ملاحق

ملحق (أ): مصطلحات وتعريفات

يوضح الجدول ٢ أدناه بعض المصطلحات وتعريفاتها التي ورد ذكرها في هذه الضوابط.

جدول٢: مصطلحات وتعريفات

المصطلح	التعريف
الحماية من التهديدات المتقدمة المستمرة Advanced Persistent Threat (APT) Protection	الحماية من التهديدات المتقدمة التي تستخدم أساليب خفية تهدف إلى الدخول غير المشروع على الأنظمة والشبكات التقنية ومحاولة البقاء فيها لأطول فترة ممكنة عن طريق تفادي أنظمة الكشف والحماية. وهذه الأساليب تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware) لتحقيق هدفها.
الأصل Asset	أي شيء ملموس أو غير ملموس له قيمة بالنسبة للجهة. هناك أنواع كثيرة من الأصول؛ بعض هذه الأصول تتضمن أشياء واضحة، مثل: الأشخاص، والآلات، والمرافق، وبراءات الاختراع، والبرمجيات والخدمات. ويمكن أن يشمل المصطلح أيضاً أشياء أقل وضوحاً، مثل: المعلومات والخصائص (مثل: سمعة الجهة وصورتها العامة، أو المهارة والمعرفة).
هجوم Attack	أي نوع من الأنشطة الخبيثة التي تحاول الوصول بشكل غير مشروع أو جمع موارد النظم المعلوماتية أو المعلومات نفسها أو تعطيلها أو منعها أو تحطيمها أو تدميرها.
تدقيق Audit	المراجعة المستقلة ودراسة السجلات والأنشطة لتقييم مدى فعالية ضوابط الأمن السيبراني ولضمان الالتزام بالسياسات، والإجراءات التشغيلية، والمعايير والمتطلبات التشريعية والتنظيمية ذات العلاقة.
التحقق Authentication	التأكد من هوية المستخدم أو العملية أو الجهاز، وغالباً ما يكون هذا الأمر شرطاً أساسياً للسماح بالوصول إلى الموارد في النظام.
صلاحية المستخدم Authorization	خاصية تحديد والتأكد من حقوق/تراخيص المستخدم للوصول إلى الموارد والأصول المعلوماتية والتقنية للجهة والسماح له وفقاً لما حدد مسبقاً في حقوق/تراخيص المستخدم.
توافر Availability	ضمان الوصول إلى المعلومات والبيانات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.
النسخ الاحتياطية Backup	الملفات والأجهزة والبيانات والإجراءات المتاحة للاستخدام في حالة الأعطال أو الفقدان، أو إذا حذف الأصل منها أو توقف عن الخدمة.
أحضر الجهاز الخاص بك Bring Your Own Device (BYOD)	يشير هذا المصطلح إلى سياسة جهة تسمح (سواءً بشكل جزئي أو كلي) للعاملين فيها بجلب الأجهزة الشخصية الخاصة بهم (أجهزة الكمبيوتر المحمولة والأجهزة اللوحية والهواتف الذكية) إلى أماكن العمل في الجهة، واستخدام هذه الأجهزة للوصول إلى الشبكات والمعلومات والتطبيقات والأنظمة التابعة للجهة المقيدة بصلاحيات دخول.
الدائرة التلفزيونية المغلقة (CCTV)	يستخدم التليفزيون ذو الدائرة المغلقة، والمعروف أيضاً باسم المراقبة بالفيديو، كاميرات الفيديو لإرسال إشارة إلى مكان محدد على مجموعة محدودة من الشاشات. وغالباً ما يطلق هذا المصطلح على تلك التقنية المستخدمة للمراقبة في المناطق التي قد تحتاج إلى مراقبة حيث يشكل الأمن المادي مطلباً هاماً فيها.
إدارة التغيير Change Management	وهو نظام لإدارة الخدمة حيث يضمن منهجاً نظامياً واستباقياً باستخدام أساليب وإجراءات معيارية فعالة (على سبيل المثال: التغيير في البنية التحتية للجهة، وشبكاتها، إلخ). تساعد إدارة التغيير جميع الأطراف المعنيين، بما في ذلك الأفراد والفرق على حد سواء، على الانتقال من حالتهم الحالية إلى الحالة المرغوبة التالية، كما تساعد إدارة التغيير أيضاً على تقليل تأثير الحوادث ذات العلاقة على الخدمة.
الحوسبة السحابية Cloud Computing	نموذج لتمكين الوصول عند الطلب إلى مجموعة مشتركة من موارد تقنية المعلومات (مثل: الشبكات والخوادم والتخزين والتطبيقات والخدمات) التي يمكن توفيرها بسرعة وإطلاقها بالحد الأدنى من الجهد الإداري التشغيلي والتدخل/التفاعل لإعداد الخدمة من مزود الخدمة. تسمح الحوسبة السحابية للمستخدمين بالوصول إلى الخدمات القائمة على التقنية من خلال شبكة الحوسبة السحابية دون الحاجة لوجود معرفة لديهم أو تحكم في البنية التحتية التقنية التي تدعمهم. يتألف نموذج الحوسبة السحابية من خمس خصائص أساسية: خدمة ذاتية حسب الطلب، ووصول إلى الشبكة بشكل واسع، ومجمع الموارد، ومرونة سريعة، والخدمة المقاسة. وهناك ثلاثة نماذج لتقديم خدمات الحوسبة السحابية وهي: البرمجيات السحابية كخدمة Software-as-Service "SaaS"، والنظام أو المنصة السحابية كخدمة "PaaS" Platform-as-Service، والبنية التحتية السحابية كخدمة"IaaS" Infrastructure-as-Service. كما أن هناك أربعة نماذج للحوسبة السحابية حسب طبيعة الدخول: الحوسبة السحابية العامة، والحوسبة السحابية المجتمعية، والحوسبة السحابية الخاصة، والحوسبة السحابية الهجين.

انتهاك أمني **Compromise**	الإفصاح عن أو الحصول على معلومات لأشخاص غير مصرح تسريبها أو الحصول عليها، أو انتهاك السياسة الأمنية السيبرانية للجهة بالإفصاح عن أو تغيير أو تخريب أو فقد شيء سواءً بقصد أو بغير قصد. ويقصد بالانتهاك الأمني الإفصاح عن أو الحصول على بيانات حساسة أو تسريبها أو تغييرها أو تبديلها أو استخدامها بدون تصريح (بما في ذلك مفاتيح تشفير النصوص وغيرها من المعايير الأمنية السيبرانية الحرجة).
السرية **Confidentiality**	الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها بما في ذلك وسائل حماية معلومات الخصوصية والملكية الشخصية.
المعلومات (أو البيانات) الحساسة **Sensitive Data/Information**	هي المعلومات (أو البيانات) التي تعتبر غاية في الحساسية والأهمية، حسب تصنيف الجهة، والمُعدة للاستخدام من قبل جهة أو جهات محددة. وأحد الطرق التي يمكن استخدامها في تصنيف هذا النوع من المعلومات هو قياس مدى الضرر عند الإفصاح عنها أو الاطلاع عليها بشكل غير مصرح به أو فقدها أو تخريبها، حيث قد يؤدي ذلك إلى أضرار مادية أو معنوية على الجهة أو المتعاملين معها، أو التأثير على حياة الأشخاص ذو العلاقة بتلك المعلومات، أو التأثير والضرر بأمن الدولة أو اقتصادها الوطني أو مقدراتها الوطنية. وتشمل المعلومات الحساسة كل المعلومات التي يترتب على الإفصاح عنها بشكل غير مصرح به أو فقدها أو تخريبها مساءلة أو عقوبات نظامية.
البنية التحتية الوطنية الحساسة **Critical National Infrastructure**	تلك العناصر الأساسية للبنية التحتية (أي الأصول، والمرافق، والنظم، والشبكات، والعمليات، والعاملون الأساسيون الذين يقومون بتشغيلها ومعالجتها)، والتي قد يؤدي فقدانها أو تعرضها لانتهاكات أمنية إلى: • أثر سلبي كبير على توافر الخدمات الأساسية أو تكاملها أو تسليمها -بما في ذلك الخدمات التي يمكن أن تؤدي في حال تعرضت سلامتها للخطر إلى خسائر كبيرة في الممتلكات و/أو الأرواح و/أو الإصابات- مع مراعاة الآثار الاقتصادية و/أو الاجتماعية على المستوى الوطني. • تأثير كبير على الأمن الوطني و/أو الدفاع الوطني و/أو اقتصاد الدولة أو مقدراتها الوطنية.
التشفير **Cryptography**	(ويسمى أيضاً علم التشفير) وهي القواعد التي تشتمل مبادئ ووسائل وطرق تخزين ونقل البيانات أو المعلومات في شكل معين وذلك من أجل إخفاء محتواها الدلالي، ومنع الاستخدام غير المصرح به أو منع التعديل غير المكتشف، بحيث لا يمكن لغير الأشخاص المعنيين قراءتها ومعالجتها.
الهجوم السيبراني **Cyber-Attack**	محاولة متعمدة للتأثير السلبي على الأمن السيبراني، سواءً نجحت في ذلك أو لم تنجح.
المخاطر السيبرانية **Cyber Risks**	المخاطر التي تمس عمليات أعمال الجهة (بما في ذلك رؤية الجهة أو رسالتها أو إداراتها أو صورتها أو سمعتها) أو أصول الجهة أو الأفراد أو الجهات الأخرى أو الدولة، بسبب إمكانية الوصول غير المصرح به أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو تدمير المعلومات و/أو نظم المعلومات.
الصمود الأمني السيبراني **Cybersecurity Resilience**	القدرة الشاملة للجهة على الصمود أمام الأحداث السيبرانية، ومسببات الضرر، والتعافي منها.
الأمن السيبراني **Cybersecurity**	حسب ما نص عليه تنظيم الهيئة الصادر بالأمر الملكي رقم (٦٨٠١) وتاريخ (١١/ ٢ /١٤٣٩هـ)، فإن الأمن السيبراني هو حماية الشبكات وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية، ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات، من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع. ويشمل مفهوم الأمن السيبراني أمن المعلومات والأمن الإلكتروني والأمن الرقمي ونحو ذلك.
الفضاء السيبراني **Cyberspace**	الشبكة المترابطة من البنية التحتية لتقنية المعلومات، والتي تشمل الإنترنت وشبكات الاتصالات وأنظمة الحاسب الآلي والأجهزة المتصلة بالإنترنت، إلى جانب المعالِجات وأجهزة التحكم المرتبطة بها. كما يمكن أن يشير المصطلح إلى عالم أو نطاق افتراضي كظاهرة مجربة أو مفهوم مجرّد.
تصنيف البيانات والمعلومات **Data and Information Classification**	تعيين مستوى الحساسية للبيانات والمعلومات التي ينتج عنها ضوابط أمنية لكل مستوى من مستويات التصنيف. يتم تعيين مستويات حساسية البيانات والمعلومات وفقاً لفئات محددة مسبقاً حيث يتم إنشاء البيانات والمعلومات أو تعديلها أو تحسينها أو تخزينها أو نقلها. مستوى التصنيف هو مؤشر على قيمة أو أهمية البيانات والمعلومات للجهة.
أرشفة البيانات **Data Archiving**	عملية نقل البيانات التي لم تعد مستخدمة بشكل فعال في جهاز تخزين منفصل للحفظ طويل الأجل. تتكون بيانات الأرشيف من بيانات قديمة لا تزال مهمة للجهة وقد تكون مطلوبة للرجوع إليها في المستقبل، وبيانات يجب الاحتفاظ بها للالتزام بالتشريعات والتنظيمات ذات العلاقة.
الدفاع الأمني متعدد المراحل **Defense-in-Depth**	هو مفهوم لتوكيد المعلومات (Information Assurance) حيث يتم وضع مستويات متعددة من الضوابط الأمنية (كدفاع) في نظام تقنية المعلومات (IT) أو تقنية التشغيل (OT).
التعافي من الكوارث **Disaster Recovery**	الأنشطة والبرامج والخطط المصممة لإرجاع وظائف وخدمات الأعمال الحيوية للجهة إلى حالة مقبولة، بعد التعرض إلى هجمات سيبرانية أو تعطل لهذه الخدمات والوظائف.
نظام أسماء النطاقات **Domain Name System**	نظام تقني يستخدم قاعدة بيانات يتم توزيعها عبر الشبكة و/أو الإنترنت تسمح بتحويل أسماء النطاقات إلى عناوين الشبكة (IP Addresses)، والعكس، لتحديد عناوين الخدمات مثل خوادم المواقع الإلكترونية والبريد الإلكتروني.
فعالية **Effectiveness**	تشير الفعالية إلى الدرجة التي يتم بها تحقيق تأثير مخطط له. وتعتبر الأنشطة المخططة فعالة إذا تم تنفيذ هذه الأنشطة بالفعل، وتعتبر النتائج المخطط لها فعالة إذا تم تحقيق هذه النتائج بالفعل. يمكن استخدام مؤشرات قياس الأداء "Key Performance Indicators "KPIs لقياس وتقييم مستوى الفعالية.

كفاءة **Efficiency**	العلاقة بين النتائج المحققة (المخرجات) والموارد المستخدمة (المدخلات). يمكن تعزيز كفاءة العملية أو النظام من خلال تحقيق نتائج أكثر باستخدام نفس الموارد (المدخلات) أو أقل.
حدث **Event**	حدث ذو علاقة بحالة الأمن السيبراني الخاصة بشبكة، أو نظام، أو خدمة، أو بيانات، أو أي جهاز تقني آخر.
بروتوكول نقل النص التشعبي الآمن **Hyper Text Transfer Protocol Secure (HTTPS)**	بروتوكول يستخدم التشفير لتأمين صفحات وبيانات الويب عند انتقالها عبر الشبكة. وهو عبارة عن نسخة آمنة من نظام بروتوكول نقل النص التشعبي (HTTP).
هوية **Identification**	وسيلة التحقق من هوية المستخدم أو العملية أو الجهاز، وهي عادة شرط أساسي لمنح حق الوصول إلى الموارد في النظام.
حادثة **Incident**	حدث متعمد أو غير متعمد تسبب في التأثير السلبي على الأمن السيبراني.
سلامة المعلومة **Integrity**	الحماية ضد تعديل أو تخريب المعلومات بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات (Non-Repudiation) والموثوقية.
المتطلبات الدولية **International Requirements**	المتطلبات الدولية هي متطلبات طورتها جهة أو منظمة دولية عالمية للاستخدام بشكل تنظيمي في جميع أنحاء العالم (مثل:SWIFT ، PCI، وغيرها).
نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات **Intrusion Prevention System (IPS)**	نظام لديه قدرات كشف الاختراقات، بالإضافة إلى القدرة على منع وإيقاف محاولات الأنشطة والحوادث المشبوهة أو المحتملة.
مؤشر قياس الأداء **Key Performance Indicator (KPI)**	نوع من أدوات قياس مستوى الأداء يُقيّم مدى نجاح نشاط ما أو جهة تجاه تحقيق أهداف محددة.
ترميز أو علامة **Labeling**	عرض معلومات (بتسمية وترميز محدد وقياسي) توضع على أصول الجهة (مثل: الأجهزة والتطبيقات والمستندات وغيرها) ليستدل بها للإشارة إلى بعض المعلومات المتعلقة بتصنيف الأصل وملكيته ونوعه وغيرها من المعلومات المتعلقة بإدارة الأصول.
الحد الأدنى من الصلاحيات **Least Privilege**	مبدأ أساسي في الأمن السيبراني يهدف إلى منح المستخدمين صلاحيات الوصول التي يحتاجونها لتنفيذ مسؤولياتهم الرسمية فقط.
البرمجيات الضارة **Malware**	برنامج يُصيب الأنظمة بطريقة خفية (في الغالب) لانتهاك سرية أو سلامة ودقة أو توافر البيانات أو التطبيقات أو نظم التشغيل.
التحقق من الهوية متعدد العناصر **Multi-Factor Authentication (MFA)**	نظام أمني يتحقق من هوية المستخدم، باستخدام عدة عناصر من خلال تقنيات التحقق من الهوية. عناصر التحقق من الهوية هي: • المعرفة (شيء يعرفه المستخدم فقط "مثل استخدام تقنية كلمة المرور"). • الحيازة (شيء يملكه المستخدم فقط "مثل استخدام تقنية برنامج أو جهاز توليد أرقام عشوائية أو الرسائل القصيرة المؤقتة لتسجيل الدخول"، ويطلق عليها "One-Time-Password"). • الملازمة (صفة أو سمة حيوية متعلقة بالمستخدم نفسه فقط "مثل استخدام تقنية بصمة الإصبع أو الوجه").
المعمارية متعددة المستويات **Multi-tier Architecture**	معمارية أو بنية تُطبق أسلوب عميل-خادم الذي يتم فيه تطوير وصيانة منطق العملية الوظيفية، والوصول إلى البيانات، وتخزين البيانات وواجهة المستخدم كوحدات مستقلة على منصات منفصلة.
الحاجة إلى المعرفة والحاجة إلى الاستخدام **Need-to-know and Need-to-use**	القيود المفروضة على البيانات، والتي تعتبر حساسة ما لم يكن لدى الشخص حاجة محددة للاطلاع على البيانات لغرض ما متعلق بأعمال ومهام رسمية.
النسخ الاحتياطي غير المتصل أو خارج الموقع **Offline/Offsite Backup**	نسخة احتياطية لقاعدة البيانات وإعدادات الأنظمة والتطبيقات والأجهزة عندما تكون النسخة غير متصلة وغير قابلة للتحديث. عادةً ما تستخدم أشرطة (Tapes) في حالة النسخة الاحتياطية خارج الموقع.
النسخ الاحتياطي المتصل **Online Backup**	طريقة للتخزين يتم فيها النسخ الاحتياطي بانتظام عبر شبكة على خادم بعيد، (إما داخل شبكة الجهة أو بالاستضافة لدى مزود خدمة).
العاملون في الجهة **Organization Staff**	الأشخاص الذين يعملون في الجهة (بما في ذلك الموظفون الرسميون والموظفون المؤقتون والمتعاقدون).
الاسناد الخارجي Outsourcing	الحصول على (السلع أو الخدمات) عن طريق التعاقد مع مورد أو مزود خدمة.
حزم التحديثات والإصلاحات **Patch**	حزم بيانات داعمة لتحديث أو إصلاح أو تحسين نظام التشغيل للحاسب الآلي أو لتطبيقاته أو برامجه. وهذا يشمل إصلاح الثغرات الأمنية وغيرها من الأخطاء، حيث تسمى هذه الحزم عادةً إصلاحات أو إصلاح الأخطاء وتحسين إمكانية الاستخدام أو الأداء.
اختبار الاختراق **Penetration Testing**	ممارسة اختبار على نظام حاسب آلي أو شبكة أو تطبيق موقع إلكتروني أو تطبيق هواتف ذكية للبحث عن ثغرات يمكن أن يستغلها المهاجم.

رسائل التصيّد الإلكتروني **Phishing Emails**	محاولة الحصول على معلومات حساسة مثل أسماء المستخدمين وكلمات المرور أو تفاصيل بطاقة الائتمان، غالباً لأسباب ونوايا ضارة وخبيثة، وذلك بالتنكر على هيئة جهة جديرة بالثقة في رسائل بريد إلكترونية.
الأمن المادي **Physical Security**	يصف الأمن المادي التدابير الأمنية التي تم تصميمها لمنع الوصول غير المصرح به إلى المرافق والمعدات والموارد التابعة للجهة، وحماية الأفراد والممتلكات من التلف أو الضرر (مثل التجسس أو السرقة، أو الهجمات الإرهابية). ينطوي الأمن المادي على استخدام طبقات متعددة من نظم مترابطة، تشمل الدوائر التلفزيونية المغلقة (CCTV)، وحراس الأمن، وحدود أمنية، والأقفال، وأنظمة التحكم في الوصول، والعديد من التقنيات الأخرى.
سياسة **Policy**	وثيقة تحدد بنودها التزاماً عاماً أو توجيهاً أو نية ما كما تم التعبير عن ذلك رسمياً من قبل صاحب الصلاحية للجهة. سياسة الأمن السيبراني هي وثيقة تعبر بنودها عن الالتزام الرسمي للإدارة العليا للجهة بتنفيذ وتحسين برنامج الأمن السيبراني في الجهة، وتشتمل السياسة على أهداف الجهة فيما يتعلق ببرنامج الأمن السيبراني وضوابطه ومتطلباته وآلية تحسينه وتطويره.
إدارة الصلاحيات الهامة والحساسة **Privileged Access Management**	عملية إدارة الصلاحيات ذات الخطورة العالية على أنظمة الجهة والتي تحتاج في الغالب إلى تعامل خاص لتقليل المخاطر التي قد تنشأ من سوء استخدامها.
إجراء **Procedure**	وثيقة تحتوي على وصف تفصيلي للخطوات الضرورية لأداء عمليات أو أنشطة محددة في التوافق مع المعايير والسياسات ذات العلاقة. وتعرّف الإجراءات على أنها جزء من العمليات.
عملية **Process**	مجموعة من الأنشطة المترابطة أو التفاعلية تحول المدخلات إلى مخرجات. وهذه الأنشطة متأثرة بسياسات الجهة.
الاستعادة **Recovery**	إجراء أو عملية لاستعادة أو التحكم في شيء منقطع أو تالف أو مسروق أو ضائع.
مدة الاحتفاظ **Retention**	هي المدة الزمنية التي يجب فيها الاحتفاظ بالمعلومات أو البيانات أو سجلات الأحداث أو النسخ الاحتياطية، بغض النظر عن الشكل (ورقي أو إلكتروني أو غير ذلك).
المعايير الأمنية لشفرة البرامج والتطبيقات **Secure Coding Standards**	ممارسة تطوير برمجيات وتطبيقات الحاسب الآلي بطريقة تحمي من التعرض غير المقصود لثغرات الأمن السيبراني المتعلقة بالبرمجيات والتطبيقات.
مراجعة الإعدادات والتحصين **Secure Configuration and Hardening**	حماية وتحصين وضبط إعدادات جهاز الحاسب الآلي، والنظام، والتطبيق، وجهاز الشبكة، والجهاز الأمني لمقاومة الهجمات السيبرانية. مثل: إيقاف أو تغيير الحسابات المصنعية والافتراضية، إيقاف الخدمات غير المستخدمة، إيقاف منافذ الشبكة غير المستخدمة.
نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني **Security Information and Event Management (SIEM)**	نظام يقوم بإدارة وتحليل بيانات سجلات الأحداث الأمنية في الوقت الفعلي لتوفير مراقبة للتهديدات، وتحليل نتائج القواعد المترابطة لسجلات الأحداث، والتقارير حول بيانات السجلات، والاستجابة للحوادث.
الاختبار الأمني **Security Testing**	عملية تهدف إلى التأكد من أن النظام أو التطبيق المعدّل أو الجديد يتضمن ضوابط وحمايات أمنية مناسبة ولا يحتوي على أي ثغرات أمنية قد تضر بالأنظمة أو التطبيقات الأخرى، أو تؤدي إلى سوء استخدام النظام أو التطبيق أو معلوماته، وكذلك للحفاظ على وظيفة النظام أو التطبيق على النحو المنشود.
الأمن من خلال التصميم **Security-by-Design**	منهجية لتطوير الأنظمة والتطبيقات وتصميم الشبكات التي تسعى إلى جعلها خالية من نقاط الضعف والثغرات الأمنية السيبرانية، والمقدرة على صد الهجوم السيبراني قدر الإمكان من خلال عدة تدابير على سبيل المثال: الاختبار المستمر، وحماية المصادقة والتمسك بأفضل ممارسات البرمجة والتصميم، وغيرها.
فصل المهام **Segregation of Duties**	مبدأ أساسي في الأمن السيبراني يهدف إلى تقليل الأخطاء والاحتيال خلال مراحل تنفيذ عملية محددة عن طريق التأكد من ضرورة وجود أكثر من شخص لإكمال هذه المراحل وبصلاحيات مختلفة.
إطار سياسة المرسل **Sender Policy Framework**	طريقة للتحقق من أن خادم البريد الإلكتروني المستخدم في إرسال رسائل البريد الإلكتروني يتبع المجال الخاص بالجهة المرسِلة.
طرف خارجي **Third-Party**	أي جهة تعمل كطرف في علاقة تعاقدية لتقديم السلع أو الخدمات (وهذا يشمل موردي ومزودي الخدمات).
تهديد **Threat**	أي شيء قد يؤثر سلبًا على الأمن السيبراني.
المعلومات الاستباقية **Threat Intelligence**	يوفر معلومات منظمة وتحليلها حول الهجمات الأخيرة والحالية والمحتملة التي يمكن أن تشكل تهديداً سيبرانياً للجهة.
الثغرة **Vulnerability**	ضعف في أي أصل تقنية معلومات (مثال: برنامج، نظام) ، أو إجراء، أو ضابط، أو أي شيء؛ يمكن استغلاله للتأثير السلبي على الأمن السيبراني.
جدار الحماية لتطبيقات الويب **Web Application Firewall**	نظام حماية يوضع قبل تطبيقات الويب لتقليل المخاطر الناجمة من محاولات الهجوم الموجهة على تطبيقات الويب.
البرمجيات الضارة غير المعروفة مسبقا **Zero-Day Malware**	عبارة عن برمجيات ضارة (Malware) غير معروفة مسبقاً، تم إنتاجها أو نشرها حديثاً. ويصعب في العادة اكتشافها بواسطة وسائل الحماية التي تعتمد على المعرفة المسبقة للبرمجيات الضارة (Signature-based Protection).