excessive database connections اتصالات كثيرة مع قاعدة البيانات	68.4%	23.7%	7.9%	High

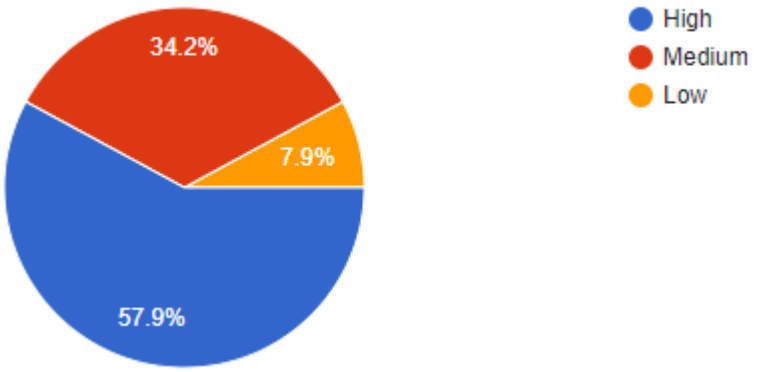
الجدول رقم (7) نتائج النطاق السابع

إذاً ومن أصل 10 سيناريو أمني في النطاق السابع تم تصنيف 9 عالي الخطورة و 1 متوسط الخطورة وصفر منخفض الخطورة.

النطاق الثامن: السيناريوهات الأمنية الخاصة بالموجهات والمبدلات Routers/Switches:

السؤال1 (Use Case1): رسائل خطأ حرجة تظهر على الموجه Emergency router error messages:

عدد الإجابات الكلي	High	Medium	Low
38	22	13	3
النسبة المئوية (%100)	57.9%	34.2%	7.9%



الشكل رقم (11) النسبة المئوية للسؤال 1 من النطاق الثامن

تبين من نتيجة الاستبيان أن هذا السيناريو يُصنف عالي الأهمية من حيث الخطورة.

وهكذا وبنفس الطريقة تم التوصل إلى النتائج التالية بخصوص النطاق الثامن:

Routers/Switches ومبدلات موجهات					
ر.ت	حالة استخدام أو مايسمى سيناريو أمني (Use Case)	عالي High	متوسط Medium	منخفض Low	النتيجة
1	Emergency router error messages رسائل خطأ حرجة تظهر على الموجه	57.9%	34.2%	7.9%	High
2	Router–power supply failure فشل وحدة التغذية في الموجه	55.3%	36.8%	7.9%	High
3	Router configuration change تغيير في إعدادات الموجه	39.5%	55.3%	5.2%	Medium
4	Critical messages observed from the switch رسائل حرجة تظهر على المبدلة	63.2%	31.6%	5.2%	High
5	Detection of land attack (DOS Attack) اكتشاف التعرض لهجمة الحرمان من الخدمة	92.1%	7.9%	0%	High

6	Detection of ping of death attack اكتشاف التعرض لهجمة بينغ حتى الموت	89.5%	10.5%	0%	High
7	Detection of new policy addition in the router اكتشاف إضافة سياسة جديدة على الموجه	47.4%	50%	2.6%	Medium
8	Detection of policy violation in the router اكتشاف خرق سياسة على الموجه	76.3%	21.1%	2.6%	High
9	Long Duration ICMP Flows (Detection of ICMP packets between hosts that last a long time) اكتشاف تدفق رزم من نوع آي سي ام بي بين جهازين لفترة طويلة	55.3%	39.5%	5.2%	High

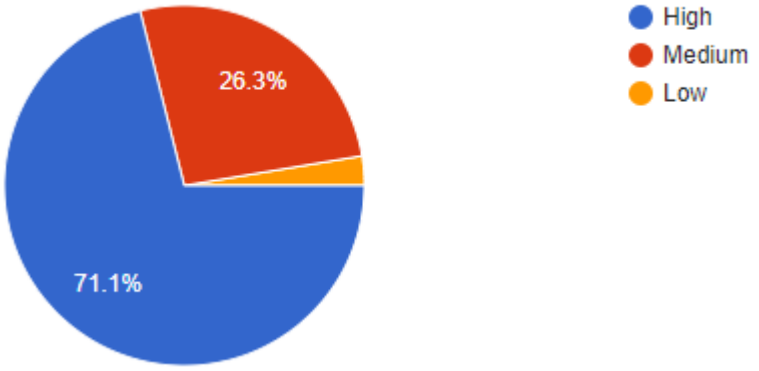
الجدول رقم (8) نتائج النطاق الثامن

إذاً ومن أصل 9 سيناريو أمني في النطاق الثامن تم تصنيف 7 عالي الخطورة و 2 متوسط الخطورة وصفر منخفض الخطورة.

النطاق التاسع: السيناريوهات الأمنية الخاصة ببرنامج مضاد الفيروسات Anti-Virus:

السؤال1 (Use Case1): اكتشاف برنامج مضاد الفيروسات لفيروس ما Anti-Virus virus detected:

عدد الإجابات الكلي	High	Medium	Low
38	27	10	1
النسبة المئوية (%100)	71.1%	26.3%	2.6%



الشكل رقم (12) النسبة المئوية للسؤال 1 من النطاق التاسع

تبين من نتيجة الاستبيان أن هذا السيناريو يُصنف عالي الأهمية من حيث الخطورة.

وهكذا وبنفس الطريقة تم التوصل إلى النتائج التالية بخصوص النطاق التاسع:

برنامج مضاد الفيروسات Anti-Virus					
ر. ت	حالة استخدام أو مايسمى سيناريو أمني (Use Case)	عالي High	متوسط Medium	منخفض Low	النتيجة
1	Anti-Virus virus detected اكتشاف برنامج مضاد الفيروسات لفيروس ما	71.1 %	26.3%	2.6%	High
2	Anti-Virus malware infection identified (not quarantined/cleaned/deleted/moved) الإصابة بالعدوى ببرنامج خبيث (أي لم يتم حجره أو حذفه أو نقله)	92.1 %	5.3%	2.6%	High
3	Multiple sources accessing the same malware URL عدة مصادر على الشبكة تقوم بالوصول لنفس المسار أو العنوان الخبيث	84.2 %	15.8%	0%	High

High	10.5 %	31.6%	57.9 %	Detection of antivirus failure update in end user machines اكتشاف حالات فشل عملية تحديث برنامج مضاد الفيروسات على أجهزة المستخدمين	4
High	5.2%	23.7%	71.1 %	Attempt to stop the daily scan schedules اكتشاف محاولة إيقاف عمليات المسح الدورية للأجهزة	5
High	0%	15.8%	84.2 %	Detecting of attempts to stop the antivirus services اكتشاف محاولات لإيقاف خدمات برنامج مضاد الفيروسات	6
Medium	10.5 %	47.4%	42.1 %	Detection of the scan which is stopped before it completes اكتشاف الحالات التي تم فيها إيقاف عملية المسح قبل انتهائها	7
High	13.2 %	36.8%	50%	Detection of the computer which is not protected with latest definitions اكتشاف الكومبيوتر الغير محمي بآخر تحديث من برنامج مضاد الفيروسات	8
High	0%	15.8%	84.2 %	Brute Force/port or host scan/privilege escalation access attempt from the Infected machine محاولات القيام بهجمات من الجهاز المصاب بالفيروس مثل (بروت فورس–مسح للمنافذ–الحصول على الصلاحيات الأعلى)	9

10	Access to critical file share, network path, SSH or Remote RDP attempt from the infected host محاولات الوصول لملفات مشاركة أو مسارات شبكة حرجة أو محاولات للاتصال عن بعد من قبل الجهاز المصاب بالفيروس	**84.2 %**	**13.2%**	**2.6%**	**High**

الجدول رقم (9) نتائج النطاق التاسع

إذاً ومن أصل 10 سيناريو أمني في النطاق التاسع تم تصنيف 9 عالي الخطورة و 1 متوسط الخطورة وصفر منخفض الخطورة.

الفصل الخامس:

نتائج البحث والتوصيات والمراجع

1. تمهيد:

يتضمن هذا الفصل ملخصاً لأهم النتائج التي توصل إليها البحث وأهم التوصيات المقترحة لتعزيز أهداف هذا البحث.

2. نتائج البحث:

في نهاية البحث تم التوصل إلى مجموعتين من النتائج: أولها هي نتائج التطبيق العملي، أما الثانية فهي نتائج عامة.

2.1. نتائج التطبيق العملي:

- إن ارتفاع نسب السيناريوهات الأمنية (use cases) ضمن الاستبيان والتي تم تصنيفها على أنها عالية الأهمية من حيث الخطورة (High) من قبل المُصوتين والتي بلغ عددها 90 من أصل 103، هو دليل على أهمية الأنظمة التي تم تشميلها في الاستبيان كمصادر للمعلومات والأحداث الأمنية بالنسبة لفرق ومسؤولي أمن المعلومات.
- إن السيناريوهات الأمنية (use cases) ضمن الاستبيان والتي تم تصنيفها على أنها عالية الأهمية من حيث الخطورة (High) وبفرق كبير جداُ عن نسبة المُصوتين على أنها متوسطة الأهمية (Medium) مثل السيناريو الأمني الثاني من النطاق الثالث (التعرض لهجمة بروت فروس على أحد حسابات مستخدمي جدار النار يتبعها تغيير في إعداداته)، هو دليل قاطع على أهمية وحراجية مثل هذه السيناريوهات وضرورة مراقبتها وضبطها لضمان أمن معلومات فعال في أي مؤسسة.
- إن السيناريوهات الأمنية (use cases) ضمن الاستبيان والتي تم تصنيفها على أنها عالية الأهمية أو متوسطة الأهمية من حيث الخطورة وبفرق بسيط بين المُصوتين على التصنيفين مثل السيناريو الأمني الخامس من النطاق الرابع (عدد كبير من الرسائل المرفوضة من نفس المرسل)، هو دليل على الأهمية النسبية لهذا السيناريو الأمني وذلك تبعاً لطبيعة المؤسسة وسياسة أمن المعلومات المطبقة فيها.
- إن تصنيف نفس السيناريو الأمني من قبل المُصوتين في الاستبيان على أنه عالي الأهمية في نطاق ما ومتوسط الأهمية في نطاق آخر مثل السيناريو الأمني التاسع في النطاق

الثالث (تغيير في إعدادت جدار النار) المُصنف (High) والسيناريو الأمني الثالث في النطاق الثامن (تغيير في إعدادات الموجه) المُصنف (Medium)، هو أيضاً دليل الأهمية النسبية لهذا السيناريو بحسب مصدر المعلومات القادم منه حيث يُعتبر جدار النار من أهم خطوط الدفاع في أي منظومة ضد الهجمات الخارجية وبالتالي فإن ضبط وتغيير إعداداته يرتبط مباشرة بسياسة أمن المعلومات في المؤسسة، بينما قد يكون حدوث تغييرات في إعدادات الموجه هو أمر تشغيلي طبيعي ضمن المؤسسة.

- إن انعدام تصنيف أي سيناريو أمني من قبل المُصوتين في الاستبيان على أنه منخفض الأهمية (Low)، هو دليل على أهمية كل السيناريوهات الأمنية المطروحة بالنسبة لمسؤولي وفرق أمن المعلومات.

2.2. نتائج عامة:

- إن وجود نظام مركزي مثل نظام SIEM لإدارة ملفات السجلات والأحداث في المنظومة المعلوماتية للبنك أو لأي مؤسسة يساعد فرق أمن المعلومات فيها في مراقبة السيناريوهات الأمنية التي تحدث على مصادر البيانات فيها مما يلعب دوراً هاماً في تعزيز ممارسة هذه الفرق لمهامها ومسؤولياتها.
- إن القيمة المُضافة التي يقدمها نظام SIEM في تعزيز دور أمن المعلومات في البنك يعتمد على مصادر البيانات التي يجب ربطها معه بحيث تقوم بإرسال ملفات logs له، وأيضاً على عدد قواعد الارتباط (correlation rules) الموجودة في النظام وتلك التي يتم إضافتها من قبل فريق أمن المعلومات للنظام والتي هي الأساس في ضبط السيناريوهات الأمنية التي سيتم مراقبتها من خلال النظام.

3. التوصيات:

- الالتزام بوضع سياسة وخطة شاملة لإدارة أمن المعلومات في البنك من قبل فريق أمن المعلومات تشمل بشكل أساسي تحديد وتحليل وتقييم مخاطر أمن المعلومات في البنك مشفوعة بالتوصيات والمقترحات الواجب تنفيذها لتخفيف هذه المخاطر، بالإضافة لتحديد المؤشرات التي تقيس مدى فعالية الضوابط المحددة في سياسة أمن المعلومات ومصادقة هذه الخطة من قبل مجلس إدارة البنك.

- دعم مجالس الإدارة والإدارة التنفيذية العليا لفرق أمن المعلومات في المصارف العاملة في الجمهورية العربية السورية لجهة توفير الأدوات والأنظمة والبرامج اللازمة لها بما يسهل ممارستها للمهام والمسؤوليات المطلوبة منها.
- تبني المصارف العاملة في الجمهورية العربية السورية وجود نظام مركزي مثل نظام SIEM في منظومتها المعلوماتية لإدارة ملفات السجلات والأحداث الصادرة عن مصادر البيانات فيها وذلك لما له من دور فعال وهام في تعزيز ممارسة فرق أمن المعلومات فيها لمهامها ومسؤولياتها لجهة حماية أصول المعلومات ضد محاولات الاختراق الداخلية والخارجية.
- توفير التدريب اللازم من قبل الإدارة العليا لفريق أمن المعلومات في أي مؤسسة وذلك لزيادة مؤهلات عناصره العلمية والمهنية مما يلعب دور هام في قدرة هذا الفريق على القيام بمهامه ومسؤولياته المطلوبة منه.
- إجراء برامج ودورات توعية للموظفين في البنك عن مخاطر أمن المعلومات والهجمات التي يمكن أن يتعرض لها البنك، وذلك لما لهذه التوعية من دور هام جداً في تعريف الموظفين حول المسؤولية التي يُشاركون فيها في الوقاية من هذه الهجمات وحماية أصول المعلومات في البنك.
- استخدام أدوات الذكاء الصناعي بما يساعد فرق أمن المعلومات في المصارف في توفير الوقت والجهد اللازم لممارسة مهامها، مع القيام أولاً بعملية تقييم لمعرفة أثر المخاطر المحتملة عن استخدام هذه الأدوات على منظومة البنك قبل البدء باستخدامها.

4. المراجع:

4.1. المراجع العربية:

- الشمالي، د. حسين علي قاسم. (2018). أمن وسرية المعلومات وأثرها في الأداء المصرفي: دراسة تطبيقية على البنوك العاملة في الأردن.
- Alkhankani, N. K. (2017). حماية امن المعلومات المصرفية وفق المواصفات العالمية (ISO 17799) ومدى تطبيقه في المصارف. THE IRAQI MAGAZINJE FOR MANAGERIAL SCIENCES، 13(54).

- المخلافي، ش. (2018). دور نظام أمن المعلومات فى تطوير الخدمات المصرفية دراسة ميدانية بالتطبيق على البنوك اليمنية. المجلة العلمية للدراسات التجارية والبيئية، 9(العدد الثاني الجزء الثاني)، 596-618.
- قرزيز، نبيلة، زيدان، & محمد. (2022). دور أمن المعلومات في تحقيق جودة الخدمات المصرفية-دراسة حالة القرض الشعبي الجزائري بالشلف-/ The role of information security in achieving the quality of banking services-Case study of the Algerian people's loan (CPA) in Chlef. مجلة الاقتصاد والمالية، 8(1)، 82-98.

4.2. المراجع الأجنبية:

- Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E., & Zunino, R. (2019). The guidelines to adopt an applicable SIEM solution. Journal of Information Security, 11(1), 46-70.
- Chapple, M., Stewart, J. M., & Gibson, D. (2018). (ISC) 2 CISSP Certified Information Systems Security Professional Official Study Guide. John Wiley & Sons.
- Reynoso Vásquez, V. K. (2009). Events Centralization and Correlation at a Finance Entity.
- Gaber, C., Gharout, S., Achemlal, M., Pasquet, M., & Urien, P. (2012). Security challenges for security information and event management systems in mobile money transfer services.
- González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors, 21(14), 4759.
- Cugnasco, F. (2023). Analysis of a multi-channel anti-fraud platform in banking (Doctoral dissertation, Politecnico di Torino).
- Remus, M. S. H., Akter, S., & Ferdous, K. (2023). Evaluation of ICT Security Implementation in Banks: Bangladesh

Perspective. European Journal of Computer Science and Information Technology, 11(6), 22-41.

- Chikonga, M. (2014). Exploring the applicability of SIEM technology in IT security (Doctoral dissertation, Auckland University of Technology).
- Jangampeta, S. (2022). Financial Data Security and SIEM: Protecting Sensitive Financial Information in Banking and Fintech Systems. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 13(2), 1185-1188.

نهاية البحث