الحلول الرقمية الابتكارية في مجال حماية الهوية و الخصوصية والأمن السيبراني خلال جائحة كوفيد-19

Innovative Digital Solutions in the Field of Information Security during the Covid-19 pandemic

أمينة بن زرارة
جامعة 8 ماي 1945- قالمة (الجزائر)
Benzerara.amina@univ-guelma.dz

أعراب فطيمة
جامعة أكلي محند أولحاج- البويرة (الجزائر)
Fatima19arab@gmail.com

ملخص:

أدت جائحة كوفيد19 إلى ظهور أنماط جديدة من جرائم الإنترنيت، وبسبب توالي هذه الجرائم ووصولها إلى أروقة صُنّاع القرار،، شجعت مختلف الدول ومن بينها الجزائر عمليات الابتكار و الحلول التي تقدمها الشركات الناشئة التكنولوجية في مجال تعزيز الأمن السيبراني، و ذلك من خلال خلق بيئة مقاولاتية لابتكار أعمال وتطبيقات تنشط في هذا المجال.

وقد جاءت هذه الدراسة بهدف تسليط الضوء على أهم نماذج المؤسسات الناشئة الرائدة في مجال حماية البيئة الرقمية من مخاطر الاختراق من خلال ما تقدمه من حلول و تقنيات مبتكرة خاصة في ظل النمو السريع في الطلب على خدمات ومنتجات الأمن السيبراني خلال جائحة كوفيد 19، وتوصلت هذه الدراسة إلى أن الدور الأساسي لهذه الشركات سيكون بالتركيز على إيجاد الحلول الوقائية والرادعة للهجمات السيبرانية من خلال ابتكار منتجات وحلول إبداعية مبتكرة في مجال الأمن السيبراني للعالم ككل و الذي يفتح آفاقا جديدة في السوق الجزائرية لتبني مثل هذه المبتكرات لتحقيق مستقبل آمن سيبرانيا.

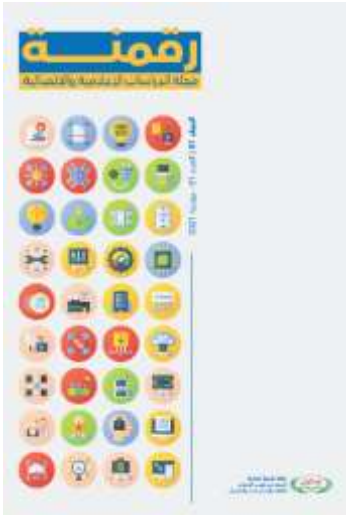
كلمات مفتاحية: الحلول الرقمية، الابتكار، الأمن السيبراني، جائحة كوفيد-19.

Abstract

The Covid-19 pandemic has led to the emergence of new patterns of cybercrime, and due to the succession of these crimes and their access to the corridors of decision-makers, various countries, including Algeria, have encouraged innovation processes and solutions offered by technological startups in the field of enhancing cybersecurity, by creating an entrepreneurial environment To create businesses and applications that are active in this field.

This study came with the aim of highlighting the most important models of pioneering emerging institutions in the field of protecting the digital environment from the risks of penetration through the innovative solutions and technologies they provide, especially in light of the rapid growth in demand for cybersecurity services and products during the Covid 19 pandemic. He pointed out that the primary role of these companies will be to focus on finding preventive and deterrent solutions for cyberattacks by creating innovative innovative products and solutions in the field of cybersecurity for the world as a whole, which opens new horizons in the Algerian market to adopt such innovations to achieve a safe future in cyberspace.

Keywords: Innovative digital solutions, cyber security, COVID-19 pandemic.



رقمنة
مجلة الدراسات الإعلامية والاتصالية

المجلد 03 | العدد 01 (خاص)
مارس 2023
الصفحات 58 - 67

ردمد | ISSN-2773-4285
EISSN | 2830-8417
الإيداع القانوني | 03/2023
العنوان | 11، طريق دودو مختار، بن عكنون، الجزائر العاصمة.
الفاكس | 50 88 23 (023)
الهاتف | 75 29 62 (0561)

تاريخ الاستلام 2022/11/29
تاريخ القبول 2022/12/22
تاريخ النشر 2023/03/18

أمينة بن زرارة
جامعة 8 ماي 1945- قالمة (الجزائر)
Benzerara.amina@univ-guelma.dz

1. مقدمة:

أظهر فيروس كورونا الحاجة الملحة إلى اعتماد الرقمنة في تقديم خدمات لمواطنين قابعين تحت الحجر الصحي، تزيل عنهم تعب التنقل وملل طرق الأبواب والطوابير. هذه الخدمات التي وإن كان بعضها موجودا، لم تستعمل بالكيفية المطلوبة التي يفرضها التطور وتحتمها العصرنة في زمن التحدي التكنولوجي. وفي هذا الإطار، أظهرت جائحة كورونا الأهمية الملحة للتكنولوجيات الرقمية مما أدى إلى تسريع وتيرة التحول الرقمي في كل مجال الخدمات وتلبية حاجيات المواطنين الإدارية والتربوية والمجتمعية وحتى الاقتصادية .

أدت جائحة كوفيد19 إلى ظهور أنماط جديدة من جرائم الأنترنيت، تتّسم بالاختراق والتسلل داخل النظم المعلوماتية، بغرض تدميرها أو نهب معلوماتها، حيث ضاعف انتقال الأعمال والدراسة والطبابة إلى العالم الافتراضي بسبب جائحة كورونا من احتمالات التعرض لهذا الخطر؛ وبسبب توالي هذه الجرائم ووصولها إلى أروقة صُنّاع القرار، دقّ ناقوس الخطر الدولي، فحشدت الدول طاقاتها ومواردها للاتحاد في سبيل مجابهة ما بات يُعرف بـ«الآفة العابرة للقارات»، أو ما يسمى «الجرائم السيبرانية، ونظرًا لاستيعابها خطورةَ المشهد، ومدى أهمية التصدي له، شجعت مختلف الدول ومن بينها الجزائر عمليات الابتكار و الحلول التي تقدمها الشركات الناشئة التكنولوجية في مجال تعزيز الأمن السيبراني، و ذلك من خلال خلق بيئة مقاولاتية لابتكار أعمال وتطبيقات تنشط في هذا المجال، في وقت تعاني فيه السوق المحلية و العالمية ومنظومة ريادة الأعمال من نقص في الأفكار والشركات الناشئة في هذا المجال خاصة مع تزايد التعاطي مع البيئة الرقمية خلال جائحة كوفيد 19، وذلك تزامنا مع التوسع في الاعتماد على تقنية المعلومات والاتصالات من قبل الناس والحكومات والقطاعات الاقتصادية كافة خلال هذه الجائحة، حيث أن الدور الأساسي لهذه الشركات سيكون بالتركيز على إيجاد الحلول الوقائية والرادعة للهجمات السيبرانية من خلال ابتكار منتجات وحلول إبداعية مبتكرة في مجال الأمن السيبراني للعالم ككل. وقد جاءت هذه الدراسة لتسليط الضوء على أهم نماذج المؤسسات الناشئة الرائدة في مجال حماية البيئة الرقمية من مخاطر الاختراق من خلال ما تقدمه من حلول و تقنيات مبتكرة خاصة في ظل النمو السريع في الطلب على خدمات ومنتجات الأمن السيبراني خلال جائحة كوفيد 19 نظراً لازدياد استخدام تقنية المعلومات والاتصالات خلال هذه الجائحة، ولكون الأمن السيبراني متطلباً أساسياً لهذه التقنية وركيزة أساسية في تفعيلها، و الذي يفتح آفاقا جديدة في السوق الجزائرية لتبني مثل هذه المبتكرات لتحقيق مستقبل آمن سيبرانيا **(القحطاني، 2018، ص ص 19-20).**

2. طبيعة تأثير جائحة "كوفيد-19" على الخصوصية و الأمن السيبراني:

إن وباء "كوفيد-19" فاقم من التحديات الأمنية المرتبطة بالأمن السيبراني مع تزايد خطر القرصنة التي تستهدف الاشخاص والدول، خاصة أن قراصنة الإنترنت اليوم باتوا على درجة عالية من التأهيل والخبرة، وبعضهم مدعوم من دول، ما يجعل القرصنة تهديداً كبيراً للأمن السيبراني. مشيراً إلى أن المؤسسات تركز على البنية التحتية للأمن السيبراني، ولكن التكنولوجيا وحدها لا تكفي، فأهم سلاح لتحقيق الأمن السيبراني هو نشر الوعي العام بالأدوات التي تستخدم لإقناع بعض الأشخاص للكشف عن المعلومات الحساسة.

لذا يجب التشديد على أهمية توفير بيئة معلوماتية آمنة لعمل المؤسسات والشركات وتأمين الأنظمة التي تمكّن الوصول عن بُعد وزيادة الوعي بالاستخدام الآمن لهذه الأنظمة، وتوفير المتطلبات الآمنة للعمل عن بعد في المنزل، مثل تحديث البرمجيات الخاصة بالحاسوب المنزلي، وعدم الضغط على أي رابط مجهول من دون تفكير، وحماية الأجهزة الإلكترونية الخاصة بالفرد، واستخدام كلمة سر قوية يصعب التعرف عليها، وترميز الرسائل الإلكترونية بحيث تصبح غير مقروءة إلا للجهة المرسل إليها بعد حصولها على كلمة سر.

إن الجرائم السيبرانية تشكل أكبر تهديد للأمن العالمي وأنها تكلف العالم ما يزيد عن 6 تريليون دولار سنوياً، موضحاً أن وباء "كوفيد-19" أتاح فرصة لقراصنة الإنترنت لكي يستغلوا ضعف الناس وبحثهم عن المعلومات ليرسلوا إليهم رسائل تعرضهم للابتزاز والتهديد، وبالفعل فقد تزايدت التهديدات التي طالت المؤسسات المالية والأفراد والمؤسسات الحكومية في الآونة الأخيرة، وباتت الشركات والمؤسسات الصغيرة هي الأكثر تضررًا من تفاقم مخاطر الأمن السيبراني بسبب ضعف أنظمة الحماية فيها.

إن الأمن السيبراني الكامل غير موجود، لأن مجرمو الإنترنت يعملون باستمرار على تطوير أساليبهم في شن هجماتهم والاستفادة من أي ثغرات موجودة، إن عدم حماية رسائل البريد الإلكتروني يمثل أحد الأخطاء القاتلة في منظومة الأمن السيبراني. وأكد على ضرورة تجديد برمجيات الحاسوب المنزلي لتكون أكثر أمناً **(عراجي، 2019،ص ص 23-24).**

3. الإرهاب السيبراني والهجمات السيبرانية:

تختلف الجرائم السيبرانية كثيراً عن الجرائم التقليدية من حيث طبيعتها ونطاقها ووسائلها وأدلتها. فقد أدى التطور السريع في مجال تقنية المعلومات والاتصالات وشبكة الإنترنت إلى ظهور أنماط جديدة من الجرائم جاءت عن طريق الاستغلال السيئ للتكنولوجيا، مما ترتب عليه خلق ظاهرة إجرامية جديدة تتم عن طريق هجمات واختراقات وتسلل داخل النظم المعلوماتية أما بغرض تدمير تلك النظم أو الحصول على معلومات سرية سواء عسكرية أو اقتصادية، الأمر الذي ينبه بوجود مخاطر على الصعيد الدولي والوطني، فلابد من إيجاد سبل للتصدي لهذه الظاهرة.

والهجمات السيبرانية هي هجمات يتم تنفيذها بواسطة أجهزة الحاسوب عبر شبكات الانترنت والاتصالات الرقمية بهدف تغيير أو تعطيل برامج أو تدمير معطيات أو سرقة معلومات أو اختراق انظمة التحكم والأوامر، والعمل على إحداث أضرار في أنظمة وبرامج وأجهزة الطرف الآخر وتعطيلها عن العمل، وغالباً ما تستهدف هذه الهجمات البنية التحتية للدول، ومحاولة إحداث أكبر الأضرار بها، وإصابتها بالشلل التام، كي تعجز عن تقديم الخدمات للسكان.

وتتنوع الأدوات التي يتم من خلالها تنفيذ الهجمات السيبرانية، حيث تشمل الفيروسات أو "الديدان الإلكترونية "، والتطبيقات السرية المعروفة تحت مسمى "الأبواب الخلفية" أو برامج "حجب الخدمة" وغيرها من البرمجيات الفيروسية التي تستهدف زعزعة أو شل الهدف أياً كان، سواء أكانت فرداً أم مجموعة من الأفراد أم منظمة أم شركة أم وكالة حكومية أو جه رسمية **(السيد، 2020).**

وتتنوع الجهات التي تقف وراء ظاهرة تنامي الهجمات السيبرانية على الصعيد العالمي في الآونة الأخيرة، وتشمل ما يلي(عبد الجابر، 2014، ص 87)

- الدول، التي تمتلك قدرات تقنية وتكنولوجية متطورة تتيح لها توظيفها في القيام بهجمات سيبرانية في مواجهة خصومها سواء لأغراض عسكرية (تدمير منشآت – وقف مشروعات) أو تجسسية كالحصول على معلومات أو إحداث تدمير في البنية التحتية الأساسية، كشبكات الكهرباء والمياه والمواصلات والاتصالات.
- عصابات الجريمة المنظمة، والتي غالباً ما تلجأ إلى الهجمات السيبرانية للحصول على فدية مالية، وتلجأ في ذلك إلى اختراق أنظمة المعلومات التي تدير الخدمات الأساسية في بعض الدول، لمساومتها للحصول على مبالغ مالية.
- القراصنة من الأشخاص العاديين والذين يمتلكون مهارات تقنية فائقة، يتم توظيفها في الحصول على مبالغ مالية أو في اختراق الأمن المعلوماتي للدول، والحصول على معلومات حساسة عن قضايا السياسة الخارجية للدول، على النحو الذي جسدته ظاهرة» ويكليكس»، حينما حيث استطاع جوليان أسانج أن يكشف العديد من أسرار السياسة الخارجية الأمريكية وعلاقات الولايات المتحدة مع العديد من القوى الكبرى.

4. كيفية تعزيز الأمن السيبراني في ظل تجربة "كوفيد-19:

يشكل الأمن السيبراني جزءاً أساسياً من أي سياسة أمنية وطنية، حيث بات معلوماً أن صناع القرار في الولايات المتحدة الأمريكية، الاتحاد الأوروبي، روسيا، الصين، الهند وغيرها من الدول، أصبحوا يصنفون مسائل الدفاع السيبراني/الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية. بالإضافة إلى ما تقدم، فقد أعلنت أكثر من 130 دولة حول العالم عن تخصيص أقساماً وسيناريوهات خاصة بالحرب السيبرانية ضمن فرق الأمن الوطني. تضاف جميع هذه الجهود إلى الجهود الأمنية التقليدية لمحاربة الجرائم الالكترونية، الاحتيال الالكتروني والأوجه الأخرى للمخاطر السيبرانية**(مليايي،2019ن ص 45.)**

و على صعيد الاشخاص، يتوجب تدريب العاملين والموظفين على أساليب العمل عن بُعد الآمنة، وزيادة التوعية بخطر القرصنة الإلكترونية لمن يعملون من المنازل حتى لا يعرضوا مؤسساتهم لمخاطر القرصنة، والتحديث المستمر لأنظمة الحماية والأجهزة المستخدمة من قبل الأفراد والمؤسسات، وضرورة العمل على توفير بيئة معلوماتية آمنة لعمل المؤسسات والشركات، ووضع التشريعات والقوانين التي تضمن الأمن السيبراني، وضرورة رفع الوعي العام بالجريمة السيبرانية بين جميع العاملين بالمؤسسات الخاصة والعامة، بالإضافة إلى توفير التكنولوجيا اللازمة لتحقيق الأمن السيبراني **(عبد اله، 2021، ص ص 67-68).**

5. أفضل 20 شركة ناشئة للأمن السيبراني لسنة 2020:

يوجد اليوم حوالي 21،729 شركة ناشئة تتنافس أو تعتمد على تقنيات وحلول الأمن السيبراني كجزء أساسي من نماذج أعمالها، وقد تلقى 1،653 منها تمويلًا أوليًا في الأشهر الـ 12 الماضية. وفقًا لاستعلام Crunchbase الأخير(https://techcrunch.com/2022/02/09/vc-cybersecurity-startups-record-year/)، تم استثمار ما يقرب من 10 مليار دولار في شركات الخصوصية والأمن في عام 2019، وهو أعلى مستوى على الإطلاق في العقد الماضي وأكثر من خمسة أضعاف من 1.7 مليار دولار في عام 2010. من الأمن الإلكتروني وأمن البيانات إلى حوكمة تكنولوجيا المعلومات وقياس المخاطر والامتثال للسياسة، وفقًا لتقرير الأمن السيبراني اتجاهات Insight's Emerging Trends ، بحلول عام 2025، يعد الأمن السيبراني صناعة متنامية بقيمة تقديرية تزيد عن 300 مليار دولار. تتوقع C.B. Insights أنه بحلول عام 2025، من المتوقع أن يصل سوق إدارة الهوية والوصول العالمي (IAM) إلى 23 مليار دولار.

في عام 2020، وفقًا لاستعلام Crunchbase الأخير، قامت 268 شركة ناشئة بجمع إجمالي 4.7 مليار دولار أمريكي، بمتوسط 21 مليون دولار أمريكي لكل منها، وتمويل متوسط قدره 6.1 مليون دولار أمريكي. من المتوقع أن ينمو إنفاق المستخدم النهائي لأمن المعلومات وإدارة المخاطر على الصعيد العالمي بمعدل سنوي مركب نسبته 9.2٪ في عام 2022 وسيصل إلى 174.5 مليار دولار أمريكي بحلول عام 2022. يرتبط النمو الجديد في الإنفاق بالتحول الرقمي والامتثال التنظيمي وزيادة التهديدات الأمنية والاستجابة وفقًا لأحدث تقديرات السوق لشركة .Gartner نظرًا لأن استثمارات الأمن السيبراني يُنظر إليها على أنها طرق لحل عدم اليقين والمحاولات التخريبية للارتفاع بشكل حاد، فإن الأساليب الجديدة ذات الطبيعة الأكثر تعقيدًا، تستمر الشركات الناشئة في جذب المستثمرين.

بناءً على قياس متساوٍ لقدرة الشركة الناشئة على جذب عملاء جدد، ونمو الإيرادات الحالية والمتوقعة، والقدرة على تكييف حلولها مع الصناعة المتطورة والموقع في السوق المختارة، تجدر الإشارة إلى ما يلي في 2020، 20 أفضل شركات الأمن السيبراني:

:Beyond Identity

استبدلت التكنولوجيا الخاصة خارج Beyond Identity الآن العملات المشفرة بشهادات X.509 المستندة إلى جميع أنحاء المؤسسة. تنشئ هذه الطريقة التي تنتظر الحصول على براءة اختراع سلسلة طويلة من إطار الثقة الذي يهدف بدء التشغيل إلى تضمينه لتحديد هوية المستخدم والجهاز، ولقطات في الوقت الفعلي لحالة أمان الجهاز من أجل المصادقة والتفويض التكيفي المستند إلى المخاطر. تتيح الحلول السحابية الأصلية التي تتجاوز الهويات للعملاء زيادة سرعة الأعمال، وتنفيذ نماذج أعمال جديدة، وخفض تكاليف التشغيل، وتنفيذ إدارة كاملة للهوية بدون عملة مشفرة. جمعت Beyond Identity إجمالي 30 مليون دولار من التمويل في جولة واحدة من التمويل**(الموقع الرسمي لشركةBeyond Identityt ،2020)**

:Confluera-Confluera

هي شركة ناشئة للأمن السيبراني تساعد المؤسسات على اكتشاف الهجمات الأمنية المعقدة التي تتم داخل البنية التحتية للمؤسسة. تستخدم الشركة الناشئة "الرسوم البيانية للهجوم المستمر" لحظر التهديدات السيبرانية ومعالجتها بشكل نهائي في الوقت الفعلي، وبالتالي توفير تتبع تسلسلي مستقل للقرصنة واستجابة عبر البنية التحتية بأكملها. وهي مصممة لكشف ومنع المهاجمين من تصفح البنية التحتية على وجه اليقين. تجمع تكنولوجيا Confluera بين الكشف الشامل عن التهديدات في الماكينة ومسارات الأنشطة التي يتم تتبعها بدقة لإيقاف الهجمات السيبرانية في الوقت الفعلي، وبالتالي تمكين الشركة من تبسيط العمليات الأمنية بشكل أساسي. إنه يمنح أفراد الأمن البشري مزيدًا من الوقت للتركيز على المهام الأكثر أهمية دون الحاجة إلى قضاء ساعات في محاولة إرباك الآلاف من التنبيهات التي يتم تلقيها يوميًا، وكثير منها إيجابيات خاطئة. جمعت كونفلويرا ما مجموعه 29 مليون دولار في جولتين من التمويل.

:Cryptoloc Technology Group-Cryptoloc

هي شركة أسترالية للأمن السيبراني حصلت على شهادة ISO 27001: 2013 وتم تأسيسها في بريسبان في عام 2010. تتميز هذه الشركة الناشئة بكيفية تطويرها والتقدم للحصول على براءات اختراع وتأمينها لتكنولوجيا العملة المشفرة عالية الأمان التي يمكن نشرها في أربعة منتجات. تتضمن هذه المنتجات نظامًا أساسيًا لتخزين مستندات B2C يسمى "ملفك الرقمي"، وما يعادله من الملصق الأبيض B2B يسمىVault ، وواجهة برمجة تطبيقات آمنة لتوقيع المستندات، وحلول لمكافحة التزييف وتتبع المنتج. في عام 2020، افتتحت الشركة الناشئة مقرًا إقليميًا جديدًا. خدمة السوق الأوروبية في كامبريدج والتخطيط لتوظيف ما يصل إلى 50 موظفًا في السنوات الثلاث المقبلة لدعم العمليات الأوروبية للشركة **(الموقع الرسمي لشركة كريبتولوك،2019)**

:Cyble

تتمثل مهمة .Cyble Inc في تزويد المؤسسات برؤية في الوقت الفعلي عن التهديدات والمخاطر السيبرانية في سلسلة الإمداد. توفر حلول SaaS المستندة إلى التعلم الآلي والتحليل اليدوي للمؤسسات رؤى حول التهديدات السيبرانية التي يقدمها الموردون. أنها

تمكنهم من الاستجابة لهم بشكل أسرع وأكثر فعالية. تسعى Cyble جاهدة لتكون شريكًا / مزود خدمة موثوقًا به للعملاء، حيث توفر معلومات الشبكة التي يتم الحصول عليها من خلال القنوات المفتوحة والمغلقة (مثلOSINT ، والويب الداكن، والمراقبة العميقة للويب، والفحص السلبي لحالة الإنترنت) لتزويد العملاء بنتيجة أمان غير مسبوقة للمورد. بالإضافة إلى ذلك، فإن الذكاء الذي يجمع بين التعلم الآلي وقدرات التحليل البشري يمكّن العملاء أيضًا من الحصول على ذكاء التهديدات السيبرانية في الوقت الحقيقي والمساعدة في بناء قدرات أفضل وأقوى لتحمل نقاط الضعف في الشبكة والمتسللين. نظرًا لطبيعة البيانات التي تم جمعها، توفر الشركة أيضًا للمشتركين قدرات استخباراتية جاهزة للتهديدات.

:Cmd – Cmd

تم إنشاء Cmd – Cmd في أوائل عام 2016 للسماح للمؤسسات بمراقبة تفاعل المستخدم والتحكم فيه بسهولة في بيئة .Linux توفر منصة Cmd رؤية كاملة وحماية ما قبل التنفيذ في الوقت الفعلي دون تدخل بشري Cmd .هي أول شركة تصمم منتجها الأساسي، والذي يمكن أن يساعد CIO و CTO وفرق الأمن على تسجيل سلوك المستخدم وفهمه والتنبؤ به والتحكم فيه في بيئة .Linuxيعتقد فريق Cmd أنه لا يمكن للمنظمات التنبؤ بسلوك المستخدم والتحكم فيه بثقة قبل تحديد مقياس الأداء "الطبيعي" الخاص بها. من خلال هذا الفهم، يمكن للمؤسسات استخدام Cmd لبناء سياسات تقيد الوصول إلى الملف، والمصادقة الفورية، وحتى منع التنفيذ المسبق للأوامر الخطرة. "ولد Cmd من النكسات المؤلمة التي واجهناها كحراس أمن يحمون لينكس. علمنا أنه يجب أن تكون هناك طريقة أفضل. لذلك بدأنا في تطويرها: حلول سهلة الاستخدام ويمكن الوصول إليها تكون معقولة لفريق DevOps الحديث قال الرئيس التنفيذي والمؤسس المشارك جيك كينغ: اركض في السحابة. جمعت Cmd ما مجموعه 21.6 مليون دولار في جولتين من التمويل.

:Darktrace

يعتمد Darktrace على الذكاء الاصطناعي ومجموعة من علماء الرياضيات باستمرار لتحسين 0 وتحسين نظام المناعة في الشركة. يعتمد نظام المناعة على الخوارزميات التي يستخدمها التعلم الآلي والذكاء الاصطناعي للكشف عن التهديدات السيبرانية والاستجابة لها في مجموعة متنوعة من البيئات الرقمية، بما في ذلك الشبكات السحابية والافتراضية، وإنترنت الأشياء، وأنظمة التحكم الصناعية. التكنولوجيا هي التعلم الذاتي ولا تتطلب أي إعدادات لتحديد التهديدات في الوقت الحقيقي وتحديث فهمها مع تغير البيئة. من خلال تطبيق تعلُّم الآلة الفريد الخاص بها، حددت63 Darktrace ، 500 تهديدًا لم تكن معروفة من قبل في أكثر من 5000 شبكة، بما في ذلك الاختلافات في اليوم صفر والتهديدات الداخلية والهجمات الخفية الدقيقة. لدى Darktrace 620 موظفًا في 32 مكتبًا ومقرًا مزدوجًا في سان فرانسيسكو وكامبريدج، المملكة المتحدة، وحصلت على جوائز "أفضل شركة أمن مبتكرة لعام 2017" و "Bloomberg Innovator" و ."GSN Homeland Security" تبلغ قيمة الشركة 825 مليون دولار، ويشمل مستثمروها Invoke Capital و Talis Capital و Hoxton Ventures و Summit Partners و KKR و Softbank و TenEleven و Samsung Ventures و.Insight Venture Partners

:Dathena Science

الغرض من إنشاء Dathena Science هو تحقيق رؤية اعتماد طريقة جديدة لتمكين الشركات من الحصول على قدر أكبر من الخصوصية وحماية أمن البيانات. تواجه الشركات في جميع أنحاء العالم تحديات خطيرة، أي استخدام البيانات وإدارتها والتحكم فيها في بيئة أكثر تنظيماً، كما أن توقعات المجتمع لحماية الخصوصية في تزايد. باستخدام أحدث تقنيات الطاقة منAI ، توفر Dathenaحلول إنتاج ضخمة للعملاء من الشركات. جمعت Dathena Science ما مجموعه 12 مليون دولار في ثلاث جولات من التمويل. تم جمع أموالهم الأخيرة من جولة التمويل في 13 مايو 2020.

:Druva –Druva

تعتبر فريدة من نوعها من حيث أنها تستطيع تطوير وإطلاق وتنفيذ بيانات النسخ الاحتياطي للمؤسسات القائمة على AWS بشكل فعال عبر مراكز البيانات والسحابات وأحمال عمل نقطة النهاية. تحرر بنية وسعر منصة Druva السحابية العملاء من

الأجهزة غير الضرورية وتخطيط السعة وأعباء إدارة البرامج، وبالتالي تقليل تكاليف النسخ الاحتياطي بنسبة 50٪. لدى Druva حاليًا أكثر من 4000 عميل وهي شركة خاصة مقرها في سانيفيل، كاليفورنيا، بتمويل من Sequoia Capital و Virgin Global Investmentsو Tenaya Capital و Riverwood Capital و Nexus Partners.

: ExtraHop-ExtraHop

الكشف عن الشبكة الأصلية والاستجابة لها لضمان سلامة المؤسسات المختلطة. يطبق نهجنا المبتكر التعلم الآلي المتقدم على كل حركة مرور الشبكة والشبكة لتوفير رؤية هجينة متعددة السحابة المتعددة واكتشاف التهديدات في الوقت الحقيقي والاستجابة الذكية. وبهذه الطريقة، نقدم للشركات العالمية الرائدة بما في ذلك Home Depot و Credit Suisse و Caesars Entertainment وجهة نظر مفادها أنها تحتاج إلى تجاوز الضوضاء لاكتشاف التهديدات، وضمان توفر التطبيقات المهمة وضمان استثمارها في السحابة. جمعت ExtraHop ما مجموعه 61.6 مليون دولار أمريكي في خمس جولات من التمويل.

:ForgeRock-ForgeRock

آفاقٌ جديدة في إدارة الهوية الرقمية وكيف يمكن للمؤسسات التفاعل بشكل آمن مع العملاء والموظفين والأجهزة والأشياء. تستخدم المنظمة منصة الهوية ForgeRock كنظام هوية رقمي مسجل للاستفادة من علاقات العملاء، وحل قواعد الخصوصية والموافقة الصارمةGDPR) ، HIPAA، خصوصيةFCC ، إلخ) والاستفادة من إنترنت الأشياء. تقدم ForgeRock خدمات للعديد من الشركات، بما في ذلك Morningstar و Vodafone و GEICO و Toyota و TomTom و Pearson وحكومات مثل النرويج وكندا وبلجيكا، مما يضمن مليارات الهويات في جميع أنحاء العالم. لدى ForgeRock مكاتب في أوروبا والولايات المتحدة وآسيا.

:HUB Security-HUB Security

متخصص في توفير حلول أمان الأجهزة للوائح والخصوصية والتكنولوجيا المالية والسحابة و .blockchain تقوم الشركة الناشئة أيضًا بتطوير الهوية العسكرية وحلول إدارة المفاتيح التي تركز على الخدمات المالية والخدمات السحابية مع أجهزة تسريع العملات الرقمية المتشابهة وأمن التصميم Fips140-2 المستوى 4. تم دمج منصة HSM لتطبيقات السحابة والتمويل و blockchain في البنوك والمؤسسات المالية السويسرية.

:Kentik

إن قدرة Kentik على إنشاء وتعديل وتوسيع منصات استخبارات الشبكة للمؤسسات لاكتشاف تغطية سياسة أمان الشبكة تستحق الاهتمام. مع Kentik ، يمكن للشركات القضاء على فجوات الرؤية والذكاء المرتبطة بتشغيل الشبكات الديناميكية والمعقدة، والحصول على أداء شبكة وموثوقية وأمان أعلى. تدمج منصة ذكاء شبكة Kentik وتحلل تدفقات البيانات المختلفة من الإنترنت، والحافة، والسحابة، ومركز البيانات، والبنية التحتية المختلطة، وتوفر التصور في الوقت الحقيقي والرؤى والأتمتة المدعومة من.AIOps

:Liongard-Liongard

هي شركة تكنولوجيا معلومات متخصصة في توفير أتمتة IT وخدمات الاستضافة والوثائق الآلية. يحتوي على منصة تطبيق برمجية تمكن الشركات والمؤسسات وفرق الإدارة التنظيمية من تسجيل لقطات يومية لبيانات التكوين الغنية للسحب والشبكات والأنظمة المحلية والتقاطها. تأسست الشركة في عام 2015 ومقرها الرئيسي في هيوستن، تكساس. جمع Liongard ما مجموعه 22.8 مليون دولار أمريكي في ثلاث جولات من التمويل.

:Ontic-Ontic

عبارة عن منصة برمجية ذكية واقية لتوحيد البيانات التاريخية والبيانات التاريخية المتعلقة بتهديدات الأمان المادي وسلوكيات التهديد المحتملة. تدعم منصتهم التعاون عبر عمليات سير العمل المتصلة، حتى تتمكن فرق الأمن من الحصول على معلومات استخبارية أكثر صلة بشكل أسرع للكشف المبكر عن التهديدات. تمكن رؤى أونيتك الآلية والذكاء والقابلة للتنفيذ سلامة الشركة

وقادة المدارس من تحديد المؤشرات المسبقة بشكل أفضل وتقييم المخاطر وتخفيف التهديدات المحتملة لحماية الموظفين والمنشآت والطلاب والمدارس. جمعت Ontic ما مجموعه 16.7 مليون دولار في جولتين من التمويل.

:RiskIQ-RiskIQ

توفر للمنظمات الرؤية والذكاء اللذين تحتاجهما لحماية بصمة الشركات الرقمية الخاصة بهم وتعيين البنية التحتية لخصومهم. تمكّن منتجات RiskIQ المدعومة بتكنولوجيا المستخدم الافتراضي المملوكة ومحركات تحليل التهديدات وشبكات الوكلاء العالمية المؤسسات من الدفاع ضد التهديدات ضد مواقع الويب وتطبيقات الهاتف المحمول والعلامات التجارية والعملاء والموظفين. تستخدم ثماني من أفضل عشر مؤسسات مالية في الولايات المتحدةRiskIQ ، وتستخدم خمس من تسع شركات إنترنت رائدة في العالم .RiskIQ يقع المقر الرئيسي للشركة في سان فرانسيسكو وبدعم من Battery Ventures و.Summit Partners

:SafeBreach-SafeBreach

هي شركة رائدة في الفئة الناشئة من محاكاة الأضرار والهجوم. توفر المنصة الخارقة للشركة "منظور الهاكر" حول الوضع الأمني للمؤسسة، بحيث يمكنها التنبؤ بشكل استباقي بالهجمات والتحقق من الضوابط الأمنية وتحسين استجابة محللي شركة نفط الجنوب. سيستخدم SafeBreach دليل Play Hacker الواسع والمتزايد (البحث وبيانات الاستطلاع الفعلية) لفرض الانتهاكات تلقائيًا. يتم تمويل SafeBreach من قبل Sequoia Capital و Deutsche Telekom Capital و HP Pathfinder والمستثمر شلومو كرامر.

:Secret Octopus-Secret Double Octopus

طور تقنية المصادقة بدون مفتاح الوحيدة في العالم والتي لا يمكن تشفيرها والتي يمكنها حماية الهوية والبيانات عبر بيئة السحابة والجوّال وإنترنت الأشياء. استنادًا إلى خوارزمية المشاركة السرية التي تم تطويرها في الأصل لحماية رمز الإطلاق النووي، تمنع تقنية الأخطبوط المزدوج السرية المهاجمين السيبرانيين من الوصول إلى معلومات حرجة كافية للهجوم، وبالتالي القضاء على العنف والتلاعب في الوسط والتلاعب بمفاتيح البنية التحتية وسرقة المفاتيح وإصدار الشهادات نقاط الضعف المؤسسية. جمع Secret Double Octopusما مجموعه 22.5 مليون دولار في ثلاث جولات من التمويل.

:Semperis-Semperis

هي شركة لحماية هوية المؤسسة تمكّن المؤسسات من التعافي بسرعة من التغييرات والكوارث غير المتوقعة أو الضارة التي تهدد Active Directoryوالمحلية والسحابية. يوفر النظام الأساسي لحماية خدمات Semperis للمؤسسات الوظائف التالية: استعادة مجموعة الغابة Active Directory تلقائيًا، واستعادة الآلاف من الكائنات أو سمات المفتاح الفردي بسرعة، والاستعادة فورًا إلى حالة Active Directory السابقة. يشمل عملاء Semperis شركات وشركات Fortune 500 في المجالات المالية والرعاية الصحية والحكومة وغيرها من الصناعات في جميع أنحاء العالم. جمعت Semperis ما مجموعه 40 مليون دولار في ست جولات من التمويل.

مصدر الدفاع – ما يجعل دفاع المصدر جديرًا بالاهتمام هو أسلوبه الفريد الذي يمكن أن يمنع الهجمات على مواقع الويب وموارد الوسائط عبر الإنترنت من مصادر خارجية. يسمح النظام الأساسي القائم على SaaS لمالكي المواقع بتعيين الأذونات وفرضها، وتلقي تنبيهات في الوقت الفعلي، ومراقبة سلوك موردي الجهات الخارجية في الوقت الفعلي. من خلال القضاء على الاعتبارات الأمنية من تكامل الجهات الخارجية، يلغي Source Defense الوقت الذي يقضيه في الاختبار والتكامل، مما يسمح للموقع بالتركيز على توليد الإيرادات والفرص الجديدة، مع الحفاظ على سلامة زوار الموقع والأداء العالي للموقع. جمعت Source Defense ما مجموعه 20.5 مليون دولار في ثلاث جولات من التمويل.

:Zero Network

الميزة الفريدة لشبكة Zero هي كيفية تطويرها وتنفيذها تلقائيًا لقواعد الوصول إلى الشبكة عبر الشبكة. تقوم تقنيتها بتخصيص من يمكنه الوصول إلى موارد محددة في الشبكة من خلال معرفة كيفية تواصل المستخدمين مع أجهزة الكمبيوتر. توفر Zero

Networkآلية تجاوز من خلال جدار المصادقة الثنائي العامل على هاتف جوال المستخدم للتأكد من أنها لا تؤثر على الاتصالات غير الطبيعية ولكنها مشروعة. تأسست Zero Networks في عام 2019 ومقرها في تل أبيب، إسرائيل.

6. خاتمة:

يعد الأمن السيبراني واحداً من أهم القطاعات التقنية اليوم في العالم وأسرعها نمواً على مستوى العالم؛ حيث من المتوقع أنه يكون هناك نمو سريع في الطلب على خدمات ومنتجات الأمن السيبراني نظراً لازدياد استخدام تقنية المعلومات والاتصالات ولكون الأمن السيبراني متطلباً أساسياً لهذه التقنية وركيزة أساسية في تفعيلها. كان لا بد من تشجيع الحلول الابتكارية لدعم نمو صناعة الأمن السيبراني والارتقاء بمستواها من خلال دعم تأسيس شركات ناشئة وواعدة في هذا المجال بما يسهم بالنمو الاقتصادي لتبادل الحلول والأفكار بين المختصين ومواكبة تلك التحديات.

7. قائمة المراجع:

- **المؤلفات:**

1- القحطاني، ذيب (2018)، أمن المعلومات، المملكة العربية السعودية، مدينة الملك بن عبد العزيز للعلوم و التقنية.
2- عراجي، انديرا(2019)، الحروب السيبرانية، فصل عصري من التحدي والإستجابة، لبنان، دار ميرزا للنشر و التوزيع.
3- عبد الإله، عثمان عبد الرحمان (2021)، الحسبة على جرائم الأمن السيبراني، السودان، جا تاون للنشر و التوزيع.

- **الأطروحات:**

4- مليايني، عبد الوهاب (2019)، أمن المعلومات في بيئة الاعمال الإلكترونية، أطروحة دكتوراه، كلية الحقوق و العلوم السياسية، جامعة ابي بكر بلقايد، تلمسان، الجزائر.
5- عبد الجابر، يوسف خليل (2014)، مدى فاعلية إجراءات الرقابة الداخلية في توفير أمن المعلومات الإلكترونية في الشركات الصناعية الأردنية، رسالة ماجستير، قسم المحاسبة والتمويل– كلية الأعمال جامعة الشرق الأوسط، الأردن.

- **مو اقع الإنترنيت:**

6- داليا السيد، الهجمات السيبرانية .. تهديد متعاظم للأمن والاستقرار والاقتصاد العالمي***(2020)***، على الرابط التالي: **http://www.nationshield.ae/index.php/home/details/research**، فحص بتاريخ 2022/11/17.
7- **https://techcrunch.com/2022/02/09/vc-cybersecurity-startups-record-year/**
8- الموقع الرسمي لشركة(2020)**Beyond Identity** على الرابط لتالي: **https://www.beyondidentity.com**، فحص بتاريخ 2022/10/29.
9- الموقع الرسمي لشركة كريبتولوك(2019) على الرابط التالي: **https://cryptoloc.com/**، فحص بتاريخ 2022/11/11.