بسم الله الرحمن الرحيم

التهديد الداخلي
مَنْعه، وكَشْفه، ورَدْعه، والحدُّ منه

تأليف

Michael G. Gelles

ترجمة

د/ راكان بن عبد الله السويل

أستاذ مساعد في تقنية وأمن المعلومات

جامعة الملك سعود

دار جامعة الملك سعود للنشر
KING SAUD UNIVERSITY PRESS

ص.ب ٦٨٩٥٣ - الرياض ١١٥٣٧ المملكة العربية السعودية

ⓒ دار جامعة الملك سعود للنشر، ١٤٤٣هـ (٢٠٢٢م)

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

جيليس، مايكل ج.

التهديد الداخلي: مَنْعه، وكَشْفه، ورَدْعه، والحدُّ منه./ مايكل ج. جيليس؛ راكان عبدالله السويل.- الرياض، ١٤٤٣هـ.

٢٦٢ ص؛ ١٩سم × ٢٣,٥ سم

ردمك: ١- ٠٢٨ - ٥١٠ - ٦٠٣ - ٩٧٨

١- أمن المعلومات أ. السويل، راكان عبدالله (مترجم) ب. العنوان

ديوي ٠٠٥,٨ ١٤٤٣/٥١٩٦

رقم الإيداع: ١٤٤٣/٥١٩٦

ردمك: ١ - ٠٢٨ - ٥١٠ - ٦٠٣ - ٩٧٨

هذه ترجمة عربية محكمة صادرة عن مركز الترجمة بالجامعة لكتاب:

Insider Threat: Prevention, Detection, Mitigation, and Deterrence
By: Michael G. Gelles
© Elsevier Inc., 2016

وقد وافق المجلس العلمي على نشرها في اجتماعه الثاني للعام الدراسي ١٤٤٣هـ، المعقود بتاريخ ٧/ ٢/ ١٤٤٣هـ، الموافق ١٤/ ٩/ ٢٠٢١م.

جميع حقوق النشر محفوظة. لا يسمح بإعادة نشر أي جزء من الكتاب بأي شكل وبأي وسيلة سواء كانت إلكترونية أو آلية بما في ذلك التصوير والتسجيل أو الإدخال في أي نظام حفظ معلومات أو استعادتها بدون الحصول على موافقة كتابية من دار جامعة الملك سعود للنشر.

دار جامعة الملك سعود للنشر
KING SAUD UNIVERSITY PRESS

مقدِّمة المترجم

تعود أهمية أمن المعلومات إلى الاعتماد الكبير على المعلومات في الاتصال والتجارة والكثير من الأنشطة، ويُقدِّر الخبراء عدد ضحايا الجرائم الإلكترونية في العالم بأكثر من ١,٨ مليون ضحية يوميًّا، في حين بلغ الإنفاق العالمي على قطاع أمن المعلومات عام ٢٠١٦ مبلغ ٨٢ بليون دولار تقريبًا، في ظل زيادة مخاطر الهجمات الإلكترونية تتكبَّد الشركات والحكومات خسائر مالية ومعنوية كبيرة، لذلك تُنفق المؤسسات العامة والخاصة أموالًا كبيرة لاستخدام منتجات قوية لحماية شبكاتها وأنظمتها من أي هجمات، إن أساليب الهجمات الإلكترونية تتطوَّر يومًا بعد يوم كلما تطوَّرت تكنولوجيا المعلومات، وتتعدَّد بطرق جديدة ومعاصرة، إن أمن المعلومات بات اليوم يمثل تحديًا جديًّا ليس فقط للدول، بل للأفراد وقطاع الأعمال جرَّاء تنامي مظاهر التهديدات والحروب الإلكترونية التي تستمر وتزداد شراسة في كل يوم، وتعتبر المملكة العربية السعودية من أكثر الدول عُرضةً للهجمات الإلكترونية على مستوى العالم بحسب التقارير الدولية المتخصصة، مثل تعرض شركة "أرامكو السعودية" في عام ٢٠١٢م لفيروس إلكتروني أثر على قرابة ٣٠ ألف جهاز كمبيوتر، إن التهديدات الداخلية الناجمة عن الموظفين تعتبر أخطر من التهديدات الخارجية، وإدراكًا منا لأهمية زيادة ونشر الوعي بأمن المعلومات في المجتمعات العربية قمنا بترجمة كتاب بعنوان "منع التهديدات الداخلية ورَدْعها وكشفها والحد منها"، يوضِّح هذا الكتاب مسار تطوير برامج الحماية من التهديدات الداخلية في أي منظمة خطوة بخطوة، مع التركيز على إدارة ومشاركة الموظفين والجوانب الأخلاقية والقانونية، والخصوصية. يتضمَّن الكتاب أساليب وتكتيكات حول كيفية جَمْع مؤشرات المخاطر المحتملة، ورَبْطها وتصوُّرها في نظام قوي لحماية الأصول الهامة للمنظمات والشركات من التهديدات الداخلية.

أتقدم بالشكر الجزيل للأستاذ/ طاهر علي الشهاري الذي قام بمراجعة وتدقيق هذا الكتاب وساهَم في إخراجه.

د/ راكان عبد الله السويل
عضو هيئة التدريس بجامعة الملك سعود

نبذة عن ديلويت (Deloitte)

تعود شركة ديلويت إلى شركة أو أكثر من شركة ديلويت توش توهمتسو المحدودة (Deloitte Touche Tohmatsu Limited)، وهي شركة خاصة في المملكة المتحدة مقيَّدة بضمان، ولها شبكة من الشركات الأعضاء، ولكل منها كيان مستقل منفصل قانونيًّا. يرجى زيارة الموقع www.deloitte.com/about للحصول على وصف تفصيلي للهيكل القانوني لشركة ديلويت توش توهمتسو المحدودة وشركاتها الأعضاء، يرجى الاطلاع على الموقع www.deloitte.com/us/ للحصول على وصف تفصيلي للهيكل القانوني لشركة ديلويت إل إل بي (Deloitte LLP) والشركات التابعة لها، قد لا تتوفَّر بعض الخدمات لإثبات العملاء بموجب قواعد وأنظمة المحاسبة العامة.

نبذة عن المؤلف

يشغل الدكتور مايكل جي. جيلس حاليًّا منصب مدير عام في شركة ديلويت لاستشارات التدريب الفيدرالي في واشنطن العاصمة (Washington, D.C.)، وهو مستشار في مجالات تطبيق القانون، والأمن والاستخبارات، الدكتور جيلس هو قائد الفكر في مجال التهديدات الداخلية المرتبطة بالمخاطر الأمنية المحتملة، وفُقدان الأصول، والاستغلال، والإرهاب، والعنف والتخريب في مكان العمل، يقدِّم الدكتور جيلس استشارات لمنظمات القطاع الحكومي والخاص في مجال التهديدات الداخلية، وضمان الأعمال، والتحول التنظيمي، وتخطيط القوى العاملة، وتطويرالقيادة والتخطيط الإستراتيجي، مع التركيز بشكل خاص على الأشخاص، والمهام، والمخاطر، قاد الدكتور جيلس عملية تطوير عدد من حلول ديلويت المبتكرة، بالإضافة إلى تهديدات المُهدّدين الداخليين ليشمل حلول القوى العاملة متعدِّدة الأجيال، وتطوير قوة عمل حاسوبية آمنة، لقد كان في السابق مديرًا تنفيذيًّا في تطبيق القانون الفيدرالي، ورئيس قسم علم النفس في خدمة التحقيق الجنائي البحري (إن سي آي إس) Naval Criminal Investigative Service (NCIS) لأكثر من ١٦ عامًا، في تلك المناصب، قدَّم المساعدة لخدمة التحقيق الجنائي البحري وعدد كبير من المؤسسات الفيدرالية الأخرى، ووكالات تطبيق القانون المحلي والفيدرالي في عمليات التحقيق ضد التجسس والعمليات المتعلقة بالجرائم ومكافحة الإرهاب، شارك الدكتور جيلس في التحقيق والاستجواب لعدد من المُهدِّدين الداخليين المتهمّين بأفعال تجسُّسية وتخريبية، ألَّف العديد من المقالات وفصول الكتب، بالإضافة إلى كتاب في إدارة التهديدات وتقييم المخاطر، لقد حصل الدكتور جيلس على درجة البكالوريوس في الآداب من جامعة ديلاوير (Delaware) ودرجة الماجستير والدكتوراه في علم النفس من جامعة يشيفا (Yeshiva) في نيويورك، أكمل التدريب العملي والطب الشرعي في مركز الطب البحري القومي (National Naval Medical Center) والتدريب المتقدم في مدرسة واشنطن للطب النفسي (Washington School of Psychiatry) ، شغل مناصب أكاديمية سابقة في جامعة الخدمات الموحَّدة للعلوم الصحية (Uniformed Services University of the Health Sciences) ومدرسة واشنطن للطب النفسي (Washington School of Psychiatry).

تمهيد

إن المخاطر التي تهدِّد الأصول الهامة للمنظمات في الوقت الحالي هي أكبر مما كانت عليه في الماضي، إن الأعمال التي يتم تنفيذها على الإنترنت عالميًّا عبر القوى العاملة، وظهور التقنيات التي مكَّنَت من الوصول إلى المعلومات المتاحة من أي مكان وعلى أي جهاز قد زادت من مخاطر البيانات بشكل كبير، حيث يمكن الوصول إلى المعلومات وتنزيلها وتسريبها في ثوانٍ قليلة، وفي تلك الثواني يمكن سرقة واستغلال معلومات الملكية الفكرية للمنظمة، وكذلك بيانات العملاء السرية قبل أن يلاحظ ذلك أيُّ أحد، الأهم من ذلك أن استغلال أصول المنظمات يمكن أن يتسبَّب بضرر بالغ على العلامة التجارية، والسمعة، والثقة العامة، وكذلك الأمن القومي والسلامة العامة في حالة الحكومات، وبالتالي فإن تطوير برنامج للحماية من التهديدات الداخلية أمر بالغ الأهمية؛ لتتمكَّن المنظمة من منع، وكشف، وردع التهديدات الداخلية، والرد عليها.

خلال العقد الماضي استثمرت منظمات القطاع العام والخاص بشكل كبير في حماية مجالها من الهجمات الإلكترونية الخارجية، بينما ظلَّت عُرضةً للتهديدات الداخلية الذين يمكنهم التحايل على الدفاعات السيبرانية بقصدٍ ضارٍّ، أو تساهُل غير مقصود، يعالج هذا الكتاب التهديدات الداخلية: كيفية تطوير برنامج يحمي الأصول الهامة للمنظمة من منظور استباقي وشامل، من خلال سياسة المنظمة، وعمليات الأعمال، والتقنية، والوعي الأمني، والتدريب.

يجب النظر لعملية تطوير برنامج الحماية من التهديدات الداخلية على أنها أكثر من مجرد تنفيذ تكتيكي للتقنية لمراقبة نشاط الموظفين، يجب على المنظمة أن تأخذ في الاعتبار ثلاثة عناصر رئيسة، عند تطوير برنامج الحماية من التهديدات الداخلية، أولًا: ما أهمية فَهْم الأنشطة والسلوكيات العادية للموظفين أثناء قيامهم بأعمالهم، بعد ذلك ما أهمية تحديد الحالات الشاذة، وارتفاع مستوى المخاطر على أصول المنظمة، بالرغم من أن التقنية تشكل عنصرًا أساسيًّا للبرنامج الشامل فقد تعلَّمْنا أن إلقاء نظرة نقدية على سياسات المنظمة، وعمليات الأعمال، واتصالات القوى العاملة، وتدريب الموظفين على التعامل مع المعلومات الحساسة أو السرية، تعتبر أمرًا بالغ الأهمية في تحديد برنامج الحماية من التهديدات الداخلية، أخيرًا إن فعالية الحماية السيبرانية للمنظمة وفَهْم سلوكيات وأنشطة الموظفين العادية، ورَبْطها بشكل مناسب من خلال استخدام التحليلات السلوكية، تعتبر الأساس لنضج برنامج الحماية من التهديدات الداخلية الذي يراقب ويكشف الأحداث.

لقد تعلَّمْنا من خلال خبرتنا أن هناك ثلاثة عناصر رئيسة لإستراتيجية حماية البيانات: برنامج المعلومات السرية، وبرنامج الأمن السيبراني لحماية المحيط، وبرنامج الحماية من التهديدات الداخلية، هذه العناصر ترتبط ارتباطًا وثيقًا بإستراتيجية حماية بيانات المنظمة، بسبب وجود أوجه ترابط رئيس لحماية أصول المنظمة، إن استخدام إطار "الأمن، واليقظة، والمرونة" هو أحد الطرق لتحقيق الترابط الوثيق، ويعتبر إستراتيجية شاملة لحماية معلومات المنظمة، ومعلومات العملاء، والتجهيزات، والأهم من ذلك الأشخاص.

إن البرنامج الشامل للحماية من التهديدات الداخلية يفرض جهدًا تعاونيًّا عبر مديري المستوى التنفيذي (C-suite)، وأصحاب المصلحة التنفيذيين الرئيسين، غالبًا ما يتضمَّن أولئك المديرون التنفيذيون إدارة المخاطر، وتقنية المعلومات، والموارد البشرية، والقانون، وأخلاقيات المهنة، والأمن المادي الذين بإمكانهم التأثير على التغيير في السياسة، والعمليات، وأحداث دورة حياة الموظف، وضوابط أمن المعلومات والأمن المادي، من المهم الحصول على دعم من رئيس موظفي المعلومات (سي آي أو) Chief Information(CIO) Officer ورئيس موظفي أمن المعلومات (سي آي إس أو) Chief Information Security Officer (CISO) بشكل خاص من أجل توفير الضوابط التقنية اللازمة، والبيانات من الأنظمة التي تسجِّل وتربط أنشطة السلوكيات التي تدل على أنشطة شاذة، وتشير إلى مخاطر محتملة عالية، من الضروري أيضًا تنفيذ أداة التحليلات المتقدمة بشكل إستراتيجي لربط البيانات التي تؤدي إلى الكشف عن الحالات الشاذة، وتسهّل إيقاف تقدُّم التهديدات الداخلية المحتملة، ويجب النظر إلى أصحاب المصلحة هؤلاء على أنهم شركاء في الجهد العام؛ نظرًا لأنهم مالكو البيانات الهامة في المنظمة، ومالكو السياسات الذين يمكنهم المساعدة في حماية الأصول، وتحسين ضمان الأعمال، بعبارة أخرى: إن أولئك المديرين التنفيذيين الرئيسين هم أصحاب حماية المنظمة، وتحسينها، والحفاظ على سمعتها.

باختصار إن التحديات التي تواجهها المنظمة في تطوير برنامج شامل واستباقي للحماية من التهديدات الداخلية هي: (١) الموافقة والدعم من جميع أصحاب المصلحة التنفيذيين الرئيسين (المخاطر، وتقنية المعلومات، والموارد البشرية، والقانون، والمالية، وما إلى ذلك)؛ (٢) السياسات وعمليات الأعمال المحدَّدة الموائمة لتحديد السلوكيات الوظيفية الأساسية للموظفين؛ (٣) الربط بين الأمن السيبراني للمنظمة، والسياسات، والعمليات، وتدريب الموظفين على التعامل مع المعلومات السرية، وبرنامج الحماية من التهديدات الداخلية الناتج عن ذلك؛ (٤) وأخيرًا: العناصر التقنية لبرنامج الحماية من التهديدات الداخلية، ويعتبر دمج أنظمة المصادر مع أداة التحليلات أمرًا ضروريًّا لجعل المؤشرات تتدفق من الحواسيب الطرفية وأنظمة المصادر الأخرى إلى أداة التحليلات المتقدمة، حيث يتم تحميل البيانات، وربطها، إنشاء التنبيهات، وتصعيد الحالات الشاذة والتحقيق فيها.

يقدِّم الكتاب العديد من وجهات النظر المختلفة التي يجب مراعاتها عند تطوير برنامج الحماية من التهديدات الداخلية، بدءًا من التحديات التي تواجهها المنظمات، إلى التفكير من خلال الملكية، والخصوصية، واستخدام التقنية للمراقبة، بالإضافة إلى إستراتيجيات التحقيق، بالإضافة إلى ذلك

سيُلقي الكتاب نظرة عن كَثَب في كيفية تكامُل ودمج برنامج الحماية من التهديدات الداخلية مع إستراتيجية كبرى للأمن السيبراني، بالإضافة إلى تقديم منظور حول الأطراف الخارجية ومخاطر سلسلة التوريد، أخيرًا نظرًا لأن التهديدات الداخلية تتعلَّق في الواقع بالأشخاص سيتم مناقشة أهمية ارتباط الموظفين بالمنظمة كإستراتيجية للحَدِّ من مخاطر فقدان الأصول، حافِظْ على الأمن، واليقظة، والمرونة!

رالف سورينتينو
كبير مسؤولي السرية في الولايات المتحدة، المدير الرئيس لشركة ديلويت إل.إل.بي للاستشارات.

Ralph Sorrentino
US Chief Confidentiality Officer, Principal Deloitte Consulting LLP

كلمة شكر

يمثِّل هذا الكتاب تحوُّلًا مهنيًّا بالنسبة لي من خلال خبرة مهنية تمتد لـ 30 عامًا في دراسة التهديدات الداخلية، إنه يعكس بشكل جماعي مساهمات الأسرة، والمرشدين، والزملاء الذين أدَّى تفكيرهم، وتأثيرهم، وتوجيههم إلى تطوُّر كيفية الحد من مخاطر التهديدات الداخلية الحالية بشكل أفضل. إن الرحلة التي دعمتها زوجتي ليزا (Lisa) وأولادي بريان (Bryan) ولورين (Lauren)، والتفكير الذي تطوَّر مع التطوُّر من عالم "الطوب والإسمنت" إلى عالم "البِتَّات والبايتات" لم يكن دخولي لمجال المُهدِّدين الداخليين ليحدث على الإطلاق لولا المرشِدان الدكتور ملفين جرافيتز (Dr. Melvin Gravitz)، والدكتور جو كروفتشيك (Joe Krofcheck)، لقد شَكَّلَ تعليمهم ورؤاهم تفكيري في هذا المجال، خلال مسيرتي المهنية كان هناك العديد ممن ساهموا في فَهْم التهديدات الداخلية من خلال المنظور العملي: د. نيل هيبلر (Dr. Neil Hibler) و د. ريتشارد أولت (Dr. Richard Ault)، الذين عرَّفوني على فَهْم تفكير الجاسوس من خلال مشروع سلامر (Slammer)؛ د. روبرت فين، وكريس هاتشر، وجيم تورنر (Drs. Robert Fein, Chris Hatcher, Jim Turner) الذين أسهم إرشادهم وتعليمهم في فهمي للعنف المستهدف، وتقييم التهديدات؛ د. كاثلين سيفييلو، راندي بوروم، راسل بالاريا، وكريس موهاندي (Drs. Cathleen Civiello, Randy Borum, Russel Palarea, Kris Mohandie)، الذين ساعدوا كزملاء في تشكيل تفكيري طوال سنوات عديدة من النظر في التهديدات الداخلية، شكر خاص للدكتورة جيم تورنر(Dr. Jim Turner) التي تعاونت معي في كتابي الأول حول تقييم التهديدات، بالإضافة إلى ذلك كان هناك الكثير ممن سمحوا لي بالتفكير بشكل مبدع، واستكشاف جوانب مختلفة من التهديدات الداخلية، ديف برانت (Dave Brant)، صديقي المقرَّب والمدير السابق لخدمة التحقيق الجنائي البحري (إن سي آي إس)، الذي شجَّع ودعم فرص تجاربي في مكافحة التجسس فيها وفي جميع أقسام الحكومة، إن الوكلاء المميَّزين الذين حَظِيتُ بالعمل معهم في الكثير من المسائل التي لا يَسَعُ المجال لذكرهم؛ مع ذلك الشكر والعرفان مهم لكل من تعلَّمتُ منهم: مارك فالون، وبوب ماكفادين، ورالف بلينكوي، وتوم بيترو، وكيم ساساكي- سويندل، وستيف كوربيت، وبريان فوسكويل، وماثيو دوهرتي، وتوم نير، وعلي صوفان، وجريج سكوفيل، ومايك دورسي، ومايك براوت، وكارول كولك، وساندي ماكساك (Mark Fallon, Bob McFadden, Ralph Blincoe, Tom Betro, Kim Sasaki- Swindle, Steve Corbett, Bryan Vossekuil, Matthew Doherty, Tom Neer, Ali Soufan, Greg Scovel, Mike Dorsey, Mike Prout, Carl Caulk, and Sandy MacIsaac). وفي ديلويت بدأت مرحلة

جديدة من الرحلة، لقد علَّمني الشركاء الكبار: جريج بيليجرينو، دان هيلفريتش، ليندا سولومون، ناثان هاوسر، شون موريس، أليكس ميركو، مارشال بيلينجسلي، وجيسيكا كوزموسكي (Greg Pellegrino و Dan Helfrich و Linda Solomon و Nathan Houser و Sean Morris و Alex Mirkow و Marshall Billingslea و Jessica Kosmowski) كيفية تحديث النهج إلى حلول أعمال أكثر قوة، كما أقدِّم امتناني العظيم لشركائي وفريق العمل الذين طوَّرُوا وساهَمُوا في تفكيري المعاصر في الحد من التهديدات الداخلية، وهذا الكتاب الذي يعالج التحديات الحالية اليوم: د. كواسي ميتشل (Dr. Kwasi Mitchell)، شريك ومتعاوِن، أكملَ وجهة نظري السلوكية في الأعمال والتقنية بحكمة؛ للمساعدة في تقديم هذا الحل الذي يحتاج أن يبدو عليه اليوم، بورنا إمامي (Borna Emami)، التي تحدثنا كلٌّ منا بلا كَلَل للتفكير بشكل أكثر ابتكارًا وإبداعًا حول المخاطر، وكيفية دَمْج السلوك، والعمليات، والتقنية في نمذجة المخاطر والذين ساهموا مع الدكتور ميتشل (Dr. Mitchell) بشكل كبير في هذا الكتاب؛ جون كاسيدي (John Cassidy)، الذي ساعد في إنشاء أول تقييم لأعمال المُهدِّدين الداخليين في وقت كانت فيه التهديدات الداخلية لا تزال حدثًا كثير التكرار، وقليل التأثير في أذهان العديد من القادة؛ وشركائي في خدمات المخاطر السيبرانية (Cyber Risk Services: Ed Powers و Adnan Amjad و Craig A strich و James O'Kane و Deborah Golden)، الذين ساعَدُوا في تقديم منظور متكامل عن التهديدات الداخلية، ودمج عامل المخاطر السيبرانية، وهو أمر ضروري لأي برنامج أو حل، أنا مُمْتَنٌّ لصداقتي مع دوغ توماس (Doug Thomas) الذي يقود برنامج لوكهيد مارتن (Martin Lockheed) والذي كان قدوة لنا جميعًا في كيفية نقل تجربتنا الجماعية، وتفعيلها إلى برنامج ناجح يعتبر نموذجًا معترَفًا به في القطاعَيْن العام والخاص، تقديري لرئيس موظَّفِي الأمن في ديلويت تيد ألماي (Ted Almay) لأفكاره ودعمه، أيضًا كيت سوفورد، لاسي غراي، هانا كارلايل، وجون تاونسلي (Kate Swofford, Lacey Gray, Hannah Carlisle, and John Townsley)، الذين قادوا الكتاب إلى الانتهاء من خلال تحريرهم المتميز وإدارة المشروع.

هذا الكتاب هو جهد جماعي مع عدد من مساهمات من العديد من المهنيين في ديلويت الذين قدَّمُوا العديد من الحلول للقطاعَيْن الحكومي والخاص؛ للمساعدة في إنشاء ونُضْج برامج الحماية من التهديدات الداخلية، ويُشار إلى العديد من أعضاء الفريق كمساهمين ومشارِكِي تأليف وباحثين رئيسِيين في جدول المحتويات، هذا هو الجيل القادم الذي سيواصل الحلول المبتكرة في بيئة التهديدت الناشئة، أنا ممتنٌّ بشكل خاص لرالف سورينتينو (Ralph Sorrentino)، كبير مسؤولي السرية في ديلويت، الذي كتب بلباقة التمهيدَ، وللقيادة والتوجيه من شاك سايا (Chuck Saia)، كبير مسؤولي المخاطر والتنظيم والسمعة في ديلويت، في دعم تطوير برنامج الحماية من التهديدات الداخلية في ديلويت، لقد عكست أفعالهم وقيادتهم في توجيه المنظمة معًا للتعاون بشكل جماعي في تحديد التهديدات، المعيار الذهبي للمنظمات في الإدارة والحد من المخاطر لحماية بيانات العملاء، والعلامة التجارية، والسمعة.

المحتويات

مقدمة المترجم..... هـ
نبذة عن ديلويت.....ز
نبذة عن المؤلف.....ط
تمهيد.....ك
كلمة شكر .....س

الفصل ١ المقدمة - التهديدات الداخلية اليوم ١
مقدمة.....١
ما هي التهديدات الداخلية.....٣
العوامل البيئية.....٥
كشف التهديدات الداخلية.....٨
الحد من فقدان الأصول: نهج متكامل.....١٠
أفضل ١٠ نصائح للقادة.....١٤
الملخَّص.....١٧
النقاط الرئيسة.....١٧

الفصل ٢ التحديات المشتركة لنضج برنامج الحماية من التهديدات الداخلية.....١٩
المقدمة.....١٩
التحديات التي يواجهها مديرو البرامج.....٢٠
النقاط الرئيسة.....٣٥

الفصل ٣ من الطوب والإسمنت إلى البتات والبايتات.....٣٩
التحول من الطوب والإسمنت إلى البتات والبايتات.....٣٩
التهديدات الداخلية في عالم الطوب والإسمنت.....٤١
مرحلة التحوُّل.....٤٢
التهديدات الداخلية في عالم البتات و البايتات.....٤٣
النقاط الرئيسة.....٤٨

الفصل ٤ تحديد الملكية الوظيفية.....٥١
المقدمة.....٥١

موقع البرنامج..... ٥١
تطوير إطار برنامج للمنع، والكشف، والرد على التهديدات الداخلية..... ٥٣
التحديات الرئيسة..... ٦٣
النقاط الرئيسة..... ٦٤

الفصل ٥ تحديد المؤشرات الهامة في البيانات التنظيمية..... ٦٥
مؤشرات المخاطر المحتملة..... ٦٦
تحويل المعرفة حول المُهدِدين الداخليين إلى بيانات تنظيمية..... ٧٢
تحديد المؤشرات الهامة في جميع أنحاء المنظمة..... ٧٧
التحديات الرئيسة..... ٧٨
النقاط الرئيسة..... ٧٩

الفصل ٦ تحديد مستوى تقبُّل المخاطر في المنظمة..... ٨١
تعريف تحمُّل المخاطر..... ٨١
تحديد الأصول الهامة لمنظمتك..... ٨٤
تحديد التهديدات التي يُشكلها المُهدِدون الداخليون على أصولك الهامة..... ٨٦
موازنة استثمارات الأمن وتحمُّل الخسائر..... ٨٨
إعادة تقييم أولويات الأصول..... ٩٢
الملخَّص..... ٩٣
دراسة حالة ١: شركة خدمات مالية..... ٩٣
دراسة حالة ٢: مزوّدو الرعاية الصحية..... ٩٤
دراسة حالة ٣: الاتصالات، والإعلام، والتقنية..... ٩٤
النقاط الرئيسة..... ٩٥

الفصل ٧ إدارة المخاطر باستخدام التحليلات المتقدمة..... ٩٧
مقدمة للتحليلات المتقدمة..... ٩٧
المبادئ التوجيهية..... ٩٩
التحليلات المتقدمة قيد التنفيذ..... ١٠٠
اختيار الأداة المناسبة..... ١٠٥
نهج وتطور قواعد العمل..... ١٠٧
أمن التحليلات المتقدمة..... ١٠٨
تحليلات الأمن كأداة لتمكين الأعمال..... ١٠٩
النقاط الرئيسة..... ١١١

الفصل ٨ أمن المعلومات ودمج التقنية..... ١١٣
المقدمة..... ١١٣
الضوابط الإدارية والإجرائية..... ١١٥
الضوابط التقنية..... ١١٩
الضوابط المادية..... ١٢١
مستقبل الضوابط الأمنية..... ١٢٢

الختام..... ١٢٣
النقاط الرئيسة..... ١٢٣

الفصل ٩ إدارة المخاطر السيبرانية وأداء الأعمال..... ١٢٥
طرق التفكير السليمة: الآمنة، واليقظة، والمرنة..... ١٢٦
التهديدات الداخلية: مشكلة ديناميكية، متعددة المستويات..... ١٣٠
بناء طرق تفكير جماعية ونماذج قوية..... ١٣١
الخصائص الشائعة للبرامج الآمنة، واليقظة، والمرنة..... ١٣٣
النقاط الرئيسة..... ١٣٤

الفصل ١٠ التهديدات التي يُشكِّلها المُهدِدون الداخليون كطرف ثالث: اعتبارات لبرنامج فحص المورّدين ١٣٧
المقدمة..... ١٣٧
الاتجاهات الدافعة لانتشار الموردين في السوق الأمريكية..... ١٣٨
أمثلة للتهديدات التي يُشكِّلها المورّدون..... ١٣٩
تعريف فحص المورّدين..... ١٤٢
نهج فحص المورّدين..... ١٤٣
النقاط الرئيسة..... ١٤٣

الفصل ١١ ارتباط الموظفين بالمنظمة: مسألة هامة في الحد من مخاطر التهديدات الداخلية..... ١٤٩
المقدمة..... ١٤٩
فهم لماذا ارتباط الموظفين بالمنظمة مسألة هامة..... ١٥٠
ارتباط القوى العاملة تحدي بالغ الأهمية اليوم..... ١٥١
دوافع مكان العمل لارتباط الموظفين..... ١٥٢
قياس ارتباط الموظفين بالمنظمة..... ١٥٦
تحسين ارتباط الموظفين بالمنظمة واستدامته..... ١٥٦
النقاط الرئيسة..... ١٥٨

الفصل ١٢ التهديدات الداخلية والعنف في مكان العمل..... ١٥٩
المقدمة..... ١٥٩
نظرة تاريخية ومتراكمة للتهديدات الداخلية والعنف في مكان العمل..... ١٦٠
المفاهيم الرئيسة..... ١٦٣
الأساطير المتعلقة بالعنف في مكان العمل..... ١٦٦
العلامات التحذيرية..... ١٦٨
النقاط الرئيسة..... ١٦٨

الفصل ١٣ المراقبة والتحقق..... ١٦٩
المراقبة..... ١٧٠
الرد على التهديدات الداخلية..... ١٧٦
النقاط الرئيسة..... ١٨١

الفصل ١٤ اعتبارات الخصوصية في برامج الحد من التهديدات الداخلية..... ١٨٣
المقدمة..... ١٨٣
خصوصية البيانات وجمع مؤشرات المخاطر المحتملة (برايس)..... ١٨٤
موازنة خصوصية البيانات مع الحد الفعَّال من التهديدات الداخلية..... ١٨٦
تقييم تأثير الخصوصية (بيا)..... ١٨٦
الاعتبارات الإضافية للخصوصية..... ١٨٩
الختام..... ١٩٢
النقاط الرئيسة..... ١٩٣

الفصل ١٥ ما يحمله المستقبل..... ١٩٥
التهديدات الداخلية: نظرة مستقبلية..... ١٩٥
التعريف المتغير للمُهدِّد الداخلي..... ١٩٥
فهم البيئة الكلية..... ١٩٦
الاتجاهات الناشئة..... ١٩٨
البيانات الكبيرة وتحليلات المخاطر..... ٢٠١
تخطيط السيناريو..... ٢٠١
ماذا بعد؟..... ٢٠٣

الملحقات ٢٠٥
ثبت المصطلحات
أولاً: عربي - إنجليزي ٢٢٩
ثانياً: إنجليزي - عربي ٢٤٢
كشاف الموضوعات ٢٥٥