الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

المملكة العربية السعودية

الإطار السعودي لكوادر الأمن السيبراني (سيوف)

SCyWF - 1 : 2020

إشارة المشاركة: أبيض، تصنيف الوثيقة: متاح

بســـم اللّه الرحمـــن الرحيـــم

بروتوكول الإشارة الضوئية (TLP):

تم إنشاء نظام بروتوكول الإشارة الضوئية لمشاركة أكبر قدر من المعلومات الحساسة ويستخدم على نطاق واسع في العالم وهناك أربعة ألوان (إشارات ضوئية):

أحمر – شخصي وسري للمستلم فقط

المستلم لا يحق له مشاركة المصنف بالإشارة الحمراء مع أي فرد سواء من داخل أو خارج المنشأة خارج النطاق المحدد للاستلام.

برتقالي – مشاركة محدودة

المستلم بالإشارة البرتقالية يمكنه مشاركة المعلومات في نفس المنشأة مع الأشخاص المعنيين فقط، ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر – مشاركة في نفس المجتمع

حيث يمكنك مشاركتها مع آخرين من منشأتك أو منشأة أخرى على علاقة معكم أو بنفس القطاع، ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

أبيض – غير محدود

قائمة المحتويات

قائمة الجداول

قائمة الرسوم التوضيحية

١. المقدمة

تعمل الهيئة الوطنية للأمن السيبراني على حماية الفضاء السيبراني للمملكة. ويتطلب ذلك كوادر وطنية مؤهلة في مجال الأمن السيبراني، تكون قادرة على تنفيذ كافة أعمال الأمن السيبراني. وبموجب الأمر الملكي الكريم رقم ٦٨٠١، وتاريخ ١٤٣٩/٢/١١هـ ، تتضمن اختصاصات الهيئة الوطنية للأمن السيبراني بناء القدرات الوطنية المتخصصة في مجالات الأمن السيبراني، والمشاركة في إعداد البرامج التعليمية والتدريبية الخاصة بها، وإعداد المعايير المهنية والأطر وبناء وتنفيذ المقاييس والاختبارات القياسية المهنية ذات العلاقة. لذا طورت الهيئة الوطنية للأمن السيبراني الإطار السعودي لكوادر الأمن السيبراني (سيوف)، ليكون مرجعاً أساسياً في هذا الجانب.

١-١ نظرة عامة

يعنى الإطار السعودي لكوادر الأمن السيبراني بتصنيف أعمال كوادر الأمن السيبراني في المملكة العربية السعودية، وتعريف الأدوار الوظيفية لكل فئة، وتوصيف متطلبات كل دور وظيفي من حيث المهام والمعارف والمهارات والقدرات.

إن الهدف الرئيسي من هذا الإطار هو تقديم دليل مرجعي لإعداد كوادر الأمن السيبراني وتطويرها واستقطابها وإدارتها. ويقدم الإطار مرجعاً موحداً لتحسين التواصل وتطوير المحتوى في أنشطة تأهيل وإدارة الكوادر، ويساعد أيضاً في ربط مخرجات التعلم لبرامج التعليم والتدريب بالمعارف والمهارات والقدرات المطلوبة للأدوار الوظيفية المختلفة في مجال الأمن السيبراني.

وتوصي الهيئة كافة الجهات بتبني هذا الإطار واستخدامه لضمان المواءمة مع الأطر والإرشادات الوطنية في هذا المجال. ولا يمنع ذلك أن تقوم كل جهة بعمل بعض التعديلات والإضافات لتكييف هذا الإطار مع احتياجاتها الوظيفية دون إخلال بالبنية الأساسية لهذا الإطار.

وبما أن مجال الأمن السيبراني متغير ومتطور باستمرار فستتم مراجعة محتويات هذا الإطار وتحديثه بصفة دورية.

١-٢ المنهجية والبنية

تم تطوير الإطار السعودي لكوادر الأمن السيبراني بما يتوافق مع منهجية إطار كوادر الأمن السيبراني التابع للمبادرة الوطنية لتعليم الأمن السيبراني (NICE) الصادر من قبل المعهد الوطني الأمريكي للمعايير والتقنية (NIST)[1]. وينظم هذا الإطار أعمال الأمن السيبراني بشكل هرمي يتكون من فئات ومجالات تخصص وأدوار وظيفية. ومن المهم الإشارة إلى أن الفئات ومجالات التخصص والأدوار الوظيفية الواردة في الإطار السعودي لكوادر الأمن السيبراني مختلفة عن تلك الواردة في إطار الكوادر التابع للمبادرة الوطنية لتعليم الأمن السيبراني (NICE)، حيث صُممت لتلائم احتياج كوادر الأمن السيبراني في المملكة العربية السعودية. وفيما يلي تعريف بمكونات هيكل هذا الإطار.

• **الدور الوظيفي**: هو مجموعة من مهام الأمن السيبراني المطلوب أداؤها في وظيفة أمن سيبراني محددة. ويتم تعريف الدور الوظيفي من خلال مجموعة من المهام المطلوب أداؤها في سياق هذا الدور الوظيفي، وكذلك قائمة المعارف والمهارات

[1] المنشور الخاص رقم ٨٠٠-١٨١، الصادر عن المعهد الوطني الأمريكي للمعايير والتقنية، " إطار كوادر المبادرة الوطنية لتعليم الأمن السيبراني (NICE)"، ٢٠١٧.

https://doi.org/10.6028/NIST.SP.800-181

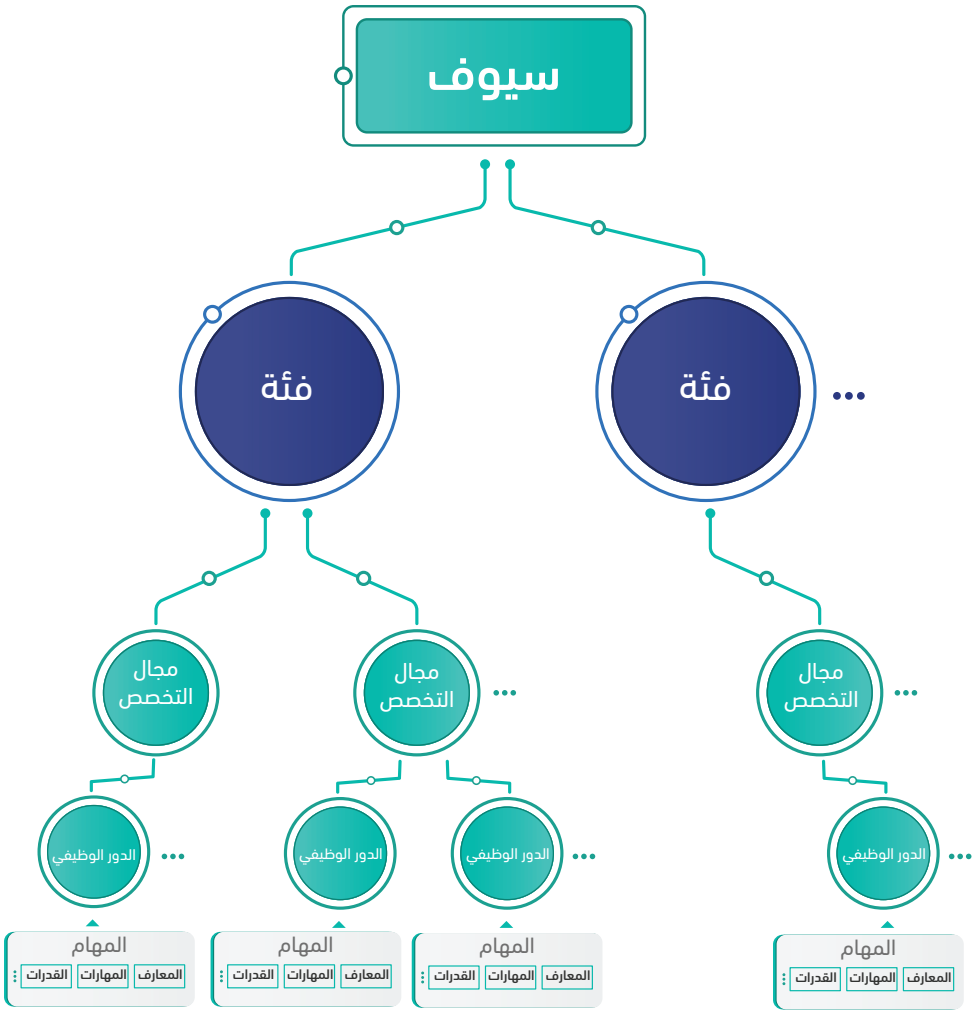
والقدرات اللازمة لأداء تلك المهام. ويحوي "الملحق أ" قائمة بجميع الأدوار الوظيفية للإطار السعودي لكوادر الأمن السيبراني.

- **مجال التخصص**: هو مجموعة من الأدوار الوظيفية التي تخدم وظيفة محددة في مجال الأمن السيبراني، وتتشارك في المهام والمعارف والمهارات والقدرات المطلوبة.
- **الفئة**: هي مجموعة من مجالات التخصص التي تخدم عددًا من وظائف الأمن السيبراني ذات العلاقة فيما بينها.

يقتصر هذا الإطار على الأدوار الوظيفية ذات العلاقة بالأمن السيبراني. وتوجد أدوار وظيفية أخرى خارج نطاق أدوار وظائف الأمن السيبراني ولكنها تتضمن بعض مسؤوليات الأمن السيبراني أو تتطلب بعض المعارف والمهارات والقدرات الخاصة بالأمن السيبراني، وأغلب تلك الأدوار الوظيفية تتعلق بمجال تقنية المعلومات، وهي خارج نطاق هذا الإطار. ومن المفترض أن يمتلك جميع الموظفين والمستفيدين من خدمات تقنية المعلومات قدراً مناسباً من الوعي بمخاطر الأمن السيبراني وممارساته المثلى.

يوضح (الشكل ١) هيكل الإطار السعودي لكوادر الأمن السيبراني.

(الشكل ١): هيكل الإطار السعودي لكوادر الأمن السيبراني



٢. تصنيف الإطار السعودي لكوادر الأمن السيبراني

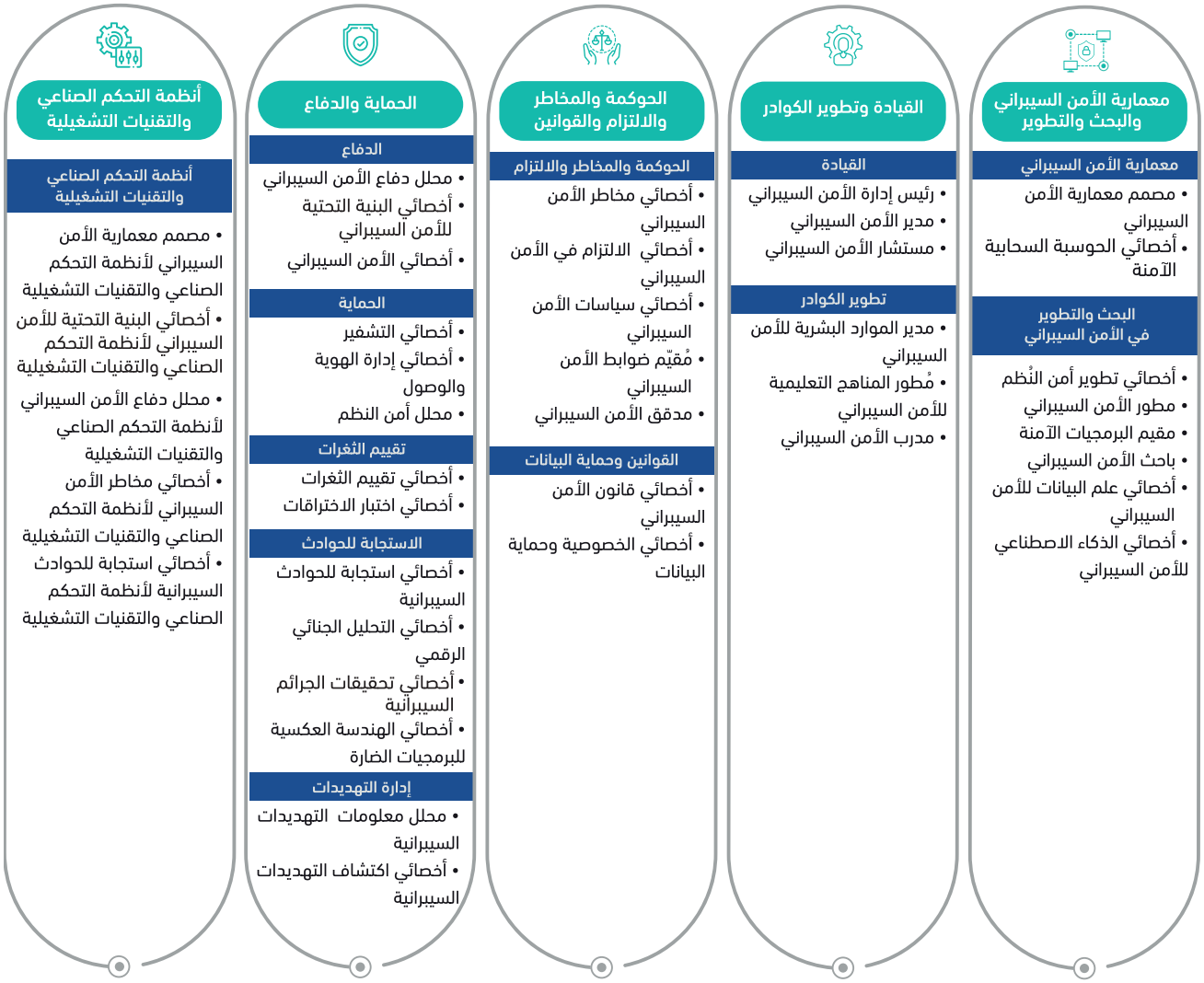
يتضمن الإطار السعودي لكوادر الأمن السيبراني خمس فئات عمل واثني عشر مجال تخصص وأربعين دوراً وظيفياً. ويتم تعريفها جميعا من خلال وصف موجز للأعمال التي يتم أداؤها في سياق الفئة المخصصة أو مجال التخصص أو الدور الوظيفي. ويرتبط كل دور وظيفي بمجموعة من المهام المطلوب أداؤها في سياق ذلك الدور الوظيفي، وقائمة بالمعارف والمهارات والقدرات اللازمة لأداء تلك المهام.

- **المعرفة**: هي مجموعة من البيانات والحقائق والمعلومات والنظريات والمفاهيم والقضايا والتوجهات ذات الصلة بموضوع معين.
- **المهارة**: هي القدرة على تطبيق المعرفة وتسخير الأدوات والأساليب المناسبة لأداء مهمة ما.
- **القدرة**: هي الكفاءة المستندة إلى السلوك والواجب توفرها لأداء العمل في مجال معين.
- **المهمة**: هي مجموعة من الأنشطة التي يجب إكمالها كجزء من دور وظيفي معين.

إن المهام والمعارف والمهارات والقدرات المطلوبة لأداء كل دور وظيفي في هذا الإطار قد تم تطويرها باستخدام المهام والمعارف والمهارات والقدرات المقدمة في إطار المبادرة الوطنية لتعليم الأمن السيبراني (NICE) مع عمل ما يلزم من التعديلات لعكس احتياجات كوادر الأمن السيبراني في المملكة. ويحتوي "الملحق ب" على قوائم بجميع المهام والمعارف والمهارات والقدرات المستخدمة في هذا الإطار.

يبين (الشكل٢) كل الفئات ومجالات التخصص والأدوار الوظيفية في الإطار السعودي لكوادر الأمن السيبراني.

(الشكل ٢): تصنيف الإطار السعودي لكوادر الأمن السيبراني



يوضح (الجدول ١) فئات الإطار السعودي لكوادر الأمن السيبراني. ويلاحظ أن كل فئة لديها مُعرّف فريد يتكون من الأحرف الأولى من اسم الفئة باللغة الإنجليزية (مثال: PD الذي يرمز إلى فئة الحماية والدفاع - Protection and Defense). وهذا المُعرّف يمثل جزءًا من مُعرّف الدور الوظيفي لكل الأدوار الوظيفية التي تندرج تحت الفئة كما هو موضح في تفاصيل الأدوار الوظيفية في "الملحق أ".

(جدول ١): فئات الإطار السعودي لكوادر الأمن السيبراني

الفئة	الوصف
معمارية الأمن السيبراني والبحث والتطوير (CARD)	تنفيذ أعمال التصميم والمعمارية والبحوث والتطوير في مجال الأمن السيبراني.
القيادة وتطوير الكوادر (LWD)	قيادة وتطوير فرق عمل الأمن السيبراني وأعمالها ، وتطوير كوادر الأمن السيبراني.
الحوكمة والمخاطر والالتزام والقوانين (GRCL)	تطوير سياسات الأمن السيبراني للمنظمة، وحوكمة هياكل الأمن السيبراني وعملياته، وإدارة مخاطر الأمن السيبراني، وضمان الالتزام بمتطلبات إدارة المخاطر والأمن السيبراني للمنظمة والمتطلبات القانونية ذات الصلة.
الحماية والدفاع (PD)	تحديد تهديدات وثغرات نُظم وشبكات تقنية المعلومات، وتحليلها ومراقبتها والتعامل معها وإدارتها، واستخدام التدابير الدفاعية، والمعلومات التي تم الحصول عليها من مصادر متنوعة، للإبلاغ عن الأحداث والاستجابة للحوادث.
أنظمة التحكم الصناعي والتقنيات التشغيلية(ICS/OT)	تنفيذ أعمال الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية.

يصف (الجدول ٢) مجالات التخصص للإطار السعودي لكوادر الأمن السيبراني والفئات التي تنتمي إليها؛ فكل مجال تخصص لديه مُعرّف فريد يتكون من الأحرف الأولى من اسم مجال التخصص باللغة الإنجليزية، (مثال : VA يرمز لمجال تخصص تقييم الثغرات Vulnerability Assessment). ويستخدم هذا المُعرّف مع مُعرّف الفئة عند إنشاء مُعرّفات الأدوار الوظيفية للأدوار الوظيفية التي تنتمي لكل مجال تخصص كما في الوصف في "ملحق أ".

(جدول ٢) : مجالات التخصص في الإطار السعودي لكوادر الأمن السيبراني

الفئة	مجال التخصص	الوصف
معمارية الأمن السيبراني والبحث والتطوير (CARD)	معمارية الأمن السيبراني (CA)	تصميم أنظمة الأمن السيبراني ومكوناته التابعة لنظم وشبكات تقنية المعلومات، والإشراف على تطويرها وتنفيذها.
	البحث والتطوير في الأمن السيبراني (CRD)	القيام بأعمال البحث والتطوير في مجال الأمن السيبراني.
القيادة وتطوير الكوادر (LWD)	القيادة (L)	الإشراف على فرق الأمن السيبراني وأعمالها، وإدارتها وقيادتها.
	تطوير الكوادر (WD)	تطبيق معارف ومهارات الأمن السيبراني ومنهجيات تعليم وتطوير الموارد البشرية لتطوير مهارات كوادر الأمن السيبراني وإدارتها والحفاظ عليها وتحسينها.
الحوكمة والمخاطر والالتزام والقوانين (GRCL)	الحوكمة والمخاطر والالتزام (GRC)	حوكمة هياكل الأمن السيبراني وعملياته، وإدارة مخاطر الأمن السيبراني، وضمان تلبية متطلبات إدارة المخاطر والأمن السيبراني للمنظمة لكافة نُظم وتقنيات المعلومات. وكذلك تطوير سياسات الأمن السيبراني داخل المنظمة وتحديثها.
	القوانين وحماية البيانات (LDP)	ضمان التزام المنظمة بقوانين وتنظيمات الأمن السيبراني وحماية البيانات.
الحماية والدفاع(PD)	الدفاع (D)	استخدام أدوات المراقبة والتحليل لتحديد الأحداث وتحليلها والكشف عن حوادث الأمن السيبراني.
	الحماية (P)	استخدام أدوات الأمن السيبراني لحماية المعلومات والأنظمة والشبكات من التهديدات السيبرانية.
	تقييم الثغرات (VA)	اختبار نُظم وشبكات تقنية المعلومات، وتقييم التهديدات والثغرات.
	الاستجابة للحوادث (IR)	مباشرة الحوادث السيبرانية وتحليلها والاستجابة لها.
	إدارة التهديدات (TM)	جمع وتحليل المعلومات عن التهديدات والبحث عن التهديدات غير المكتشفة، وتقديم رؤى قابلة للتطبيق لدعم عمليات اتخاذ القرار في الأمن السيبراني.
أنظمة التحكم الصناعي والتقنيات التشغيلية (ICS/OT)	أنظمة التحكم الصناعي والتقنيات التشغيلية (ICS/OT)	القيام بأعمال الأمن السيبراني المتعلقة بالحوكمة وإدارة المخاطر، ومتابعة الالتزام، والتصميم والتطوير، والتشغيل والإشراف، والحماية والدفاع في نظم التقنيات التشغيلية التي تشمل نُظم التحكم الصناعي، ونُظم التحكم الإشرافي وحيازة البيانات «سكادا».

٢-١ الأدوار الوظيفية في فئة معمارية الأمن السيبراني والبحث والتطوير (CARD)

(الجدول ٣) يصف الأدوار الوظيفية في فئة معمارية الأمن السيبراني والبحث والتطوير.

(جدول ٣): الأدوار الوظيفية في فئة معمارية الأمن السيبراني والبحث والتطوير (CARD)

الرقم	مجال التخصص	الدور الوظيفي	مُعرّف الدور الوظيفي	الوصف
١	معمارية الأمن السيبراني (CA)	مصمم معمارية الأمن السيبراني	CARD-CA-001	تصميم نُظم وشبكات الأمن السيبراني، والإشراف على إعداداتها وتطويرها وتنفيذها.
٢		أخصائي الحوسبة السحابية الآمنة	CARD-CA-002	تصميم نُظم الحوسبة السحابية الآمنة وتنفيذها وتشغيلها، مع تطوير سياسات السحابة الآمنة.
٣	البحث والتطوير في الأمن السيبراني (CRD)	أخصائي تطوير أمن النُظم	CARD-CRD-001	تصميم أمن نُظم المعلومات وتطويره واختباره وتقييمه في كافة مراحل تطوير تلك النُظم.
٤		مطور الأمن السيبراني	CARD-CRD-002	تطوير برمجيات الأمن السيبراني وتطبيقاته ونُظمه ومنتجاته.
٥		مقيم البرمجيات الآمنة	CARD-CRD-003	تقييم أمن تطبيقات الحاسب وبرمجياته وشفراته أو برامجه، مع تقديم نتائج قابلة للتطبيق.
٦		باحث الأمن السيبراني	CARD-CRD-004	إجراء الأبحاث العلمية في مجال الأمن السيبراني.
٧		أخصائي علم البيانات للأمن السيبراني	CARD-CRD-005	استخدام نماذج رياضية ومنهجيات وعمليات علمية لتصميم وتنفيذ خوارزميات وأنظمة لاستخلاص استنتاجات ومعارف الأمن السيبراني من مصادر متعددة لمجموعة بيانات واسعة النطاق.
٨		أخصائي الذكاء الاصطناعي للأمن السيبراني	CARD-CRD-006	استخدام نماذج الذكاء الاصطناعي وتقنياته (شاملا أساليب التعلم الآلي) لتصميم وتنفيذ خوارزميات وأنظمة لأتمتة وتحسين كفاءة وفعالية مهام الأمن السيبراني.

٢-٢ الأدوار الوظيفية في فئة القيادة وتطوير الكوادر (LWD)

(الجدول ٤) يصف الأدوار الوظيفية في فئة القيادة وتطوير الكوادر.

(جدول ٤): الأدوار الوظيفية في فئة القيادة وتطوير الكوادر (LWD)

الرقم	مجال التخصص	الدور الوظيفي	مُعرّف الدور الوظيفي	الوصف
٩	القيادة (L)	رئيس إدارة الأمن السيبراني	LWD-L-001	إدارة أعمال الأمن السيبراني داخل المنظمة، ووضع الرؤية والتوجه بشأن الأمن السيبراني، والاستراتيجيات والموارد والأنشطة ذات العلاقة وتقديم المرئيات لقيادة المنظمة حيال أساليب الإدارة الفعّالة لمخاطر الأمن السيبراني للمنظمة.
١٠		مدير الأمن السيبراني	LWD-L-002	إدارة الأمن السيبراني للوظائف والنُظم المعلوماتية داخل المنظمة. وقيادة الأمن السيبراني سواء على مستوى فريق أو وحدة أو وظيفة على المستوى المؤسسي.
١١		مستشار الأمن السيبراني	LWD-L-003	تقديم الرأي والمشورة لقيادة المنظمة وقادة وفرق الأمن السيبراني في مواضيع الأمن السيبراني.
١٢	تطوير الكوادر (WD)	مدير الموارد البشرية للأمن السيبراني	LWD-WD-001	تطوير الخطط والاستراتيجيات والإرشادات داخل المنظمة لدعم تطوير كوادر الأمن السيبراني وإدارتها.
١٣		مُطور المناهج التعليمية للأمن السيبراني	LWD-WD-002	تطوير وتخطيط وتنسيق وتقييم برامج التعليم والتدريب للأمن السيبراني والمناهج ومحتوياتها وطرقها وأساليب تقديمها، حسب الاحتياجات التعليمية.
١٤		مدرب الأمن السيبراني	LWD-WD-003	تعليم الأفراد وتدريبهم وتطويرهم واختبارهم في موضوعات الأمن السيبراني.

٢-٣ الأدوار الوظيفية في فئة الحوكمة والمخاطر والالتزام والقوانين (GRCL)

(الجدول ٥) يصف الأدوار الوظيفية في فئة الحوكمة والمخاطر والالتزام والقوانين.

(جدول ٥): الأدوار الوظيفية في فئة الحوكمة والمخاطر والالتزام والقوانين (GRCL)

الرقم	مجال التخصص	الدور الوظيفي	مُعرّف الدور الوظيفي	الوصف
١٥	الحوكمة والمخاطر والالتزام (GRC)	أخصائي مخاطر الأمن السيبراني	GRCL-GRC-001	تحديد مخاطر الأمن السيبراني للمنظمة وتقييمها وإدارتها لحماية أصولها المعلوماتية والتقنية وفقًا لسياسات وإجراءات المنظمة، وكذلك القوانين والأنظمة ذات العلاقة.
١٦		أخصائي الالتزام في الأمن السيبراني	GRCL-GRC-002	ضمان التزام برنامج الأمن السيبراني للمنظمة بالمتطلبات والسياسات والمعايير المعمول بها.
١٧		أخصائي سياسات الأمن السيبراني	GRCL-GRC-003	تطوير سياسات الأمن السيبراني وتحديثها، لدعم متطلبات الأمن السيبراني بالمنظمة ومواءمتها.
١٨		مُقيّم ضوابط الأمن السيبراني	GRCL-GRC-004	تحليل ضوابط الأمن السيبراني وتقييم فاعليتها.
١٩		مدقق الأمن السيبراني	GRCL-GRC-005	تصميم عمليات التدقيق للأمن السيبراني وتنفيذها وإدارتها بهدف تقييم مدى التزام المنظمة بالمتطلبات والسياسات والمعايير والضوابط المعمول بها، وإعداد تقارير التدقيق وتقديمها للأطراف ذات الصلاحية.
٢٠	القوانين وحماية البيانات (LDP)	أخصائي قانون الأمن السيبراني	GRCL-LDP-001	تقديم الخدمات القانونية بشأن الموضوعات ذات الصلة بالقوانين والأنظمة السيبرانية.
٢١		أخصائي الخصوصية وحماية البيانات	GRCL-LDP-002	دراسة هيكلة البيانات الشخصية وقوانين وأنظمة الخصوصية المعمول بها، مع تحليل مخاطر الخصوصية، وتطوير برنامج المنظمة للمواءمة مع ضوابط الخصوصية وحماية البيانات والسياسات الداخلية، والإشراف على تنفيذها، مع دعم استجابة المنظمة لحوادث الخصوصية أو حماية البيانات.

٤-٢ الأدوار الوظيفية في فئة الحماية والدفاع (PD)

(الجدول ٦) يصف الأدوار الوظيفية في فئة الحماية والدفاع.

(جدول ٦): الأدوار الوظيفية في فئة الحماية والدفاع (PD)

الرقم	مجال التخصص	الدور الوظيفي	مُعرّف الدور الوظيفي	الوصف
٢٢	الدفاع (D)	محلل دفاع الأمن السيبراني	PD-D-001	استخدام البيانات التي تم استخلاصها من مجموعة أدوات الدفاع السيبراني لتحليل الأحداث الواقعة داخل المنظمة بهدف الكشف عن التهديدات والتعامل معها.
٢٣		أخصائي البنية التحتية للأمن السيبراني	PD-D-002	فحص وتنصيب وصيانة الأجهزة والبرمجيات المستخدمة للدفاع وحماية الأنظمة والشبكات من التهديدات السيبرانية وتشغيلها والإشراف عليها.
٢٤		أخصائي الأمن السيبراني	PD-D-003	تقديم الدعم العام للأمن السيبراني، والمساعدة في مهام الأمن السيبراني.
٢٥	الحماية (P)	أخصائي التشفير	PD-P-001	تطوير أنظمة التشفير وخوارزمياته، وتقييمها وتحليلها وتحديد نقاط ضعفها وسبل تحسينها.
٢٦		أخصائي إدارة الهوية والوصول	PD-P-002	إدارة هوية الأفراد والكيانات، وصلاحيات وصولهم إلى الموارد من خلال تطبيق أنظمة وعمليات التعريف والتوثيق والتصريح.
٢٧		محلل أمن النظم	PD-P-003	تطوير أمن النظم واختباره وصيانته، وتحليل أمن العمليات والأنظمة المدمجة.
٢٨	تقييم الثغرات (VA)	أخصائي تقييم الثغرات	PD-VA-001	تقييم ثغرات النُظم والشبكات، وتحديد مواطن انحرافها عن الإعدادات المقبولة أو السياسات المعمول بها، وقياس فاعلية البنية الدفاعية متعددة الطبقات ضد الثغرات المعروفة.
٢٩		أخصائي اختبار الاختراقات	PD-VA-002	أداء محاولات اختراق مصرح لها لأنظمة الحاسبات أو الشبكات والمنشآت المادية باستخدام أساليب تهديد واقعية لتقييم حالتها الأمنية وكشف الثغرات المحتملة.

٣٠	الاستجابة للحوادث (IR)	أخصائي استجابة للحوادث السيبرانية	PD-IR-001	مباشرة الحوادث المتعلقة بالأمن السيبراني وتحليلها والاستجابة لها.
٣١		أخصائي التحليل الجنائي الرقمي	PD-IR-002	جمع الأدلة الرقمية وتحليلها، والتحقيق في حوادث الأمن السيبراني لاستخلاص معلومات مفيدة لمعالجة ثغرات النُظم والشبكات.
٣٢		أخصائي تحقيقات الجرائم السيبرانية	PD-IR-003	تعريف الأدلة وجمعها وفحصها والحفاظ عليها، باستخدام أساليب تحرٍ واستقصاء موثقة ومقننة.
٣٣		أخصائي الهندسة العكسية للبرمجيات الضارة	PD-IR-004	تحليل البرمجيات الضارة (عن طريق تفكيكها وإعادتها إلى صيغة برمجية مفهومة)، وفهم طريقة عملها وتأثيرها وغرضها، وتقديم توصيات للوقاية منها والاستجابة للحوادث الناتجة عنها.
٣٤	إدارة التهديدات (TM)	محلل معلومات التهديدات السيبرانية	PD-TM-001	جمع معلومات عن التهديدات السيبرانية من مصادر مختلفة وتحليلها لتكوين فهم وإدراك عميقين للتهديدات السيبرانية، وخطط المخترقين، والأساليب والإجراءات المتبعة، لاستنباط وتوثيق مؤشرات من شأنها مساعدة المنظمات في الكشف عن الحوادث السيبرانية والتنبؤ بها، وحماية النُظم والشبكات من التهديدات السيبرانية.
٣٥		أخصائي اكتشاف التهديدات السيبرانية	PD-TM-002	البحث الاستباقي عن التهديدات غير المكتشفة في الشبكات والنُظم، وتحديد مؤشرات الاختراق، وتقديم التوصيات للتعامل معها.

٥-٢ الأدوار الوظيفية في فئة أنظمة التحكم الصناعي والتقنيات التشغيلية (ICS/OT)

(الجدول ٧) يصف الأدوار الوظيفية في فئة أنظمة التحكم الصناعي والتقنيات التشغيلية.

(جدول ٧): الأدوار الوظيفية في فئة أنظمة التحكم الصناعي والتقنيات التشغيلية (ICS/OT)

الرقم	مجال التخصص	الدور الوظيفي	مُعرّف الدور الوظيفي	الوصف
٣٦	أنظمة التحكم الصناعي والتقنيات التشغيلية (ICS/OT)	مصمم معمارية الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	ICSOT- ICSOT-001	تصميم نُظم وشبكات الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية والإشراف على إعداداتها وتطويرها وتنفيذها.
٣٧		أخصائي البنية التحتية للأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	ICSOT- ICSOT-002	فحص وتنصيب وصيانة الأجهزة والبرمجيات المستخدمة للدفاع وحماية الأنظمة والشبكات من التهديدات السيبرانية في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية وتشغيلها والإشراف عليها.
٣٨		محلل دفاع الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	ICSOT- ICSOT-003	استخدام البيانات، التي تم جمعها من مجموعة متنوعة من أدوات الأمن السيبراني لتحليل الأحداث الواقعة في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية بهدف الكشف عن تهديدات الأمن السيبراني والتعامل معها.
٣٩		أخصائي مخاطر الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية	ICSOT- ICSOT-004	تحديد مخاطر الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية وتقييمها وإدارتها، مع تقييم وتحليل فاعلية ضوابط الأمن السيبراني القائمة، وتقديم الملاحظات والتوصيات بناء على تلك التقييمات.
٤٠		أخصائي استجابة للحوادث السيبرانية لأنظمة التحكم الصناعي والتقنيات التشغيلية	ICSOT- ICSOT-005	مباشرة حوادث الأمن السيبراني وتحليلها والاستجابة لها في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية.

للاطلاع على المهام والمعارف والمهارات والقدرات المطلوبة لكل دور وظيفي والمهام المرتبطة به يُرجى الاطلاع على "الملحق أ".

٣ الملاحق

٣-١ الملحق أ: تفاصيل الدور الوظيفي

٣-١-١ مجموعة الفئة: معمارية الأمن السيبراني والبحث والتطوير (CARD)

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مُصمِم معمارية الأمن السيبراني
معرف الدور الوظيفي	CARD-CA-001
الفئة	معمارية الأمن السيبراني والبحث والتطوير
مجال التخصص	معمارية الأمن السيبراني
وصف الدور الوظيفي	تصميم نُظم وشبكات الأمن السيبراني، والإشراف على إعداداتها وتطويرها وتنفيذها.
المهام	T0036, T0043, T0507, T0508, T0509, T0510, T0511, T0512, T0514, T0515, T0516, T0517, T0518, T0519, T0520, T0523, T0524, T0525, T0526, T0527, T0528, T0529, T0530, T0531, T2511, T4502
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0014, K0016, K0017, K0020, K0021, K0022, K0023, K0025, K0026, K0027, K0028, K0034, K0035, K0040, K0041, K0042, K0044, K0045, K0046, K0048, K0053, K0057, K0058, K0061, K0062, K0074, K0093, K0101, K0109, K0111, K0112, K0116, K0120, K0124, K0125, K0126, K0129, K0131, K0133, K0146, K0148, K0149, K0151, K0503, K0504, K0505, K0506, K0507, K0508, K0509, K0510, K0511, K0512, K0513, K0514, K0515, K1015, K1036, K1505, K4000, K5503
المهارات	S0003, S0007, S0008, S0010, S0016, S0021, S0027, S0038, S0039, S0061, S0064, S0065, S0501, S0502, S0503, S0504, S0505, S0506, S1008
القدرات	A0003, A0009, A0010, A0011, A0013, A0035, A0043, A0044, A0500, A0502, A0503, A0504, A2504

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي الحوسبة السحابية الآمنة
معرف الدور الوظيفي	CARD-CA-002
الفئة	معمارية الأمن السيبراني والبحث والتطوير
مجال التخصص	معمارية الأمن السيبراني
وصف الدور الوظيفي	تصميم نُظم الحوسبة السحابية الآمنة وتنفيذها وتشغيلها، مع تطوير سياسات السحابة الآمنة.
المهام	T0134, T0500, T0501, T0502, T0503, T0504, T0505, T0506, T0521, T0522
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0014, K0019, K0025, K0044, K0045, K0046, K0048, K0071, K0074, K0084, K0085, K0106, K0121, K0132, K0500, K0502, K1011, K2001
المهارات	S0012, S0019, S0060, S0500
القدرات	A0009, A0034, A0501

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي تطوير أمن النظم
معرف الدور الوظيفي	CARD-CRD-001
الفئة	معمارية الأمن السيبراني والبحث والتطوير
مجال التخصص	البحث والتطوير في الأمن السيبراني
وصف الدور الوظيفي	تصميم أمن نُظم المعلومات وتطويره واختباره وتقييمه في كافة مراحل تطوير تلك النُظم.
المهام	T0004, T0006, T0007, T0012, T0013, T0022, T0039, T0043, T0096, T0105, T0506, T0508, T1004, T1007, T1008, T1015, T1016, T1017, T1018, T1021, T1022, T1026, T1027, T1031, T1033, T1034, T1038, T1042, T1044, T1047, T1048, T1049, T1053, T1056, T1063, T1079, T1084, T1087, T1088, T1089, T1090, T2512
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0020, K0022, K0023, K0026, K0027, K0035, K0038, K0040, K0041, K0042, K0045, K0046, K0048, K0049, K0050, K0056, K0057, K0058, K0062, K0073, K0074, K0076, K0092, K0093, K0100, K0101, K0111, K0113, K0124, K0125, K0126, K0130, K0133, K0136, K0140, K0146, K0148, K0149, K0151, K1004, K1006, K1007, K1008, K1009, K1011, K1014, K1015, K1017, K1018, K1036, K1504 , K5503
المهارات	S0001, S0007, S0008, S0012, S0028, S0061, S1004, S1007, S1008, S1027, S2512
القدرات	A0001, A0002, A0003, A0005, A0009, A0010, A0011, A0012, A0013, A0019, A0032, A0035, A0044, A0500, A1005, A2503, A2507, A2511, A2513, A2524

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مطور الأمن السيبراني
معرف الدور الوظيفي	CARD-CRD-002
الفئة	معمارية الأمن السيبراني والبحث والتطوير
مجال التخصص	البحث والتطوير في الأمن السيبراني
وصف الدور الوظيفي	تطوير برمجيات الأمن السيبراني وتطبيقاته ونُظمه ومنتجاته.
المهام	T0035, T0039, T0040, T0091, T0114, T1002, T1003, T1005, T1006, T1009, T1010, T1011, T1013, T1014, T1023, T1030, T1031, T1035, T1036, T1040, T1043, T1054, T1055, T1071, T1075, T1078, T1080, T1085, T1092, T5060
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0022, K0030, K0035, K0039, K0045, K0050, K0051, K0052, K0074, K0076, K0083, K0093, K0100, K0110, K0112, K0124, K0125, K0126, K0127, K0146, K0147, K1000, K1004, K1008, K1011, K1012, K1013, K1014, K1015, K1017, K1018, K1019, K1021, K1022, K1023 , K1039, K1040, K5503
المهارات	S0001, S0007, S0017, S0036, S0038, S0047, S0048, S0061, S1001, S1002, S1003, S1007, S1008, S1026, S1031, S1034
القدرات	A0035, A0044, A1000, A1001, A1004

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مقيم البرمجيات الآمنة
معرف الدور الوظيفي	CARD-CRD-003
الفئة	معمارية الأمن السيبراني والبحث والتطوير
مجال التخصص	البحث والتطوير في الأمن السيبراني
وصف الدور الوظيفي	تقييم أمن تطبيقات الحاسب وبرمجياته وشفراته أو برامجه، مع تقديم نتائج قابلة للتطبيق.
المهام	T0039, T0040, T0077, T1005, T1006, T1009, T1012, T1013, T1024, T1030, T1031, T1035, T1040, T1041, T1043, T1046, T1054, T1055, T1076, T1077, T1078, T1081, T1082, T1086, T1092 , T1104
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0015, K0022, K0030, K0035, K0039, K0045, K0050, K0051, K0052, K0074, K0076, K0083, K0093, K0100, K0110, K0112, K0124, K0125, K0126, K0127, K0146, K0153, K0168, K1000, K1004, K1008, K1011, K1012, K1013, K1014, K1015, K1017, K1018, K1019, K1021, K1022, K1023, K1024, K1037, K5503
المهارات	S0001, S0007, S0036, S0038, S0047, S0048, S0061, S1007, S1008, S1010
القدرات	A0035, A0044, A1001

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	باحث الأمن السيبراني
معرف الدور الوظيفي	CARD-CRD-004
الفئة	معمارية الأمن السيبراني والبحث والتطوير
مجال التخصص	البحث والتطوير في الأمن السيبراني
وصف الدور الوظيفي	إجراء الأبحاث العلمية في مجال الأمن السيبراني.
المهام	T0052, T0089, T0090, T1019, T1045, T1050, T1051, T1057, T1058, T1073, T1074, T1091, T1093
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0017, K0044, K0056, K0073, K0074, K0092, K0093, K0094, K0095, K0096, K0097, K0098, K0100, K0112, K0114, K0128, K0135, K0143, K0153, K0159, K1026, K1029, K1030, K1031, K1032, K1033, K1034, K1035, K1038
المهارات	S0003, S0018, S0045, S1002, S1024, S1025, S1028
القدرات	A0001, A0004, A0005, A0044

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي علم البيانات للأمن السيبراني
معرف الدور الوظيفي	CARD-CRD-005
الفئة	معمارية الأمن السيبراني والبحث والتطوير
مجال التخصص	البحث والتطوير في الأمن السيبراني
وصف الدور الوظيفي	استخدام نماذج رياضية ومنهجيات وعمليات علمية لتصميم وتنفيذ خوارزميات وأنظمة لاستخلاص استنتاجات ومعارف الأمن السيبراني من مصادر متعددة لمجموعة بيانات واسعة النطاق.
المهام	T0080, T0083, T0084, T1000, T1001, T1020, T1034, T1037, T1039, T1059, T1060, T1061, T1062, T1064, T1065, T1066, T1067, T1068, T1069, T1070, T1071, T1072, T1083, T1103
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0015, K0018, K0039, K0040, K0042, K0045, K0049, K0051, K0059, K0074, K0076, K0105, K0108, K0156, K1001, K1002, K1003, K1005, K1010, K1016, K1020, K1021, K1025, K1027, K1028, K1036
المهارات	S0017, S0029, S0030, S0031, S0032, S1000, S1002, S1005, S1006, S1009, S1011, S1012, S1013, S1014, S1015, S1016, S1017, S1018, S1019, S1020, S1021, S1022, S1023, S1027, S1029, S1030 , S1034
القدرات	A0008, A0014, A1002, A1003, A2509

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي الذكاء الاصطناعي للأمن السيبراني
معرف الدور الوظيفي	CARD-CRD-006
الفئة	معمارية الأمن السيبراني والبحث والتطوير
مجال التخصص	البحث والتطوير في الأمن السيبراني
وصف الدور الوظيفي	استخدام نماذج الذكاء الاصطناعي وتقنياته (شاملا أساليب التعلم الآلي) لتصميم وتنفيذ خوارزميات وأنظمة لأتمتة وتحسين كفاءة وفعالية مهام الأمن السيبراني.
المهام	T0134, T1071, T1072, T1094, T1095, T1096, T1097, T1098, T1099, T1100, T1101, T1103
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0074, K0119, K1039, K1040, K1041, K1042, K1043, K1044, K1046, K1047
المهارات	S1031, S1032, S1033, S1034, S1035, S1036, S1037
القدرات	A1006, A1007, A1008

٣-١-٢ مجموعة الفئة: القيادة وتطوير الكوادر (LWD)

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	رئيس إدارة الأمن السيبراني
معرف الدور الوظيفي	LWD-L-001
الفئة	القيادة وتطوير الكوادر
مجال التخصص	القيادة
وصف الدور الوظيفي	إدارة أعمال الأمن السيبراني داخل المنظمة، ووضع الرؤية والتوجه بشأن الأمن السيبراني، والاستراتيجيات والموارد والأنشطة ذات العلاقة وتقديم المرئيات لقيادة المنظمة حيال أساليب الإدارة الفعّالة لمخاطر الأمن السيبراني للمنظمة.
المهام	T0002, T0008, T0059, T0077, T0081, T0085, T0093, T0095, T0105, T0126, T0127, T0128, T0137, T1500, T1501, T1503, T1511, T1515, T1525, T1526, T1528, T1529, T1531, T1534, T1535, T1536, T1541, T2000, T2003, T2007, T2008, T2009
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0021, K0052, K0054, K0064, K0073, K0074, K0080, K0082, K0092, K0093, K0135, K0143, K0153, K0168, K2021, K5503
المهارات	S0010, S0058, S0059, S1500, S1501, S1502, S1503, S3001
القدرات	A0006, A0015, A0017, A0021, A0024, A0025, A0029, A0030, A0031, A0032, A1500, A1501

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مدير الأمن السيبراني
معرف الدور الوظيفي	LWD-L-002
الفئة	القيادة وتطوير الكوادر
مجال التخصص	القيادة
وصف الدور الوظيفي	إدارة الأمن السيبراني للوظائف والنُظم المعلوماتية داخل المنظمة. وقيادة الأمن السيبراني سواء على مستوى فريق أو وحدة أو وظيفة على المستوى المؤسسي.
المهام	T0001, T0002, T0008, T0016, T0020, T0023, T0048, T0053, T0059, T0061, T0063, T0115, T0137, T1500, T1502, T1503, T1504, T1505, T1506, T1507, T1508, T1509, T1510, T1511, T1512, T1514, T1515, T1516, T1517, T1518, T1519, T1520, T1521, T1522, T1523, T1524, T1525, T1526, T1527, T1528, T1529, T1530, T1531, T1532, T1533, T1534, T1542, T2000, T2001, T2007, T2008, T2009, T2510, T2514
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0016, K0019, K0021, K0024, K0029, K0031, K0033, K0034, K0036, K0037, K0043, K0044, K0046, K0052, K0056, K0061, K0064, K0073, K0074, K0082, K0090, K0091, K0092, K0093, K0100, K0101, K0110, K0118, K0124, K0125, K0126, K0128, K0133, K0148, K0150, K0153, K0168, K0169, K1500, K1501, K1502, K1503, K1504, K1505, K1506, K1507, K1509, K1511, K2501 , K5503
المهارات	S0010, S1500, S1501, S3001
القدرات	A0036, A0044, A1502

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مستشار الأمن السيبراني
معرف الدور الوظيفي	LWD-L-003
الفئة	القيادة وتطوير الكوادر
مجال التخصص	القيادة
وصف الدور الوظيفي	تقديم الرأي والمشورة لقيادة المنظمة وقادة وفرق الأمن السيبراني، في مواضيع الأمن السيبراني.
المهام	T0001, T0002, T0093, T1501, T1503, T1511, T1515, T1525, T1528, T1529, T1537, T1538, T1539, T1540, T2001, T2003, T2052
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0016, K0019, K0021, K0029, K0031, K0033, K0034, K0036, K0037, K0044, K0046, K0052, K0056, K0061, K0064, K0073, K0074, K0082, K0090, K0091, K0092, K0093, K0100, K0101, K0110, K0118, K0124, K0128, K0133, K0148, K0150, K0153, K0169, K1500, K1501, K1502, K1503, K1504, K1505, K1506, K1507, K1509, K1510, K1511, K5503
المهارات	S0058, S1500, S1501, S1502, S1503
القدرات	A0006, A0015, A0017, A0021, A0024, A0025, A0029, A0030, A0031, A0032, A0043, A1500, A1501

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مدير الموارد البشرية للأمن السيبراني
معرف الدور الوظيفي	LWD-WD-001
الفئة	القيادة وتطوير الكوادر
مجال التخصص	تطوير الكوادر
وصف الدور الوظيفي	تطوير الخطط والاستراتيجيات والإرشادات داخل المنظمة لدعم تطوير كوادر الأمن السيبراني وإدارتها.
المهام	T0002, T0008, T0017, T0020, T0045, T0046, T0078, T0081, T0082, T0085, T0086, T0088, T0092, T0093, T0095, T0099, T0103, T0104, T0108, T0109, T0110, T1500, T1503, T2006, T2022, T2023, T2025, T2026, T2027, T2028, T2030, T2031, T2032, T2033, T2034, T2035, T2037, T2038, T2039, T2040, T2047, T2052, T2053
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0061, K0074, K0079, K0080, K0091, K0092, K0118, K0141, K0142, K0150, K1501, K2002, K2011, K2013, K2014, K2019
المهارات	S2008, S2508
القدرات	A0006, A2006, A2008, A2009, A2506, A2510

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مُطور المناهج التعليمية للأمن السيبراني
معرف الدور الوظيفي	LWD-WD-002
الفئة	القيادة وتطوير الكوادر
مجال التخصص	تطوير الكوادر
وصف الدور الوظيفي	تطوير وتخطيط وتنسيق وتقييم برامج التعليم والتدريب للأمن السيبراني والمناهج ومحتوياتها وطرقها وأساليب تقديمها، حسب الاحتياجات التعليمية.
المهام	T0052, T1528, T2011, T2012, T2021, T2022, T2024, T2028, T2029, T2036, T2040, T2041, T2044, T2045, T2050, T2052, T2054
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0044, K0074, K0079, K0080, K0133, K2000, K2002, K2003, K2004, K2006, K2007, K2009, K2012, K2014, K2015, K2016, K2018, K2021
المهارات	S0055, S2003, S2004, S2005, S2007, S2009
القدرات	A0002, A0003, A0004, A0005, A0015, A0016, A0019, A0024, A0025, A0027, A0028, A0031, A0032, A2004, A2005, A2007, A2010, A2011, A2013, A2014, A2015

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مدرب الأمن السيبراني
معرف الدور الوظيفي	LWD-WD-003
الفئة	القيادة وتطوير الكوادر
مجال التخصص	تطوير الكوادر
وصف الدور الوظيفي	تعليم الأفراد وتدريبهم وتطويرهم واختبارهم في موضوعات الأمن السيبراني.
المهام	T0083, T0084, T0087, T2002, T2004, T2005, T2010, T2011, T2012, T2013, T2014, T2015, T2016, T2017, T2018, T2019, T2020, T2022, T2028, T2029, T2042, T2043, T2045, T2046, T2048, T2049, T2051, T2052, T2054
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0044, K0071, K0074, K0079, K0080, K0133, K2000, K2001, K2002, K2003, K2004, K2006, K2007, K2008, K2009, K2010, K2012, K2014, K2015, K2016, K2018, K2019, K2020, K2021
المهارات	S0001, S0004, S0015, S0017, S0019, S0020, S0021, S0026, S0027, S0034, S0035, S0041, S0058, S1502, S2000, S2001, S2002, S2003, S2005, S2006, S2010, S2501, S2515, S2534, S2539, S4504, S4505, S4508, S5012, S5017
القدرات	A0002, A0003, A0004, A0005, A0014, A0015, A0016, A0019, A0024, A0025, A0027, A0028, A0031, A0032, A2001, A2002, A2003, A2004, A2005, A2007, A2011, A2013, A2014, A2015, A2502, A2503, A2504, A2505, A2506

٣-١-٣ مجموعة الفئة: الحوكمة والمخاطر والالتزام والقوانين (GRCL)

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي مخاطر الأمن السيبراني
معرف الدور الوظيفي	GRCL-GRC-001
الفئة	الحوكمة والمخاطر والالتزام والقوانين
مجال التخصص	الحوكمة والمخاطر والالتزام
وصف الدور الوظيفي	تحديد مخاطر الأمن السيبراني للمنظمة وتقييمها وإدارتها لحماية أصولها المعلوماتية والتقنية وفقًا لسياسات وإجراءات المنظمة، وكذلك القوانين والأنظمة ذات العلاقة.
المهام	T0001, T0006, T0012, T0013, T0014, T0020, T0039, T0043, T0053, T0105, T0128, T0129, T0130, T0131, T0132, T0133, T2500, T2513
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0029, K0037, K0073, K0074, K0080, K0081, K0082, K0083, K0089, K0092, K0107, K0127, K0160, K0162, K0166, K0167, K0508, K5503
المهارات	S0044, S0057, S0062
القدرات	A0033, A0037, A0038, A0039, A0040, A0041, A0042, A0045, A2501

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي الالتزام في الأمن السيبراني
معرف الدور الوظيفي	GRCL-GRC-002
الفئة	الحوكمة والمخاطر والالتزام والقوانين
مجال التخصص	الحوكمة والمخاطر والالتزام
وصف الدور الوظيفي	ضمان التزام برنامج الأمن السيبراني للمنظمة بالمتطلبات والسياسات والمعايير المعمول بها.
المهام	T0003, T0019, T0022, T0023, T0063, T0111, T2500, T2501, T2502, T2504, T2506, T2509, T2514, T2518, T2519, T3052
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0074, K0091, K0165, K0118, K2508, K5503
المهارات	S0058, S0061
القدرات	A0006, A0007, A0023, A0024, A0026, A2005

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي سياسات الأمن السيبراني
معرف الدور الوظيفي	GRCL-GRC-003
الفئة	الحوكمة والمخاطر والالتزام والقوانين
مجال التخصص	الحوكمة والمخاطر والالتزام
وصف الدور الوظيفي	تطوير سياسات الأمن السيبراني وتحديثها، لدعم متطلبات الأمن السيبراني بالمنظمة ومواءمتها.
المهام	T0011, T0017, T0045, T0046, T0078, T0082, T0085, T0086, T0088, T0092, T0093, T0095, T0099, T0103, T0104, T0108, T0109, T0110
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0052, K0074, K0079, K0091, K0118, K0122, K0141, K0142, K0150, K0168, K2019, K2503, K5503
المهارات	S2513, S2530
القدرات	A0006, A2500, A2510

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مُقيّم ضوابط الأمن السيبراني
معرف الدور الوظيفي	GRCL-GRC-004
الفئة	الحوكمة والمخاطر والالتزام والقوانين
مجال التخصص	الحوكمة والمخاطر والالتزام
وصف الدور الوظيفي	تحليل ضوابط الأمن السيبراني وتقييم فاعليتها.
المهام	T0036, T0037, T0039, T0043, T0050, T0053, T0059, T0061, T0074, T0079, T2503, T2505, T2507, T2508, T2509, T2510, T2511, T2512, T2514, T2516
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0013, K0016, K0017, K0019, K0020, K0021, K0022, K0028, K0029, K0031, K0035, K0037, K0038, K0042, K0044, K0052, K0055, K0060, K0061, K0073, K0074, K0079, K0091, K0092, K0093, K0100, K0110, K0113, K0118, K0124, K0125, K0126, K0128, K0133, K0146, K0153, K0168, K0169, K1004, K1017, K1511, K2500, K2501, K2502, K5503
المهارات	S0001, S0004, S0010, S0019, S0023, S0034, S0036, S0037, S0038, S0040, S0044, S0045, S0046, S0047, S0048, S0050, S0051, S0055, S0061, S0063, S0064, S1008, S2500, S2501, S2502, S2503, S2504, S2505, S2506, S2507, S2508, S2509, S2510, S2511, S2512, S2513, S2514, S2515, S2516, S2517, S2521, S2523, S2524, S2525, S2527, S2528, S2529, S2530, S2531, S2532, S2533, S2534, S2535, S2536, S2539, S2540, S2541, S2542, S2543
القدرات	A0001, A0002, A0003, A0004, A0005, A0008, A0012, A0015, A0016, A0017, A0018, A0019, A0021, A0025, A0027, A0028, A0029, A0030, A0031, A0032, A0035, A0044, A2502, A2503, A2504, A2505, A2506, A2507, A2508, A2509, A2511, A2512, A2513, A2514, A2515, A2516, A2517, A2518, A2519, A2520, A2521, A2523, A2524, A2525, A2526, A2527

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مدقق الأمن السيبراني
معرف الدور الوظيفي	GRCL-GRC-005
الفئة	الحوكمة والمخاطر والالتزام والقوانين
مجال التخصص	الحوكمة والمخاطر والالتزام
وصف الدور الوظيفي	تصميم عمليات التدقيق للأمن السيبراني وتنفيذها وإدارتها بهدف تقييم مدى التزام المنظمة بالمتطلبات والسياسات والمعايير والضوابط المعمول بها، وإعداد تقارير التدقيق وتقديمها للأطراف ذات الصلاحية.
المهام	T0024, T0038, T0039, T0041, T0048, T0059, T0060, T0109, T2502, T2508, T2509, T2510, T2512, T2515, T2520
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0013, K0021, K0022, K0028, K0035, K0038, K0056, K0074, K0079, K0109, K0133, K0144, K1004, K2500, K2501, K2504, K2505, K2506, K2507, K5503
المهارات	S0004, S0010, S0023, S0028, S0036, S0040, S0046, S0047, S0048, S0051, S0055, S1008, S2500, S2501, S2502, S2503, S2504, S2505, S2506, S2507, S2508, S2509, S2510, S2511, S2512, S2513, S2514, S2515, S2516, S2519, S2521, S2523, S2524, S2525, S2526, S2527, S2528, S2529, S2532, S2533, S2534, S2536, S2539, S2540, S2541, S2545, S2546
القدرات	A0001, A0002, A0004, A0005, A0015, A0016, A0017, A0019, A0021, A0022, A0025, A0027, A0028, A0029, A0030, A0031, A0032, A0035, A0044, A2502, A2503, A2504, A2505, A2506, A2507, A2508, A2509, A2510, A2511, A2512, A2513, A2514, A2515, A2516, A2517, A2519, A2520, A2521, A2523, A2524, A2525, A2526, A2527, A2528, A2529, A2530

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي قانون الأمن السيبراني
معرف الدور الوظيفي	GRCL-LDP-001
الفئة	الحوكمة والمخاطر والالتزام والقوانين
مجال التخصص	القوانين وحماية البيانات
وصف الدور الوظيفي	تقديم الخدمات القانونية بشأن الموضوعات ذات الصلة بالقوانين والأنظمة السيبرانية.
المهام	T0019, T0038, T1501, T3000, T3001, T3002, T3003, T3004, T3005, T3006, T3007, T3008, T3009, T3010, T3052
المعارف	K0002, K0003, K0004, K0005, K0006, K0044, K0065, K0074, K0084, K0125, K0126, K0128, K3000, K3001, K3002, K3004, K5503
المهارات	S0058
القدرات	A3000

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي الخصوصية وحماية البيانات
معرف الدور الوظيفي	GRCL-LDP-002
الفئة	الحوكمة والمخاطر والالتزام والقوانين
مجال التخصص	القوانين وحماية البيانات
وصف الدور الوظيفي	دراسة هيكلة البيانات الشخصية وقوانين وأنظمة الخصوصية المعمول بها، مع تحليل مخاطر الخصوصية، وتطوير برنامج المنظمة للمواءمة مع ضوابط الخصوصية وحماية البيانات والسياسات الداخلية، والإشراف على تنفيذها. مع دعم استجابة المنظمة لحوادث الخصوصية أو حماية البيانات.
المهام	T0007, T0126, T0127, T3011, T3012, T3013, T3014, T3015, T3016, T3017, T3018, T3019, T3020, T3021, T3022, T3023, T3024, T3025, T3026, T3027, T3028, T3029, T3030, T3031, T3032, T3033, T3034, T3035, T3036, T3037, T3038, T3039, T3040, T3041, T3042, T3043, T3044, T3045, T3046, T3047, T3048, T3049, T3050, T3051, T3052, T3053
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0008, K0029, K0030, K0035, K0050, K0074, K3004, K3005, K3006, K5503
المهارات	S0058, S0061, S0064, S3000, S3002
القدرات	A0006, A0007, A0023, A0024, A0026, A0027, A0035, A2005, A2526, A2527, A3001, A3002

٣-١-٤ مجموعة الفئة: الحماية والدفاع (PD)

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	محلل دفاع الأمن السيبراني
معرف الدور الوظيفي	PD-D-001
الفئة	الحماية والدفاع
مجال التخصص	الدفاع
وصف الدور الوظيفي	استخدام البيانات التي تم استخلاصها من مجموعة أدوات الدفاع السيبراني لتحليل الأحداث الواقعة داخل المنظمة بهدف الكشف عن التهديدات والتعامل معها.
المهام	T0009, T0015, T0025, T0028, T0029, T0037, T0040, T0044, T0054, T0055, T0056, T0064, T0065, T0066, T0067, T0068, T0069, T0070, T0071, T0072, T0073, T0075, T0076, T0097, T0098, T0100, T0101, T0102, T0107, T0111, T3500, T3501, T3503, T3504
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0014, K0016, K0017, K0020, K0024, K0031, K0033, K0035, K0036, K0038, K0042, K0043, K0044, K0045, K0046, K0049, K0052, K0053, K0054, K0058, K0060, K0063, K0064, K0065, K0067, K0068, K0069, K0070, K0072, K0074, K0076, K0077, K0078, K0084, K0086, K0087, K0088, K0090, K0091, K0099, K0100, K0101, K0102, K0103, K0104, K0113, K0117, K0118, K0124, K0125, K0126, K0134, K0136, K0137, K0138, K0139, K0145, K0146, K0147, K0148, K0152, K0153, K0168 , K5503
المهارات	S0006, S0009, S0010, S0012, S0015, S0023, S0033, S0040, S0041, S0042, S0046, S0048, S0057, S0061, S0063, S2002, S2514, S2534, S2543, S3500, S3501, S3502, S5524
القدرات	A0003, A0014, A0035, A0036, A3500, A3501

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي البنية التحتية للأمن السيبراني
معرف الدور الوظيفي	PD-D-002
الفئة	الحماية والدفاع
مجال التخصص	الدفاع
وصف الدور الوظيفي	فحص وتنصيب وصيانة الأجهزة والبرمجيات المستخدمة للدفاع وحماية الأنظمة والشبكات من التهديدات السيبرانية وتشغيلها والإشراف عليها.
المهام	T0005, T0038, T0057, T0114, T3502, T3505, T3506, T3507, T3508, T3509, T3510, T3511, T3512, T4023
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0019, K0024, K0033, K0035, K0043, K0046, K0055, K0063, K0064, K0074, K0084, K0100, K0104, K0119, K0147, K0148, K1022, K3500, K3501, K3502, K3503, K3504, K5012
المهارات	S0005, S0008, S0014, S0016, S0021, S0022, S0024, S0035, S0038, S0061, S0065, S1007, S2507, S3500
القدرات	A0001, A0035, A0044

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي الأمن السيبراني
معرف الدور الوظيفي	PD-D-003
الفئة	الحماية والدفاع
مجال التخصص	الدفاع
وصف الدور الوظيفي	تقديم الدعم العام للأمن السيبراني، والمساعدة في مهام الأمن السيبراني.
المهام	T0005, T0009, T0026, T0028, T0102, T0113, T0136, T3500, T3501, T3503, T3504
المعارف	K0001, K0004, K0005, K0006, K0007, K0009, K0013, K0014, K0017, K0019, K0020, K0024, K0031, K0033, K0035, K0038, K0043, K0045, K0051, K0053, K0055, K0063, K0068, K0074, K0084, K0104, K0115, K0119, K0152, K3504, K3505
المهارات	S0002, S0009, S0010, S0012, S0019, S0021, S0022, S0023, S0027, S0028, S0035, S0042, S0062, S3501, S3502
القدرات	A0001, A0003, A0036, A3501

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي التشفير
معرف الدور الوظيفي	PD-P-001
الفئة	الحماية والدفاع
مجال التخصص	الحماية
وصف الدور الوظيفي	تطوير أنظمة التشفير وخوارزمياته، وتقييمها وتحليلها وتحديد نقاط ضعفها وسبل تحسينها.
المهام	T0010, T0016, T0090, T0091, T0096, T0114, T4000, T4008, T4012, T4021, T4022
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0010, K0014, K0015, K0016, K0017, K0018, K0024, K0028, K0029, K0030, K0035, K0038, K0039, K0040, K0042, K0044, K0046, K0050, K0051, K0053, K0074, K0102, K0112, K0113, K0116, K0131, K0140, K0155, K0157, K0158, K0163, K1000, K1011, K4000, K4009, K4010, K4011, K4013, K4014, K4015, K4017
المهارات	S0004, S0016, S0038, S0039, S0061, S1002, S1028, S4001, S4002 , S4003
القدرات	A0035, A1001, A4000, A4001, A5000

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي إدارة الهوية والوصول
معرف الدور الوظيفي	PD-P-002
الفئة	الحماية والدفاع
مجال التخصص	الحماية
وصف الدور الوظيفي	إدارة هوية الأفراد والكيانات، وصلاحيات وصولهم إلى الموارد من خلال تطبيق أنظمة وعمليات التعريف والتوثيق والتصريح.
المهام	T0100, T0114, T1049, T3508, T4016, T4017, T4018, T4019, T4020, T4024, T4025, T4026, T4027, T4028, T4029
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0024, K0028, K0035, K0042, K0049, K0059, K0074, K0079, K0085, K0106, K0107, K0108, K0112, K0124, K0125, K0126, K0132, K0133, K0144, K0151, K0156, K1019, K3505, K4000, K4001, K4002, K4004, K4012, K4016, K4018, K5503
المهارات	S0005, S0061, S1007, S4000
القدرات	A0035, A4002, A4003

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	محلل أمن النظم
معرف الدور الوظيفي	PD-P-003
الفئة	الحماية والدفاع
مجال التخصص	الحماية
وصف الدور الوظيفي	تطوير أمن النظم واختباره وصيانته، وتحليل أمن العمليات والأنظمة المدمجة.
المهام	T0004, T0005, T0015, T0036, T0040, T0043, T0050, T0074, T0079, T0097, T0098, T0100, T0102, T0107, T0111, T1026, T4000, T4001, T4002, T4003, T4004, T4005, T4006, T4007, T4009, T4010, T4011, T4012, T4013, T4014, T4015, T4023
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0017, K0020, K0026, K0027, K0031, K0035, K0038, K0040, K0042, K0045, K0046, K0048, K0054, K0058, K0062, K0074, K0100, K0101, K0111, K0113, K0120, K0124, K0125, K0126, K0127, K0128, K0129, K0130, K0133, K0134, K0136, K0146, K0149, K0152, K1015, K4006, K4007, K4008, K4009 , K5503
المهارات	S0008, S0010, S0012, S0017, S0040, S0042, S0061, S1007, S2511
القدرات	A0003, A0035

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي تقييم الثغرات
معرف الدور الوظيفي	PD-VA-001
الفئة	الحماية والدفاع
مجال التخصص	تقييم الثغرات
وصف الدور الوظيفي	تقييم ثغرات النُظم والشبكات، وتحديد مواطن انحرافها عن الإعدادات المقبولة أو السياسات المعمول بها، وقياس فاعلية البنية الدفاعية متعددة الطبقات ضد الثغرات المعروفة.
المهام	T0003, T0009, T0024, T0041, T0113, T0133, T2502, T4500, T4501, T4502, T4507, T4518
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0017, K0019, K0024, K0035, K0042, K0046, K0051, K0052, K0055, K0064, K0074, K0076, K0087, K0088, K0090, K0099, K0100, K0113, K0115, K0119, K0133, K0138, K0140, K0148, K0153, K0154, K0163, K0168, K4500, K4501, K5503
المهارات	S0001, S0009, S0026, S0037, S0044, S0061, S1023, S2506, S2515, S2527, S2545, S4500, S4502, S4504, S4505, S4507, S4508
القدرات	A0001, A0033, A0035

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي اختبار الاختراقات
معرف الدور الوظيفي	PD-VA-002
الفئة	الحماية والدفاع
مجال التخصص	تقييم الثغرات
وصف الدور الوظيفي	أداء محاولات اختراق مصرح لها لأنظمة الحاسبات أو الشبكات والمنشآت المادية باستخدام أساليب تهديد واقعية لتقييم حالتها الأمنية وكشف الثغرات المحتملة.
المهام	T4500, T4503, T4504, T4505, T4506, T4507, T4508, T4509, T4510, T4511, T4512, T4513, T4514, T4515, T4516, T4517, T5545
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0038, K0054, K0057, K0074, K0075, K0080, K0134, K0140, K0153, K0158, K0161, K0163, K1013, K4502, K4503, K4504, K4505, K4506, K4507, K4508, K4509, K4510, K5503
المهارات	S0011, S0027, S2514, S2515, S4501, S4503, S4504, S4505, S4506, S4508, S4509, S4510, S4511, S5002, S5015, S5016, S5502, S5509, S5510
القدرات	A0001, A0003, A0008, A4501, A4502, A4503, A4504, A4505

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي استجابة للحوادث السيبرانية
معرف الدور الوظيفي	PD-IR-001
الفئة	الحماية والدفاع
مجال التخصص	الاستجابة للحوادث
وصف الدور الوظيفي	مباشرة الحوادث المتعلقة بالأمن السيبراني وتحليلها والاستجابة لها.
المهام	T0009, T0026, T0027, T0028, T0031, T0034, T0044, T0047, T0051, T0058, T0062, T0087, T0101, T0106, T5003, T5025, T5031, T5040, T5054
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0019, K0021, K0024, K0025, K0032, K0033, K0036, K0043, K0047, K0052, K0064, K0074, K0084, K0087, K0088, K0090, K0099, K0100, K0117, K0121, K0123, K0133, K0148, K0168, K0169, K5503
المهارات	S0002, S0004, S0006, S0009, S0010, S0011, S0012, S0013, S0014, S0015, S0018, S0019, S0020, S0022, S0023, S0024, S0025, S0026, S0027, S0033, S0035, S0041, S0044, S0046, S0048, S0051, S0052, S0054, S0060, S1022, S1023, S1033, S1503, S2000, S2002, S2506, S2523, S2526, S2532, S2533, S2535, S2538, S3500, S3501, S5000, S5001, S5002, S5003, S5004, S5005, S5006, S5007, S5008, S5009, S5010, S5011, S5012, S5013, S5014, S5017, S5501, S5502, S5503, S5504, S5505, S5506, S5507, S5508, S5509, S5510, S5511, S5512, S5513, S5514
القدرات	A0034, A0036

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي التحليل الجنائي الرقمي
معرف الدور الوظيفي	PD-IR-002
الفئة	الحماية والدفاع
مجال التخصص	الاستجابة للحوادث
وصف الدور الوظيفي	جمع الأدلة الرقمية وتحليلها، والتحقيق في حوادث الأمن السيبراني لاستخلاص معلومات مفيدة لمعالجة ثغرات النُظم والشبكات.
المهام	T0010, T0030, T0032, T0033, T0034, T0049, T5000, T5002, T5004, T5006, T5007, T5010, T5013, T5014, T5015, T5016, T5017, T5019, T5020, T5022, T5023, T5024, T5025, T5026, T5027, T5028, T5029, T5030, T5031, T5036, T5037, T5038, T5039, T5040, T5041, T5044, T5050, T5051, T5059, T5062, T5534
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0016, K0019, K0033, K0045, K0052, K0066, K0074, K0075, K0090, K0091, K0100, K0119, K0138, K0168, K1503, K5000, K5002, K5003, K5005, K5006, K5007, K5008, K5009, K5010, K5011, K5014, K5016, K5017, K5018, K5019, K5020, K5021, K5022, K5023, K5024, K5028, K5029, K5030, K5031, K5503
المهارات	S0011, S0013, S0019, S0020, S0029, S0030, S0041, S5000, S5001, S5002, S5003, S5004, S5005, S5006, S5007, S5008, S5009, S5010, S5011, S5012, S5013, S5014
القدرات	A5000, A5001

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي تحقيقات الجرائم السيبرانية
معرف الدور الوظيفي	PD-IR-003
الفئة	الحماية والدفاع
مجال التخصص	الاستجابة للحوادث
وصف الدور الوظيفي	تعريف الأدلة وجمعها وفحصها والحفاظ عليها، باستخدام أساليب تحرٍ واستقصاء موثقة ومقننة.
المهام	T0018, T0021, T5001, T5005, T5008, T5009, T5010, T5011, T5012, T5018, T5021, T5023, T5033, T5034, T5035, T5040, T5042, T5043, T5046, T5047, T5048, T5049, T5054, T5059, T5061
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0052, K0065, K0067, K0074, K0091, K0168, K5001, K5003, K5006, K5007, K5008, K5013, K5016, K5025, K5026, K5032, K5503
المهارات	S0013, S0018, S1501, S5003
القدرات	A5002, A5003

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي الهندسة العكسية للبرمجيات الضارة
معرف الدور الوظيفي	PD-IR-004
الفئة	الحماية والدفاع
مجال التخصص	الاستجابة للحوادث
وصف الدور الوظيفي	تحليل البرمجيات الضارة (عن طريق تفكيكها وإعادتها إلى صيغة برمجية مفهومة)، وفهم طريقة عملها وتأثيرها وغرضها، وتقديم توصيات للوقاية منها والاستجابة للحوادث الناتجة عنها.
المهام	T0089, T0135, T5016, T5052, T5055, T5057, T5058, T5510, T5519, T5525, T5534, T5535, T5536, T5537, T5538, T5539, T5540, T5541, T5542, T5544, T5545
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0014, K0016, K0039, K0043, K0047, K0067, K0074, K0094, K0095, K0096, K0097, K0098, K0099, K0100, K0101, K0102, K0103, K0104, K0105, K5017, K5018, K5019, K5020, K5021, K5022, K5023, K5024
المهارات	S0001, S0029, S0030, S0031, S0032, S0048, S0049, S0052, S0053, S1503, S5007, S5008, S5009, S5010, S5011, S5012, S5013, S5014, S5015, S5016, S5017
القدرات	A0001, A0025, A0046, A3500, A5000, A5004, A5502

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	محلل معلومات التهديدات السيبرانية
معرف الدور الوظيفي	PD-TM-001
الفئة	الحماية والدفاع
مجال التخصص	إدارة التهديدات
وصف الدور الوظيفي	جمع معلومات عن التهديدات السيبرانية من مصادر مختلفة وتحليلها لتكوين فهم وإدراك عميقين للتهديدات السيبرانية، وخطط المخترقين، والأساليب والإجراءات المتبعة، لاستنباط وتوثيق مؤشرات من شأنها مساعدة المنظمات في الكشف عن الحوادث السيبرانية والتنبؤ بها، وحماية النُظم والشبكات من التهديدات السيبرانية.
المهام	T5056, T5502, T5503, T5504, T5505, T5506, T5507, T5508, T5510, T5515, T5517, T5519, T5524, T5525, T5526, T5527, T5528, T5529, T5530, T5531, T5535, T5536, T5537, T5538, T5539, T5540, T5541, T5542, T5543, T5544
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0027, K0043, K0066, K0074, K0099, K0155, K0157, K0159, K0161, K0163, K0165, K5500, K5501, K5502, K5503, K5504, K5506, K5507, K5508, K5509, K5511, K5512, K5513, K5514, K5515, K5516, K5517, K5518, K5519, K5520, K5523, K5524, K5527, K5528, K5530, K5532, K5533
المهارات	S0049, S0051, S0055, S2536, S5500, S5501, S5502, S5504, S5507, S5509, S5510, S5516, S5517, S5518, S5520, S5521
القدرات	A0002, A0014, A0016, A0018, A0019, A0020, A0022, A0025, A2513, A2514, A2516, A2523, A2525, A5500, A5501, A5502

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي اكتشاف التهديدات السيبرانية
معرف الدور الوظيفي	PD-TM-002
الفئة	الحماية والدفاع
مجال التخصص	إدارة التهديدات
وصف الدور الوظيفي	البحث الاستباقي عن التهديدات غير المكتشفة في الشبكات والنُظم، وتحديد مؤشرات الاختراق، وتقديم التوصيات للتعامل معها.
المهام	T0009, T0017, T0018, T0021, T0026, T0027, T0028, T0030, T0032, T0033, T0034, T0035, T0049, T0054, T0055, T0056, T0057, T0060, T0069, T0080, T0089, T0109, T0135, T0136, T1528, T5010, T5016, T5023, T5500, T5501, T5507, T5509, T5510, T5511, T5512, T5513, T5514, T5515, T5517, T5518, T5519, T5520, T5521, T5523, T5524, T5525, T5532, T5533, T5534, T5536, T5544
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0013, K0014, K0016, K0028, K0031, K0032, K0033, K0034, K0035, K0043, K0044, K0047, K0050, K0064, K0065, K0067, K0068, K0074, K0086, K0088, K0107, K0116, K0154, K5503, K5519, K5521, K5522, K5525, K5526, K5530, K5534
المهارات	S0001, S0029, S0030, S0031, S0032, S0050, S0051, S0052, S0059, S0062, S2525, S2526, S2527, S2532, S4508, S5007, S5008, S5009, S5010, S5011, S5503, S5505, S5506, S5511, S5512, S5513, S5514, S5515, S5519, S5522, S5523, S5524
القدرات	A0001, A0025, A0033, A0046, A3500, A5000, A5502

٣-١-٥ مجموعة الفئة: أنظمة التحكم الصناعي والتقنيات التشغيلية (ICS/OT)

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مصمم معمارية الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية
معرف الدور الوظيفي	ICSOT- ICSOT-001
الفئة	أنظمة التحكم الصناعي والتقنيات التشغيلية
مجال التخصص	أنظمة التحكم الصناعي والتقنيات التشغيلية
وصف الدور الوظيفي	تصميم نُظم وشبكات الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية والإشراف على إعداداتها وتطويرها وتنفيذها.
المهام	T0036, T0043, T0507, T0508, T0509, T0510, T0511, T0512, T0514, T0515, T0516, T0517, T0518, T0519, T0520, T2511, T4502, T6000, T6001, T6002, T6003, T6004, T6009, T6010, T6011, T6012, T6013
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0014, K0016, K0017, K0020, K0021, K0022, K0023, K0025, K0026, K0027, K0028, K0034, K0035, K0040, K0041, K0042, K0044, K0045, K0046, K0048, K0053, K0057, K0058, K0061, K0062, K0074, K0093, K0101, K0109, K0111, K0112, K0116, K0120, K0124, K0125, K0126, K0129, K0131, K0133, K0146, K0148, K0149, K0151, K1015, K1036, K1505, K4000, K5503, K6000, K6001, K6002, K6003, K6004, K6005, K6006, K6007, K6008, K6009, K6010, K6011, K6012, K6013, K6014, K6015, K6016, K6017, K6018, K6019, K6020
المهارات	S0003, S0007, S0008, S0010, S0016, S0021, S0027, S0038, S0039, S0061, S0064, S0065, S1008, S6000, S6001, S6002, S6003, S6004, S6005, S6006, S6007
القدرات	A0003, A0009, A0010, A0011, A0013, A0035, A0043, A0044, A0500, A2504, A6000, A6001, A6002, A6004

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي البنية التحتية للأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية
معرف الدور الوظيفي	ICSOT- ICSOT-002
الفئة	أنظمة التحكم الصناعي والتقنيات التشغيلية
مجال التخصص	أنظمة التحكم الصناعي والتقنيات التشغيلية
وصف الدور الوظيفي	فحص وتنصيب وصيانة الأجهزة والبرمجيات المستخدمة للدفاع وحماية الأنظمة والشبكات من التهديدات السيبرانية في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية وتشغيلها والإشراف عليها.
المهام	T0005, T0038, T0057, T0114, T3502, T3505, T3506, T3507, T3508, T3509, T3510, T3511, T3512, T4023, T6007, T6008, T6012
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0017, K0019, K0024, K0033, K0035, K0043, K0046, K0055, K0063, K0064, K0074, K0084, K0100, K0104, K0119, K0147, K0148, K1022, K3500, K3501, K3502, K3503, K3504, K5012, K6001, K6012, K6014, K6015, K6016, K6017, K6018, K6019, K6020
المهارات	S0005, S0008, S0009, S0014, S0016, S0021, S0022, S0024, S0035, S0038, S0061, S0065, S1007, S2507, S3500, S6004, S6005, S6007
القدرات	A0001, A0035, A0044

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	محلل دفاع الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية
معرف الدور الوظيفي	ICSOT- ICSOT-003
الفئة	أنظمة التحكم الصناعي والتقنيات التشغيلية
مجال التخصص	أنظمة التحكم الصناعي والتقنيات التشغيلية
وصف الدور الوظيفي	استخدام البيانات، التي تم جمعها من مجموعة متنوعة من أدوات الأمن السيبراني لتحليل الأحداث الواقعة في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية بهدف الكشف عن تهديدات الأمن السيبراني والتعامل معها.
المهام	T0009, T0015, T0025, T0028, T0029, T0037, T0040, T0044, T0054, T0055, T0056, T0058, T0064, T0065, T0066, T0067, T0068, T0069, T0070, T0071, T0072, T0073, T0075, T0076, T0097, T0098, T0100, T0101, T0102, T0107, T0111, T3500, T3501, T3503, T3504
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0014, K0016, K0017, K0020, K0024, K0031, K0033, K0035, K0036, K0038, K0042, K0043, K0044, K0045, K0046, K0049, K0052, K0053, K0054, K0058, K0060, K0063, K0064, K0065, K0067, K0068, K0069, K0070, K0072, K0074, K0076, K0077, K0078, K0084, K0086, K0087, K0088, K0090, K0091, K0099, K0100, K0101, K0102, K0103, K0104, K0113, K0117, K0118, K0124, K0125, K0126, K0134, K0136, K0137, K0138, K0139, K0145, K0146, K0147, K0148, K0152, K0153, K0168, K5503, K6001, K6012, K6014, K6015, K6016, K6017, K6018, K6019, K6020
المهارات	S0006, S0009, S0010, S0012, S0015, S0023, S0033, S0040, S0041, S0042, S0046, S0048, S0057, S0061, S0063, S2002, S2534, S3500, S3501, S3502, S6004, S6005, S6006, S6007
القدرات	A0003, A0014, A0035, A0036, A3500, A3501, A6004, A6005

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي مخاطر الأمن السيبراني لأنظمة التحكم الصناعي والتقنيات التشغيلية
معرف الدور الوظيفي	ICSOT- ICSOT-004
الفئة	أنظمة التحكم الصناعي والتقنيات التشغيلية
مجال التخصص	أنظمة التحكم الصناعي والتقنيات التشغيلية
وصف الدور الوظيفي	تحديد مخاطر الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية وتقييمها وإدارتها، مع تقييم وتحليل فاعلية ضوابط الأمن السيبراني القائمة، وتقديم الملاحظات والتوصيات بناء على تلك التقييمات.
المهام	T0001, T0006, T0012, T0013, T0014, T0020, T0034, T0039, T0043, T0053, T0105, T0109, T0128, T0129, T0130, T0131, T0132, T0133, T0136, T2500, T6014, T6016
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0008, K0009, K0029, K0037, K0073, K0074, K0080, K0081, K0082, K0083, K0089, K0092, K0107, K0127, K0160, K0162, K0166, K0167, K5503, K6001, K6003, K6005, K6012, K6014, K6015, K6016, K6017, K6018, K6019, K6020
المهارات	S0044, S0057, S0062, S6006, S6007
القدرات	A0033, A0037, A0038, A0039, A0040, A0041, A0042, A0045, A2501, A6004, A6005

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي استجابة للحوادث السيبرانية لأنظمة التحكم الصناعي والتقنيات التشغيلية
معرف الدور الوظيفي	ICSOT- ICSOT-005
الفئة	أنظمة التحكم الصناعي والتقنيات التشغيلية
مجال التخصص	أنظمة التحكم الصناعي والتقنيات التشغيلية
وصف الدور الوظيفي	مباشرة حوادث الأمن السيبراني وتحليلها والاستجابة لها في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية.
المهام	T0009, T0026, T0027, T0028, T0031, T0044, T0047, T0051, T0058, T0062, T0087, T0101, T0106, T5025, T5031, T6014, T6015
المعارف	K0001, K0002, K0003, K0004, K0005, K0006, K0019, K0021, K0024, K0025, K0032, K0033, K0036, K0043, K0047, K0052, K0064, K0074, K0084, K0087, K0088, K0090, K0099, K0100, K0117, K0121, K0123, K0133, K0148, K0168, K5503, K6001, K6012, K6014, K6015, K6016, K6017, K6018, K6019, K6020
المهارات	S0002, S0004, S0006, S0009, S0010, S0011, S0012, S0013, S0014, S0015, S0018, S0019, S0020, S0022, S0023, S0024, S0025, S0026, S0027, S0033, S0035, S0041, S0044, S0046, S0048, S0051, S0052, S0054, S0060, S1022, S1023, S1033, S1034, S1503, S2000, S2002, S2506, S2523, S2526, S2532, S2533, S2535, S2538, S3500, S3501, S5000, S5001, S5002, S5003, S5004, S5005, S5006, S5007, S5008, S5009, S5010, S5011, S5012, S5013, S5014, S5017, S5501, S5502, S5503, S5504, S5505, S5506, S5507, S5508, S5509, S5510, S5511, S5512, S5513, S5514, S6001, S6004, S6006, S6007
القدرات	A6004, A6005, A6006

٢-٣ الملحق ب: قائمة المهام والمعارف والمهارات والقدرات

كما ذُكر سابقا، فقد تم تطوير الإطار السعودي لكوادر الأمن السيبراني باستخدام المنهجية المتبعة في إطار كوادر الأمن السيبراني التابع للمبادرة الوطنية لتعليم الأمن السيبراني (NICE) الصادر من المعهد الوطني الأمريكي للمعايير والتقنية (NIST)، إلا أن الفئات ومجالات التخصص والأدوار الوظيفية الواردة في الإطار السعودي لكوادر الأمن السيبراني مختلفة عن تلك الواردة في إطار الكوادر التابع للمبادرة الوطنية لتعليم الأمن السيبراني (NICE) حيث تم تصميمها لتلائم احتياج كوادر الأمن السيبراني في المملكة العربية السعودية.

وقد تم تعريف المهام والمعارف والمهارات والقدرات المطلوبة لأداء كل دور وظيفي في هذا الإطار باستخدام القائمة الطويلة من المهام والمعارف والمهارات والقدرات الموجودة في إطار المبادرة الوطنية لتعليم الأمن السيبراني (NICE) مع عمل ما يلزم من التعديلات لعكس احتياجات كوادر الأمن السيبراني في المملكة. كما تم ترقيم المهام والمعارف والمهارات والقدرات حسب ما هو موضح في (الجدول ٨). ويقدم (الجدول ٩) و(الجدول ١٠) و(الجدول ١١) و(الجدول ١٢) أوصاف المهام والمعارف والمهارات والقدرات المستخدمة في هذا الإطار.

(جدول ٨): نظام ترقيم المهام والمعارف والمهارات والقدرات في الإطار السعودي لكوادر الأمن السيبراني

الفئة	مجال التخصص	مدى الترقيم للمهام والمعارف والمهارات والقدرات
الأدوار العامة	عام	0000-0499
معمارية الأمن السيبراني والبحث والتطوير	معمارية الأمن السيبراني	0500-0999
	البحث والتطوير في الأمن السيبراني	1000-1499
القيادة وتطوير الكوادر	القيادة	1500-1999
	تطوير الكوادر	2000-2499
الحوكمة والمخاطر والالتزام والقوانين	الحوكمة والمخاطر والالتزام	2500-2999
	القوانين وحماية البيانات	3000-3499
الحماية والدفاع	الدفاع	3500-3999
	الحماية	4000-4499
	تقييم الثغرات	4500-4999
	الاستجابة للحوادث	5000-5499
	إدارة التهديدات	5500-5999
أنظمة التحكم الصناعي والتقنيات التشغيلية	أنظمة التحكم الصناعي والتقنيات التشغيلية	6000-6499

(جدول ٩): أوصاف المهام

رمز المهمة	وصف المهمة
T0001	التواصل الفعال مع الإدارة العليا بشأن مخاطر الأمن السيبراني.
T0002	التواصل الفعال مع الإدارة العليا بشأن الجوانب المالية للأمن السيبراني.
T0003	تحليل سياسات الدفاع السيبراني للمنظمة وإعداداتها، وذلك لتقييم مدى التزامها بالتنظيمات والتوجيهات المؤسسية.
T0004	تطبيق السياسات الأمنية على التطبيقات المتداخلة بين بعضها البعض.
T0005	تطبيق السياسات الأمنية لتحقيق الأهداف الأمنية للنظام.
T0006	تطوير أوصاف للمخاطر الأمنية لنظم الحاسب من خلال تقييم التهديدات لتلك النظم وثغراتها.
T0007	إجراء تقييمات لمدى التأثير على الخصوصية لضمان حماية سرِّية معلومات المعرفات الشخصية بشكل مناسب.
T0008	التعاون مع أصحاب المصلحة لضمان تلبية برامج استمرارية الأعمال والتعافي من الكوارث لمتطلبات المنظمة.
T0009	ربط بيانات الحوادث لتحديد الثغرات.
T0010	فك تشفير البيانات المضبوطة باستخدام وسائل تقنية.
T0011	تطوير سياسات الأمن السيبراني والوثائق ذات العلاقة.
T0012	تطوير استراتيجيات للحد من المخاطر من أجل إدارة المخاطر في ظل سياسات المنظمة لمستويات المخاطرة المقبولة.
T0013	تطوير إجراءات مضادة خاصة بالأمن السيبراني واستراتيجيات لمعالجة المخاطر.
T0014	توصيف مخاطر الأمن السيبراني الأولية أو المتبقية التي تؤثر على تشغيل النظام.
T0015	استخدام منتجات الأمن السيبراني أو تقنيات التحكم الأمني للحد من المخاطر المكتشفة إلى مستويات مقبولة.
T0016	التأكد من توافق قدرات الاكتشاف والحماية السيبرانية مع استراتيجية وسياسات الأمن السيبراني للمنظمة، ومع المستندات الأخرى ذات العلاقة.
T0017	تأسيس قنوات اتصال ملائمة مع أصحاب المصلحة، والحفاظ عليها.
T0018	إنشاء علاقات بين فريق الاستجابة للحوادث والمجموعات الداخلية والخارجية الأخرى.
T0019	تقييم جوانب الأمن السيبراني للعقود لضمان الالتزام بالمتطلبات المالية، والتعاقدية، والقانونية، والتنظيمية.
T0020	التأكد من أن القرارات المتخذة بشأن الأمن السيبراني تستند على المبادئ الأساسية لإدارة المخاطر.

رمز المهمة	وصف المهمة
T0021	تحديد البيانات التي ستضيف قيمة لعمليات التحقيق.
T0022	التأكد من أن أي منتج يتم استخدامه لإدارة مخاطر الأمن السيبراني تم تقييمه بفعالية والتصريح باستخدامه.
T0023	التعرف على أنماط عدم الالتزام بسياسات الأمن السيبراني والوثائق ذات العلاقة بهدف تعريف طرق لتحسينها.
T0024	الحفاظ على مجموعة أدوات تدقيق الدفاع السيبراني القابلة للتفعيل، بناء على أفضل الممارسات في القطاع، وذلك لدعم عمليات تدقيق الدفاع السيبراني.
T0025	توثيق وتصعيد الحوادث السيبرانية التي من شأنها أن تؤدي إلى أثر فوري أو مستمر.
T0026	تحليل السجلات من مصادر متعددة لتحديد التهديدات المحتملة لأمن الشبكة.
T0027	تحليل أولويات الحوادث لتحديد الثغرة ونطاقها وأولويتها وتأثيرها المحتمل، ومن ثم تقديم توصيات من شأنها توفير العلاج السريع.
T0028	تحليل توجهات الدفاع السيبراني، وتقديم تقارير بشأنها.
T0029	ربط المعلومات من مصادر متعددة للإلمام بالحالة وتحديد فاعلية الهجمة المرصودة.
T0030	تحليل الملفات لتحديد سماتها المميزة.
T0031	إجراء جمع أولي للصور الجنائية بموجب معايير البحث الجنائي ذات العلاقة، وفحصها لتحديد أنسب إجراءات المعالجة.
T0032	إجراء تحليل جنائي رقمي حي.
T0033	تحليل الخط الزمني للأحداث.
T0034	أداء مهام الاستجابة للأحداث دعما لفرق الاستجابة للأحداث، شاملا جمع الأدلة الجنائية، وربط حالات التسلل، والتتبع، وتحليل التهديدات ومعالجة الأنظمة.
T0035	أداء البرمجة الآمنة وتحديد مواطن الخلل المحتملة في الشفرات البرمجية لمعالجة الثغرات.
T0036	إجراء مراجعات الأمن السيبراني، وتحديد الفجوات في المعمارية الأمنية، من أجل إصدار خطط لإدارة المخاطر السيبرانية.
T0037	إجراء مراجعات الأمن السيبراني، وتحديد الثغرات الأمنية في المعمارية الأمنية لدعم استراتيجيات معالجة المخاطر.
T0038	إدارة النظم على نظم وبرامج مخصصة للأمن السيبراني.
T0039	تحليل المخاطر كلما خضع أي برنامج أو نظام لتغيير جوهري.

رمز المهمة	وصف المهمة
T0040	تحليل نتائج التمارين وبيئة النظام للتخطيط وللتوصية بتعديلات وتسويات.
T0041	إعداد تقارير التدقيق والتقييم التي تحدد النتائج التقنية والإجرائية، وتشمل توصيات بالاستراتيجيات والحلول العلاجية.
T0042	تقديم إرشادات توعوية في مجال الأمن السيبراني لدعم خطط استمرارية الأعمال وحماية البيانات.
T0043	توفير مدخلات لإطار إدارة المخاطر والوثائق ذات الصلة.
T0044	تحليل تنبيهات الشبكة التي يتم الحصول عليها من مصادر مختلفة لتحديد الأسباب المحتملة لأي أحداث يتم اكتشافها.
T0045	مراجعة السياسات القائمة والمقترحة والوثائق ذات العلاقة مع أصحاب المصلحة.
T0046	توفير الخبرة الاستشارية في الأمن السيبراني في مجالس السياسات التنظيمية والقطاعية.
T0047	تتبع الحوادث السيبرانية وتوثيقها منذ اكتشافها إلى حلها النهائي.
T0048	تتبع نتائج وتوصيات التدقيق لضمان اتخاذ إجراءات معالجة ملائمة.
T0049	تسخير أدوات مراقبة الشبكات لرصد وتحليل حركة البيانات الشبكية ذات العلاقة بالعمليات الضارة.
T0050	مراجعة وثائق الأمن السيبراني العاكسة لتصميم النظام، وتحديثها وحفظها.
T0051	كتابة ونشر أساليب وإرشادات الدفاع السيبراني وتقارير الأحداث السيبرانية، ومشاركتها مع الجهات ذات العلاقة.
T0052	البحث في التقنيات المعاصرة لفهم قدرات الدفاع السيبراني المطلوبة من قبل النظم أو الشبكة.
T0053	ضمان تعريف مخاطر الأمن السيبراني ومعالجتها بالطريقة المناسبة من خلال عملية حوكمة المخاطر للمنظمة.
T0054	الكشف عن الهجمات والأنشطة المشبوهة وحالات إساءة الاستخدام، والتعرف عليها والتنبيه بشأنها في الوقت المناسب، وتمييزها عن الأنشطة الاعتيادية.
T0055	تسخير أدوات الدفاع السيبراني للمراقبة المستمرة لأنشطة النظم وتحليلها بهدف تعريف الأنشطة الضارة.
T0056	تحليل الأنشطة الخبيثة لتحديد الثغرات المستغلة، وأساليب الاستغلال، والتأثيرات على النظم والمعلومات.
T0057	تحديد حماية البنية التحتية الحاسمة للدفاع السيبراني ومواردها، وترتيب أولوياتها وتنسيقها.

رمز المهمة	وصف المهمة
T0058	تطبيق مبادئ وممارسات الدفاع الأمني متعدد المستويات بما يتماشى مع سياسات المنظمة.
T0059	إدارة معالجة الثغرات بفعالية.
T0060	ضمان الحفاظ على سجل تدقيق أدلة التدابير الأمنية.
T0061	ضمان مراعاة متطلبات المنظمة للأمن السيبراني في عمليات الدمج والاستحواذ والاستعانة بالموارد الخارجية وغيرها من العمليات التي تشمل طرفا ثالثا.
T0062	جمع آثار التسلل، واستخدام البيانات المكتشفة للحد من حوادث الأمن السيبراني المحتملة داخل المنظمة.
T0063	المراجعة الدورية لاستراتيجية الأمن السيبراني وسياساته والوثائق ذات العلاقة للمحافظة على الالتزام بالقوانين والأنظمة المعمول بها.
T0064	تحديد الخطط والأساليب و الإجراءات (TTP) لمجموعات التسلل.
T0065	فحص المخططات الشبكية لفهم تدفقات البيانات عبر الشبكة.
T0066	التوصية بتصحيحات لثغرات البيئة.
T0067	استخدام البيانات الوصفية للتعرف على حالات الاشتباه في حركة مرور البيانات عبر الشبكة وتحليلها.
T0068	تحديد المؤشرات والتحذيرات من خلال البحث والتحليل والربط عبر مجموعات بيانات متعددة.
T0069	استخدام أدوات تحليل الحزم للتحقق من تنبيهات نظام كشف التسلل.
T0070	عزل البرمجيات الضارة وإزالتها.
T0071	استخدام حركة مرور البيانات عبر الشبكة لتحديد تطبيقات أحد أجهزة الشبكة ونظم التشغيل الخاصة به.
T0072	استخدام حركة المرور عبر الشبكات لإعادة تمثيل النشاط الخبيث.
T0073	تحديد عمليات محاولة التعرف على التصميم الشبكي وأنشطة التعرف على أنظمة التشغيل.
T0074	تقييم فاعلية ضوابط الأمن السيبراني.
T0075	المساعدة في حصر خواص التعرف (التواقيع) لتفعيل استخدامها في أدوات الأمن السيبراني للشبكة وذلك للاستجابة للتهديدات الجديدة والتهديدات التي تمت ملاحظتها سابقاً.
T0076	الإبلاغ عن الحوادث السيبرانية المشتبه بها وفقًا لخطة المنظمة للاستجابة للحوادث السيبرانية.

رمز المهمة	وصف المهمة
T0077	الإشراف على الموظفين القائمين على مهام الأمن السيبراني وإسناد الأعمال إليهم بفاعلية.
T0078	ضمان توفير التمويل الكافي لموارد التدريب للأمن السيبراني.
T0079	تقييم عملية إدارة الإعدادات.
T0080	جمع المقاييس وبيانات التوجهات.
T0081	تخصيص الموارد لأدوار الأمن السيبراني.
T0082	ضمان التزام سياسات وعمليات إدارة كوادر الأمن السيبراني بالمتطلبات القانونية ومتطلبات المنظمة.
T0083	تقديم المعلومات التقنية للجماهير التقنية وغير التقنية.
T0084	عرض البيانات بصيغ مبتكرة.
T0085	رفع الوعي بالسياسة والاستراتيجية السيبرانية بين مديري المنظمة.
T0086	مراجعة وتقييم فاعلية الكوادر السيبرانية لتحديد الفجوات في المهارات واحتياجات التدريب.
T0087	تحرير ونشر المراجعات للتعلم ولنشر الدروس المستفادة من أحداث الأمن السيبراني.
T0088	تفسير وتطبيق الأنظمة المطبقة والقوانين واللوائح والوثائق التنظيمية لضمان عكسها في سياسات الأمن السيبراني.
T0089	تحديد وتطوير أدوات الهندسة العكسية لتعزيز القدرات والكشف عن الثغرات.
T0090	تطوير قدرات إدارة البيانات الآمنة لدعم القوى العاملة المتنقلة.
T0091	تمكين التطبيقات بالمفاتيح العامة من خلال مكتبات البنية التحتية للمفاتيح العمومية القائمة، مع تضمين إدارة الشهادات والتشفير حسب الحاجة.
T0092	تحليل سياسات الأمن السيبراني للمنظمة.
T0093	العمل مع أصحاب المصلحة لتطوير سياسات الأمن السيبراني والوثائق المصاحبة بما يتوافق مع استراتيجية الأمن السيبراني للمنظمة.
T0094	التعريف والدمج ما بين بيئة الرسالة الحالية والمستقبلية لضمان الحفاظ على التجانس وتقليل الأعباء الإدارية.
T0095	موافقة استراتيجية الأمن السيبراني للمنظمة مع استراتيجيتها للأعمال.

رمز المهمة	وصف المهمة
T0096	تصميم ضوابط وإجراءات أمن النُظم التي توفر السرية والسلامة والتوافر والتحقق وعدم الإنكار، وتطويرها وتحقيق تكاملها وتحديثها.
T0097	تحليل التوجهات في الحالة الأمنية للمنظمة، والإبلاغ عنها.
T0098	تحليل التوجهات في الحالة الأمنية للنُظم، والإبلاغ عنها.
T0099	صياغة ونشر سياسات الأمن السيبراني للمنظمة.
T0100	تقييم مدى كفاية ضوابط التحكم بالوصول بناء على سياسات المنظمة.
T0101	مراقبة مصادر البيانات الخارجية للمحافظة على فهم محدث لحالة تهديدات الأمن السيبراني وتحديد القضايا الأمنية التي قد تؤثر على المنظمة.
T0102	تقييم ومراقبة جوانب الأمن السيبراني لممارسات المنظمة بتطبيق النُظم واختبارها.
T0103	مراقبة مدى كفاءة التطبيق لسياسات ومبادئ وممارسات الأمن السيبراني عند تقديم خدمات التخطيط والإدارة.
T0104	السعي إلى توافق آراء أصحاب المصلحة بشأن التغييرات المقترحة في سياسة الأمن السيبراني.
T0105	إجراء تقييم لمخاطر الأمن السيبراني.
T0106	تنسيق وظائف الاستجابة للحوادث.
T0107	تقديم توصيات الأمن السيبراني للقيادة استنادًا إلى التهديدات والثغرات الجسيمة.
T0108	تقديم إرشادات في حق السياسة لإدارة الأمن السيبراني والعاملين والمستخدمين.
T0109	مراجعة تدقيقات البرامج والمشاريع السيبرانية، أو تنفيذها، أو المشاركة فيها.
T0110	دعم المسؤول الأول لتقنية المعلومات (CIO) في صياغة سياسات الأمن السيبراني.
T0111	العمل مع أصحاب المصلحة لحل حوادث الأمن السيبراني وقضايا الثغرات في الالتزام.
T0112	توفير المشورة في الأمن السيبراني ومدخلات لخطط التعافي من الكوارث، وخطط الأحداث الطارئة، وخطط استمرارية التشغيل.
T0113	أداء تقييمات تقنية وغير تقنية للمخاطر والثغرات للبيئات التقنية للمنظمة.
T0114	تطبيق وظائف الأمن السيبراني (مثل التشفير والتحكم في الوصول وإدارة الهوية) لتقليل فرص الاستغلال.

رمز المهمة	وصف المهمة
T0115	البقاء على معرفة بتهديدات الأمن السيبراني على المنظمة.
T0116	البحث والتحليل المتعمقان في تهديدات الأمن السيبراني.
T0117	توفير مصادر المعلومات المطلوبة للإجابة على طلبات المنظمة لمعلومات الأمن السيبراني.
T0118	إنشاء طلبات لمعلومات الأمن السيبراني.
T0119	إنتاج تقارير المعلومات الإستباقية للتهديدات السيبرانية ذات العلاقة بوقت قصير، وذلك بدمج المعلومات من مصادر متعددة.
T0120	توفير معلومات إستباقية حديثة عن تهديدات الأمن السيبراني لدعم أصحاب المصلحة الأساسيين في الاستجابة لتهديدات وحوادث الأمن السيبراني.
T0121	توفير تقييمات وتغذية راجعة لمصادر المعلومات الإستباقية لتهديدات الأمن السيبراني من أجل تطوير جودة معلوماتهم.
T0122	توفير إشعارات وقت حاجتها بالنوايا أو الأنشطه الوشيكة أو العدوانية والتي قد تؤثر على أهداف المنظمة أو مواردها أو قدراتها.
T0123	العمل بشكل وثيق مع أصحاب المصلحة لضمان أن المعلومات الاستباقية المتاحة للمنظمة ذات العلاقة بالتهديدات السيبرانية مفيدة ودقيقه ومحدثه.
T0124	تحديد خطط ومنهجيات التهديدات السيبرانية ذات الصلة بالمنظمة.
T0125	تحديد مصطلحات اللغات الأجنبية داخل برامج الحاسبات.
T0126	التعاون مع الآخرين بشأن السياسات والعمليات والإجراءات ذات العلاقة بالخصوصية والأمن السيبراني.
T0127	ضمان وضع الضوابط الملائمة للحد من مخاطر الأمن السيبراني بفاعلية ومعالجة مخاوف الخصوصية خلال عملية تقييم المخاطر.
T0128	التعاون مع الآخرين لتنفيذ وحفظ برنامج إدارة مخاطر الأمن السيبراني.
T0129	انتقاء أفراد وإسناد أدوار محددة لهم فيما يتعلق بتنفيذ إطار إدارة المخاطر.
T0130	وضع استراتيجية إدارة المخاطر بالمنظمة، شاملة تحديد مستوى تحمل المخاطر.
T0131	إجراء تقييم مخاطر أولي لأصول أصحاب المصلحة وتحديث تقييم المخاطر بصفة مستمرة.
T0132	العمل مع المسؤولين بالمنظمة لضمان أن بيانات أدوات المراقبة المستمرة توفر الوعي بمستويات المخاطر القائمة.
T0133	استخدام أدوات المراقبة المستمرة لتقييم المخاطر باستمرار.
T0134	تطوير عناصر المعمارية الأمنية للحد من التهديدات عند نشوئها.

رمز المهمة	وصف المهمة
T0135	مراجعة وتحليل تهديدات الأمن السيبراني لتزويد أصحاب المصلحة بالمعلومات المطلوبة للاستجابة إلى هذه التهديدات.
T0136	تقديم توصيات لتمكين المعالجة الفعالة للثغرات.
T0137	ضمان عكس مبادئ سليمة للأمن السيبراني على رسالة المنظمة ورؤيتها وأهدافها.
T0500	تقديم حلول سحابية آمنة إلى فرق التطوير، وضمان أمان السحب المنقولة، وأمان عملية تطوير التطبيقات السحابية.
T0501	العمل ضمن فرق متعددة التخصصات كخبير متخصص في معايير معمارية الأمن السحابي ومنهجياتها.
T0502	تقييم التصاميم الأمنية ومعماريتها، وتحديد مدى كفايتها.
T0503	تطوير وتنفيذ استراتيجية سحابية آمنة بالتلازم مع أعمال المعمارية المؤسسية.
T0504	تطوير وتنفيذ أنماط آمنة لاستهلاك فرق التقنية للخدمات السحابية.
T0505	بناء حلول لتحديد بيانات المنظمة المتواجدة بداخل البيئات السحابية.
T0506	توفير الخبرة المتخصصة لتطوير وهندسة الجيل القادم من الأمن السيبراني.
T0507	تنفيذ عمليات آمنة لإدارة الإعدادات.
T0508	تحديد وظائف الأعمال الحيوية وتصنيف أولوياتها بالتعاون مع أصحاب المصلحة بالمنظمة.
T0509	تقديم استشارات بشأن تكاليف المشاريع، ومفاهيم التصميم التابعة لها، أو التغييرات على تصاميمها.
T0510	تقديم المشورة بشأن المتطلبات الأمنية المطلوب إدراجها في وثائق المشتريات.
T0511	تحليل المعمارية المرشحة، وتخصيص الخدمات الأمنية واختيار الآليات الأمنية.
T0512	تعريف السياق الأمني للنُظم، ومفهوم العمليات واحتياجاتها المبدئية، وفقًا لسياسات الأمن السيبراني المطبقة.
T0513	تقييم ما ورد في وثائق المشتريات من اقتراحات للمعمارية الأمنية وتصاميمها.
T0514	تحرير المواصفات الوظيفية التفصيلية التي توثق عملية تطوير المعمارية.
T0515	تحليل احتياجات المستخدم ومتطلباته لتخطيط المعمارية.

رمز المهمة	وصف المهمة
T0516	تطوير المعمارية المؤسسية أو مكونات النظام المطلوبة لتلبية احتياجات المستخدم.
T0517	توثيق وتحديث كل أنشطة التعريف والمعمارية، حسب الضرورة.
T0518	تحديد ضوابط الأمن لنظم المعلومات والشبكات، مع توثيقها على نحو ملائم.
T0519	تقييم وتصميم وظائف إدارة الأمن السيبراني.
T0520	تعريف لمستويات التوافر المناسبة لوظائف النظم الحرجة ومتطلبات عمليات التعافي من الكوارث والاستمرارية لتقديمها.
T0521	بناء الضوابط الأمنية حيث يلزم لمراقبة وحماية المعلومات المخزنة في البيئات السحابية على نحو ملائم.
T0522	تقديم المشورة المتخصصة في أمن معمارية الحوسبة السحابية شاملا الشبكات، والتخزين، وقواعد البيانات، والتوفير والإدارة.
T0523	تحديد وترتيب أولويات قدرات النُظم أو وظائف الأعمال اللازمة لاستعادة النظام جزئيًا أو كليًا بعد وقوع عطل كارثي.
T0524	تطوير ودمج تصاميم الأمن السيبراني للنُظم والشبكات والتي لها متطلبات أمن متعددة المستويات.
T0525	توثيق ومعالجة متطلبات المنظمة للأمن السيبراني في المعمارية وهندسة النظم في كافة مراحل عمليات الشراء والاستحواذ.
T0526	ضمان اتساق النُظم والمعمارية التي تمت حيازتها أو تطويرها مع إرشادات المنظمة لمعمارية الأمن السيبراني.
T0527	ترجمة القدرات المقترحة إلى متطلبات تقنية.
T0528	العمل مع أعضاء فريق التطوير المرن لتسريع إعداد نماذج أولية ودراسات الجدوى وتقييم التقنيات الحديثة.
T0529	تصميم نُظم وحلول لدعم نجاح "حلول إثبات المبدأ" والمشاريع التجريبية في مجالات التقنيات الناشئة.
T0530	قراءة وتفسير المخططات والمواصفات والرسومات والتصاميم الأولية والرسومات البيانية التخطيطية ذات العلاقة بالأنظمة والشبكات.
T0531	تحديد وتوثيق الضوابط الأمنية للأنظمة والشبكات.
T1000	تحليل وتحديد متطلبات البيانات ومواصفاتها.
T1001	التحليل والتخطيط للتغييرات المتوقعة في متطلبات سعة البيانات.

رمز المهمة	وصف المهمة
T1002	تحليل المعلومات لتحديد متطلبات التطوير لبرنامج جديد أو تعديل برنامج قائم، والتوصية والتخطيط في ذلك كله.
T1003	تحليل كيفية تلبية احتياجات المستخدم ومتطلبات البرمجيات بما يتماشى مع سياسات الأمن السيبراني، وتحديد مدى واقعية التصميم، ضمن القيود الزمنية والمالية.
T1004	تحليل قيود التصميم والمفاضلات في التصميم التفصيلي للأمن السيبراني للنظام مع الأخذ في الاعتبار دعم دورة حياة النظام.
T1005	تطبيق معايير الأمن للبرمجة والاختبار.
T1006	توثيق الشفرات البرمجية الآمنة.
T1007	تقييم فاعلية تدابير الأمن السيبراني للنظم.
T1008	بناء نماذج أولية للمنتجات واختبارها وتعديلها، للبرهنة على التزامها بمتطلبات الأمن السيبراني، وذلك من خلال النماذج الفعلية أو النظرية.
T1009	دمج الأمن السيبراني في عملية المتطلبات عن طريق تعريف الضوابط الأمنية وتوثيقها.
T1010	ضمان توثيق سير تطوير البرامج وتحديثها، وضمان قدرة الآخرين على فهمها من خلال إدراج التعليقات في الشفرات البرمجية.
T1011	تحديد قيود المشاريع، وقدراتها، ومتطلبات أدائها، ومواطن ارتباطها.
T1012	إصدار نموذج التهديدات استنادًا إلى المقابلات مع العملاء وتحديد متطلباتهم.
T1013	تقييم مواطن الارتباط بين العتاد والبرامج من خلال التشاور مع الكوادر الهندسية.
T1014	ضمان إنتاج النتائج المرغوبة من خلال إعادة التحقق من البرنامج وإجراء التغييرات المناسبة لتصحيح الأخطاء.
T1015	تصميم وتطوير الأمن السيبراني أو المنتجات المدعومة بالأمن السيبراني.
T1016	تصميم العتاد ونُظم التشغيل وتطبيقات البرمجيات لتلبية متطلبات الأمن السيبراني.
T1017	تصميم أو دمج النسخ الاحتياطي الآمن، والتخزين المحمي لقدرات النسخ الاحتياطية للبيانات، حسب المناسب في التصاميم.
T1018	تطوير وتوجيه الإجراءات وأعمال التوثيق لعمليات اختبار النظم وعمليات المصادقة.
T1019	مراجعة برامج التنقيب عن البيانات ومستودعات البيانات وعملياتهما ومتطلباتهما، والتحقق من مصداقيتها.

رمز المهمة	وصف المهمة
T1020	تطوير معايير البيانات وسياساتها وإجراءاتها.
T1021	تطوير وثائق التصميم الأمني التفصيلية بخصوص مواصفات المكونات والواجهات لدعم تصميم النظام وتطويره.
T1022	تطوير واختبار خطط التعافي من الكوارث واستمرارية العمليات للنُظم الخاضعة للتطوير وذلك قبل إدخال النظم في بيئة الإنتاج الحية.
T1023	تطوير عمليات البرمجة الآمنة وعمليات التعامل مع الأخطاء، وتوثيقهما.
T1024	الإفادة بمعلومات لمهام إعداد الأجهزة من خلال تقييم القيود المالية والقيود الأمنية.
T1025	فحص البيانات المستعادة للحصول على معلومات ذات علاقة بأحداث وحوادث الأمن السيبراني.
T1026	تحديد وتخصيص الوظائف الأمنية للمكونات، ووصف العلاقات بينها.
T1027	تحديد وتوجيه معالجة المشكلات التقنية التي تتم مواجهتها في أثناء اختبار وتنفيذ نُظم جديدة.
T1028	تعريف وتحديد أولويات الوظائف الأساسية للنظام أو النظم الفرعية المطلوبة لدعم قدرات ووظائف الأعمال الأساسية بالمنظمة للاستعادة أوالتعافي بعد فشل النظام أو خلال حدث التعافي بناء على متطلبات النظام الكلية للاستمرارية والتوافر.
T1029	تعريف الأخطاء البرمجية الأساسية الشائعة على مستوى عال.
T1030	تطبيق المنهجيات لإصلاح الأخطاء البرمجية الشائعة ذات التبعات الأمنية لضمان تطوير برمجيات آمنة.
T1031	ضمان تضمين الأمن السيبراني بداخل عمليات تطوير البرامج، وحفظها، وإخراجها من الخدمة.
T1032	ضمان تضمين الأمن السيبراني في تصميم النظام.
T1033	ضمان إدراج تنبيهات الثغرات الأمنية في تصاميم النظام.
T1034	إدارة تجميع البيانات، وفهرستها، والتخزين المؤقت لها، وتوزيعها واسترجاعها.
T1035	إجراء اختبارات مدمجة لضمان جودة وظائف الأنظمة الأمنية وصمودها.
T1036	إعداد مخططات تدفق العمليات والرسومات البيانية التي توضح المدخلات والمخرجات والعمليات المنطقية للأنظمة الأمنية.
T1037	توفير تدفق منظم للمعلومات ذات الصلة (عن طريق البوابات الإلكترونية على الشبكة العنكبوتية أو الوسائل الأخرى) حسب متطلبات الرسالة.

رمز المهمة	وصف المهمة
T1038	تقديم إرشادات لتنفيذ النظم المطورة للعملاء أو فرق التركيب.
T1039	تقديم توصيات بشأن التقنيات والمعمارية الجديدة لقواعد البيانات.
T1040	معالجة التبعات الأمنية في مرحلة قبول البرمجيات.
T1041	تخزين البيانات واسترجاعها ومعالجتها لتحليل قدرات النظام ومتطلباته.
T1042	تقديم دعم لاختبارات الترخيص الأمنية وأنشطة التقييم.
T1043	ترجمة المتطلبات الأمنية إلى عناصر تصميم التطبيق، بما في ذلك توثيق عناصر الأجزاء المعرضة للهجوم في البرمجيات و تصميم نماذج للتهديدات وتحديد أي ضوابط أمنية خاصة.
T1044	استخدام النماذج والمحاكاة لتحليل أداء النظام في ظل ظروف تشغيل مختلفة أو التنبؤ به.
T1045	تحديد استراتيجيات القدرات السيبرانية لتطوير الأجهزة والبرمجيات المخصصة حسب متطلبات المنظمة.
T1046	ضمان إجراء اختبارات الاختراق عند الحاجة للتطبيقات الجديدة أو المحدَّثة.
T1047	تصميم وتطوير وظائف إدارة الأمن السيبراني الرئيسية.
T1048	تحليل احتياجات ومتطلبات المستخدمين للتخطيط لأمن النظام وتطويره.
T1049	تطوير تصاميم الأمن السيبراني لتلبية احتياجات تشغيلية وعوامل بيئية محددة.
T1050	التعاون مع أصحاب المصلحة لتحديد الحلول التقنية المناسبة.
T1051	تصميم وتطوير أدوات وتقنيات الأمن السيبراني الجديدة.
T1052	تحديد النظام المؤسسي للتحكم بالإصدارات عند تصميم وتطوير التطبيقات الآمنة، والاستفادة منه.
T1053	تنفيذ منهجيات دورة حياة تطوير النُظم ودمجها في بيئة التطوير لأنظمة الأمن السيبراني.
T1054	استشارة العملاء بخصوص تصميم أنظمة الأمن السيبراني وصيانتها.
T1055	توجيه أعمال البرمجة لتطبيقات الأمن السيبراني وأعمال تطوير مستنداتها التوثيقية.
T1056	توظيف عمليات إدارة الإعدادات عند تنفيذ أنظمة الأمن السيبراني.

رمز المهمة	وصف المهمة
T1057	تقييم الثغرات في بنية الشبكات.
T1058	اتباع معايير وعمليات دورة حياة هندسة البرمجيات والنُظم عند تطوير نظم وحلول الأمن السيبراني.
T1059	تحليل مصادر البيانات لتقديم توصيات قابلة للتنفيذ.
T1060	تقييم صلاحية البيانات المصدرية والنتائج اللاحقة.
T1061	اختبار الفرضيات باستخدام العمليات الإحصائية.
T1062	التشاور مع محللي النُظم والمهندسين والمبرمجين وغيرهم لتصميم تطبيقات الأمن السيبراني.
T1063	تصميم الواجهات الآمنة بين نُظم المعلومات والنُظم المادية والتقنيات المدمجة، وتنفيذها واختبارها وتقييمها.
T1064	تطوير منهجيات جمع البيانات وإتاحتها.
T1065	تطوير الرؤى الاستراتيجية من مجموعات البيانات الكبيرة.
T1066	برمجة خوارزميات مخصصة.
T1067	تقديم توصيات قابلة للتطبيق لأصحاب المصلحة، استنادًا إلى تحليل البيانات والنتائج.
T1068	استخدام المستندات أو الموارد التقنية لتنفيذ طريقة رياضية جديدة أو طريقة تعتمد على علوم البيانات أو علوم الحاسوب.
T1069	التخصيص الفعّال لسعة التخزين في تصميم نُظم إدارة البيانات.
T1070	قراءة النصوص البرمجية البسيطة وتفسيرها وتحريرها وتعديلها وتنفيذها لأداء المهام.
T1071	استخدام لغات برمجة مختلفة لكتابة الشفرات البرمجية ولفتح الملفات، ولقراءتها، ولكتابة المخرجات في ملفات مختلفة.
T1072	استخدام لغات مفتوحة المصدر.
T1073	استكشاف أخطاء التصاميم في نماذج الجدوى الأولية، ومعالجة المشاكل عبر مراحل تصميم المنتجات، وتطويرها، والإعداد لإطلاقها.
T1074	إيجاد فرص تطوير القدرات الجديدة لمعالجة الثغرات.
T1075	تحديد العمليات والخدمات الأمنية المؤسسية عند تصميم وتطوير التطبيقات الآمنة، والاستفادة منها.

رمز المهمة	وصف المهمة
T1076	إجراء أعمال التحليل لتقديم معلومات إلى أصحاب المصلحة بما يدعم تطوير تطبيقات أمنية أو تعديلها.
T1077	تحليل الاحتياجات الأمنية ومتطلبات البرمجيات، لتحديد جدوى التصميم ضمن الحدود الزمنية وقيود التكلفة والالتزامات الأمنية.
T1078	التشغيل التجريبي للبرامج وتطبيقات البرمجيات، لضمان إنتاج المعلومات المرغوبة، وضمان سلامة التعليمات والمستويات الأمنية.
T1079	التصميم حسب المتطلبات الأمنية، لضمان تلبية المتطلبات لجميع النُظم والتطبيقات.
T1080	تطوير إجراءات اختبار النظام ومصادقتها، والبرمجة والتوثيق.
T1081	تطوير إجراءات اختبار البرمجيات الآمنة والمصادقة عليها.
T1082	تطوير إجراءات اختبارات النظم ومصادقتها، شاملا البرمجة والتوثيق.
T1083	تطوير وتنفيذ برامج استخراج البيانات وبرامج مستودعات البيانات.
T1084	وضع استراتيجيات المعالجة لمواجهة المخاطر ذات الصلة بالتكلفة والجداول الزمنية والأداء والأمن.
T1085	تعديل البرمجيات القائمة وحفظها لتصحيح الأخطاء أو تكييفها مع أجهزة جديدة أو ترقية الواجهات وتحسين الأداء.
T1086	إجراء اختبارات ومراجعات وتقييمات البرامج الآمنة لتحديد مواطن الخلل المحتملة في الشفرات البرمجية ومعالجة الثغرات.
T1087	إجراء المراجعات الأمنية وتحديد الفجوات الأمنية في البنية المعمارية.
T1088	تقديم المدخلات للخطط التنفيذية لأمن أنظمة المعلومات وإجراءات التشغيل النمطية.
T1089	تتبع متطلبات النظام لتصميم المكونات وإجراء تحليل الفجوة.
T1090	التحقق من أن معمارية النظام مستقرة، وتحقق التشغيل البيني، وقابلة للنقل، وقابلة للتوسع.
T1091	بحث وتقييم التقنيات والمعايير المتوفرة، لتلبية متطلبات العملاء.
T1092	تحديد وتوثيق حزم تحديثات الإصلاح للبرمجيات أو نطاق الإصدارات الذي سينشأ عنه ثغرات بالبرامج.
T1093	مراجعة المتطلبات التشغيلية للبحث والتطوير والاستحواذ للقدرات السيبرانية، واعتمادها، وترتيب أولوياتها، وتقديمها.
T1094	تطوير العمليات المؤتمتة وحلول الذكاء الاصطناعي ذوات التصنيف العالمي.

رمز المهمة	وصف المهمة
T1095	تحديد وتطوير الحلول الحسابية المؤتمتة، شاملا الحلول التحليلية والخوارزمية.
T1096	تعزيز الأساليب الإحصائية والتعلُّم الآلي لتحديد الاتجاهات والتحليل التنبئي.
T1097	تطبيق المعرفة في التعلّم الآلي، أو الإبصار الحاسوبي، أو الاستشعار عن بُعد ومعالجة البيانات الكبيرة لأجل معالجة المشاكل المهمة من خلال تطوير البرمجيات لتحديد الخوارزميات والمنهجيات المناسبة.
T1098	تحليل البيانات وإجراء تحليل كمي للبيانات باستخدام مجموعة متنوعة من مجموعات البيانات لتحديد العمليات ومراقبتها واستكشافها.
T1099	مواكبة أبحاث الإبصار الحاسوبي والتعلُّم الآلي لنسخ وتأسيس أساليب جديدة.
T1100	استخدام الأدوات المرئية لتصور البيانات وإنشاء لوحات المعلومات لإيصال النتائج.
T1101	تشخيص البيانات وإجراء التحليل الإحصائي والتحليل من خلال التعلّم الآلي.
T1102	تحويل المخططات التفصيلية لسير العمل والرسومات البيانية للأنظمة الأمنية إلى سلسلة من التعليمات البرمجية بلغة الحاسب.
T1103	استخدام التقنيات الكمية.
T1104	تحديد المشكلات الأمنية المتعلقة بالتشغيل المستقر للبرامج وإدارتها وعمل الإجراءات الأمنية اللازمة عندما يصل منتج معين لنهاية دورة حياته.
T1500	حيازة الموارد اللازمة لتطوير وتطبيق عمليات فعالة تلبي الأهداف الأمنية والمعلوماتية الاستراتيجية.
T1501	فهم الحالة الأمنية لمعلومات المنظمة والتعبير عنها خلال عمليات التمحيص القانوني والتنظيمي.
T1502	ضمان جمع وحفظ البيانات اللازمة لتلبية المتطلبات المحددة لتقارير الأمن السيبراني.
T1503	دعم الأمن السيبراني وإبراز قيمته لدى أصحاب المصلحة في المنظمة.
T1504	ضمان تقييم أنشطة التحسينات الأمنية، وتنفيذها ومراجعتها حسب الحاجة.
T1505	ضمان تنسيق حملات تفتيش الأمن السيبراني في البيئة الشبكية، وأعمال الاختبارات والمراجعات.
T1506	ضمان إدراج متطلبات الأمن السيبراني في كافة عمليات التخطيط لاستمرارية الأعمال وتلافي الكوارث.
T1507	ضمان توافق تصاميم معمارية الأمن السيبراني مع استراتيجية الأمن السيبراني للمنظمة.
T1508	تقييم جهود التطوير للأنظمة والإجراءات الجديدة لضمان تطبيق الضوابط الأمنية المناسبة.

رمز المهمة	وصف المهمة
T1509	تحديد استراتيجيات الأمن السيبراني البديلة لتحقيق الغاية الأمنية للمنظمة.
T1510	تحديد تبعات التقنيات الجديدة وأعمال الترقية على الأمن السيبراني في جميع أرجاء المنظمة.
T1511	التواصل بفاعلية مع الأطراف الخارجية عند وقوع حادث أمن سيبراني.
T1512	مراجعة قدرات الأمن السيبراني للتقنيات الجديدة المقترحة قبل تبني المنظمة لها، واعتمادها في حال مناسبتها.
T1513	ضمان المحافظة على حالة وعي شامل للأمن السيبراني للمنظمة.
T1514	ضمان الإدارة الملائمة لمعلومات الأمن السيبراني للمنظمة، وتقييمها ومشاركتها بصفة ملائمة.
T1515	مراجعة فاعلية ضوابط الأمن السيبراني للمنظمة ومواءمتها لأهدافها الاستراتيجية.
T1516	ضمان التنفيذ الدوري لبرامج التدريب والتوعية بالأمن السيبراني.
T1517	المشاركة في تقييم مخاطر الأمن السيبراني حسب ما تقتضيه الحاجة.
T1518	المشاركة في تطوير أو تعديل خطط ومتطلبات برنامج الأمن السيبراني.
T1519	ضمان تطوير جميع الوثائق الخاصة بأمن الشبكات، وإصدارها وصيانتها.
T1520	ضمان توفير التدريب التوعوي بالأمن السيبراني لجميع الموظفين بالمنظمة.
T1521	ضمان إدراج متطلبات الأمن السيبراني في أعمال الشراء حسب الملائم.
T1522	التأكد من تقديم تقارير مناسبة إلى الإدارة العليا حسب الحاجة.
T1523	تحديد الحوادث الأمنية المحتملة والإبلاغ عنها حسب الحاجة.
T1524	التأكد من تخصيص الموارد الملائمة لتحقيق متطلبات الأمن السيبراني بالمنظمة.
T1525	إدارة التقييم والصيانة الدورية لسياسات الأمن السيبراني بالمنظمة والوثائق ذات العلاقة.
T1526	التأكد من اتخاذ الإجراءات الملائمة لمعالجة الخطر عند وقوع حادثة متعلق بالأمن السيبراني.
T1527	استخدام الوثائق المتاحة دوليًا ذات العلاقة بالأمن السيبراني لإفادة وتعزيز وثائق المنظمة.

رمز المهمة	وصف المهمة
T1528	دعم القضايا الأمنية لدى الإدارة العليا، والتأكد من شمول الأمن السيبراني ضمن الأهداف الإستراتيجية.
T1529	التأكد من معالجة استراتيجية الأمن السيبراني للمنظمة بفعالية من خلال سياسات الأمن السيبراني والوثائق ذات الصلة.
T1530	تقييم فاعلية وكفاءة وظيفة المشتريات في ضمان معالجة متطلبات الأمن السيبراني ومخاطر سلسلة الإمداد حسب الحاجة، وتنفيذ التحسينات أينما لزمت.
T1531	التأكد من تحديد متطلبات الأمن السيبراني لكافة أنظمة تقنية المعلومات.
T1532	المشاركة في عملية الاستحواذ حسب الضرورة، مع ضمان تبني الممارسات المناسبة لإدارة مخاطر سلسلة الإمداد.
T1533	التأكد من توفر موارد للأمن السيبراني الملائمة على الدوام.
T1534	تطوير سياسات الأمن السيبراني المناسبة والوثائق ذات العلاقة وحفظها لضمان حماية البنية التحتية الحساسة للمنظمة بشكل ملائم.
T1535	التعاون مع أصحاب المصلحة في المنظمة والأطراف الآخرين عند تحديد المتطلبات المستقبلية للخطة الاستراتيجية للأمن السيبراني.
T1536	تحديد وتعيين الموارد الخبيرة الملائمة للقيام بأنشطة الأمن السيبراني في المنظمة.
T1537	تزويد الإدارة العليا بموجز عن التطورات والتوجهات في الأمن السيبراني.
T1538	تزويد الإدارة العليا بموجز عن ضوابط الأمن السيبراني اللازمة لحماية المنظمة.
T1539	تقييم نواحي الأمن السيبراني عند اختيار وتقييم الموردين.
T1540	إعداد التقارير عن أحداث وفعاليات الأمن السيبراني الدولية لصالح الإدارة العليا.
T1541	حضور الفعاليات الدولية للأمن السيبراني وإلقاء الكلمات فيها.
T1542	ضمان المراجعة الدورية للفرضيات ذات العلاقة بالأمن السيبراني.
T2000	حيازة الموارد الملائمة لتنفيذ وحفظ جوانب الأمن السيبراني لخطة استمرارية أعمال فعالة.
T2001	إحاطة الإدارة العليا بالتغييرات الهامة في وضع الأمن السيبراني للمنظمة.
T2002	إجراء التدريبات التفاعلية لخلق بيئة تعليمية فعَّالة.

رمز المهمة	وصف المهمة
T2003	تطوير وحفظ خطط استراتيجية للأمن السيبراني تتوافق مع خطة الأعمال الاستراتيجية للمنظمة.
T2004	تطوير أو تحديد مواد تدريبية للتوعية مناسبة للجمهور المستهدف.
T2005	تقييم فاعلية برامج التدريب الحالية وشموليتها.
T2006	تحديد أصحاب المصلحة في السياسة التنظيمية.
T2007	التأكد من أن متطلبات الأمن السيبراني لتقنية المعلومات تتوافق مع استراتيجية الأمن السيبراني في المنظمة.
T2008	إدارة الجوانب المالية للأمن السيبراني شاملة إعداد الميزانية وتوفير الموارد.
T2009	التأكد من فاعلية إيصال المعلومات التي تخص تهديدات الأمن السيبراني وأساليب معالجتها إلى الأطراف الأخرى المهتمة.
T2010	مراجعة وثائق التدريب للأمن السيبراني.
T2011	دعم تصميم وتنفيذ سيناريوهات التمارين.
T2012	كتابة المواد التعليمية لتقديم إرشادات تفصيلية إلى موظفي المنظمة ووحداتها.
T2013	تطوير وحدات تدريبية يتم تنفيذها من خلال الحاسبات أو الفصول الدراسية، أو المساعدة في تطويرها.
T2014	تطوير واجبات مرتبطة بالدورات التدريبية أو المساعدة في تطويرها.
T2015	تطوير تقييمات الدورات أو المساعدة في تطويرها.
T2016	تطوير معايير رصد الدرجات والكفاءات أو المساعدة في تطويرها.
T2017	إعداد ما يخص التعلم والتطوير الفردي أو الجماعي، وخطط علاج فجوات المهارات أو المعارف، أو المساعدة في إعدادها.
T2018	تطوير غايات التعلُّم وأهدافه أو المساعدة في تطويرها.
T2019	تطوير مواد أو برامج التدريب على رأس العمل، أو المساعدة في تطويرها.
T2020	تطوير الاختبارات التحريرية لقياس وتقييم كفاءة المتعلم، أو المساعدة في تطويرها.
T2021	تقييم فاعلية وكفاءة التعليم بناء على مؤشرات أداء مختلفة.

رمز المهمة	وصف المهمة
T2022	إجراء تقييمات احتياجات التعلّم وتحديد المتطلبات.
T2023	العمل مع الخبراء المتخصصين، لضمان أن معايير التأهيل تعكس متطلبات المنظمة الوظيفية ومعايير القطاع.
T2024	تطوير التدريبات التعليمية التفاعلية وبيئة تعليمية فعّالة.
T2025	تطوير وتنفيذ الأوصاف الموحدة للأدوار الوظيفية استنادًا إلى الأدوار المحددة لكوادر الأمن السيبراني.
T2026	تطوير ومراجعة إجراءات الاستقطاب والتوظيف ومنع التسرب، وفقًا لسياسات الموارد البشرية الحالية.
T2027	تطوير أو تنفيذ هيكل التصنيف لمهن الأمن السيبراني لتضم متطلبات دخول المجال الوظيفي وتعريف المصطلحات كالرموز والمعرّفات.
T2028	تطوير سياسات وبروتوكولات التدريب للأمن السيبراني أو المساعدة في تطويرها.
T2029	تطوير الأهداف والغايات لمناهج المنظمة التدريبية للأمن السيبراني.
T2030	ضمان إدارة المسارات الوظيفية للأمن السيبراني وفقًا لسياسات الموارد البشرية بالمنظمة وتوجيهاتها.
T2031	إنشاء وجمع مقاييس لمراقبة سعات كوادر الأمن السيبراني وقدراتها وجاهزيتها، والتحقق من مصداقيتها.
T2032	إنشاء متطلبات دخول المجال الوظائف السيبرانية ومؤهلاته وإجراءاته، والإشراف عليها.
T2033	إنشاء مسارات مهنية للأمن السيبراني للسماح بالتدرج الوظيفي والتطوير والنمو داخل مجالات الوظائف السيبرانية وفيما بينها.
T2034	وضع متطلبات البيانات الداعمة لإدارة كوادر الأمن السيبراني ومتطلبات تقديم التقارير.
T2035	إنشاء برامج إدارة كوادر الأمن السيبراني وفقًا لمتطلبات المنظمة، وتأمين الموارد لتلك البرامج وتنفيذها وتقييمها.
T2036	تقييم الاستراتيجية التعليمية وخياراتها التنفيذية بالتعاون مع المعلمين والمدربين لتطوير خطط التعلم وجعلها أكثر فعالية للمنظمة.
T2037	مراجعة وتطبيق معايير مؤهلات المجال المهني السيبراني.
T2038	مراجعة وتطبيق سياسات المنظمة ذات الصلة بكوادر الأمن السيبراني أو المؤثرة عليها.
T2039	دعم دمج كوادر الأمن السيبراني المؤهلة في عمليات تطوير دورة حياة نُظم المعلومات.

رمز المهمة	وصف المهمة
T2040	ربط التدريب والتعليم بمتطلبات الأعمال أو الرسالة.
T2041	إعداد الدورات التدريبية المناسبة على حسب خصوصية احتياجات المتلقين والبيئة المادية أو الافتراضية.
T2042	تقديم الدورات التدريبية المناسبة على حسب خصوصية احتياجات المتلقين والبيئة المادية أو الافتراضية.
T2043	تطبيق المفاهيم والإجراءات والبرمجيات والأدوات وتطبيقات التقنية على الطلاب.
T2044	تصميم مناهج التدريب ومحتوى الدورات، حسب متطلبات المنظمة والقوى العاملة.
T2045	المشاركة في تطوير مناهج التدريب ومحتوى الدورات.
T2046	ضمان تلبية التدريب لأهداف وغايات التدريب أو التعليم أو التوعية بالأمن السيبراني.
T2047	تحديد ومعالجة المشاكل ذات الصلة بالإدارة والتخطيط لكوادر الأمن السيبراني ويشمل ذلك التعيين ومنع التسرب والتدريب.
T2048	تخطيط وتنسيق أساليب وأنماط تنفيذ التعليم لتأمين بيئة التعلم الأكثر فاعلية.
T2049	التخطيط لأساليب وأنماط التعليم خارج القاعة الدراسية.
T2050	إجراء المراجعات الدورية لمحتوى الدورات فيما يخص دقتها واكتمالها ومواءمتها وحداثتها.
T2051	التوصية بشأن التحديثات على المنهج الدراسي ومحتوى الدورة، استنادًا إلى الملاحظات من جلسات تدريب سابقة.
T2052	أداء مهام الاستشاري والمرشد الداخلي في مجال اختصاصه.
T2053	مراجعة واعتماد سياسات اختيار وإدارة موفر التدريب.
T2054	تطوير مواد التدريب لتعزيز فهم القوى العاملة لسياسات الأمن السيبراني وحماية البيانات والخصوصية بالمنظمة شاملا الالتزامات القانونية، أو المساعدة في تطويرها.
T2500	تطوير منهجيات فعالة لمراقبة وقياس المخاطر، ومدى الالتزام، وجهود توكيد الالتزام.
T2501	تطوير المواصفات لضمان أن جهود معالجة المخاطر والالتزام والضمان تلتزم بمتطلبات الأمن السيبراني.
T2502	الحفاظ المتواصل على المعرفة بالسياسات والتنظيمات ووثائق الالتزام المعمول بها في الأمن السيبراني الدفاعي حسب ما يختص منها بأعمال التدقيق للأمن السيبراني الدفاعي.
T2503	إدارة حزم الاعتماد والموافقة عليها.

رمز المهمة	وصف المهمة
T2504	مراقبة وتقييم مدى التزام النظام بمتطلبات الأمن السيبراني، ومتطلبات الصمود والاعتمادية.
T2505	تخطيط وتنفيذ أعمال المراجعة وتطوير قضايا التصريح الأمني للتثبيت الأولي للنظم والشبكات.
T2506	توفير تقييم تقني صحيح لتطبيقات البرامج أو الأنظمة أو الشبكات، وتوثيق مدى التزامها بمتطلبات الأمن السيبراني المتفق عليها.
T2507	مراجعة سجلات المخاطر والوثائق المشابهة للتأكد من أن مستوى المخاطر لكل تطبيق ونظام وشبكة يقع ضمن الحدود المقبولة.
T2508	إجراء أعمال التدقيق للحالة الأمنية للبرامج والشبكة والنظام حسب ما ورد في سياسات الأمن السيبراني، وتقديم توصيات بالأنشطة المطلوبة لعلاج الثغرات المكتشفة.
T2509	تطوير عمليات الالتزام الأمني وعمليات تدقيق للخدمات المقدمة من أطراف خارجية.
T2510	المراجعة الدورية لضمان مواءمة سياسات الأمن السيبراني والوثائق ذات العلاقة مع غايات واستراتيجيات المنظمة المعلنة.
T2511	تحديد وتوثيق أثر تنفيذ نظام جديد أو واجهات اتصال جديدة بين النُظم على الوضع الأمني للبيئة الحالية.
T2512	ضمان توثيق التصميم والتطوير لأنشطة الأمن السيبراني على نحو ملائم.
T2513	تحديد مخاطر سلسلة الإمداد وتوثيقها لعناصر الأنظمة الحرجة حيثما وجدت.
T2514	دعم أنشطة الالتزام حسب الحاجة.
T2515	ضمان أن عمليات التدقيق للأمن السيبراني تختبر جميع الجوانب ذات العلاقة بالبنية التحتية للمنظمة والالتزام بالسياسات.
T2516	ضمان أن إعدادات التطبيقات والشبكات والنُظم تلتزم بسياسات المنظمة للأمن السيبراني.
T2517	التحقق من حزم الاعتماد.
T2518	الحفاظ المتواصل على المعرفة بالقوانين المعمول بها والتنظيمات ومعايير الاعتماد، والمراجعة الدورية لها لضمان التزام المنظمة.
T2519	التعاون مع المؤسسات التنظيمية المعنية والكيانات القانونية الأخرى فيما يخص التحقيقات وعمليات مراجعة الالتزام.
T2520	تطوير العمليات مع المدققين الخارجيين حول كيفية مشاركة المعلومات بأمان.
T3000	تقييم فاعلية السياسات أو المعايير أو الإجراءات في تحقيق استراتيجية المنظمة.
T3001	تفسير وتطبيق القوانين والأنظمة والسياسات أو الإجراءات حسب الحاجة.

رمز المهمة	وصف المهمة
T3002	حل التعارضات بين السياسات أو المعايير أو الإجراءات عند خلافها مع القوانين والتنظيمات المعمول بها.
T3003	اكتساب المعرفة العملية بالمشاكل الدستورية التي تنشأ في القوانين والأنظمة والسياسات والاتفاقيات والمعايير والإجراءات، والحفاظ عليها على الدوام.
T3004	توفير الخبرات بالأمن السيبراني عند تأطير المرافعات طلبا لتحديد أيّ انتهاكات مزعومة للقوانين أو الأنظمة أو السياسات أو الإرشادات.
T3005	تطوير الإرشادات الخاصة بتنفيذ ضوابط الأمن السيبراني ذات العلاقة.
T3006	توفير إرشادات في الأمن السيبراني للمشرفين وموظفي متابعة الالتزام فيما يخص الالتزام بسياسات الأمن السيبراني والمتطلبات القانونية والتنظيمية ذات الصلة.
T3007	تقييم أثر التغييرات في القوانين والأنظمة على سياسات الأمن السيبراني بالمنظمة والوثائق ذات العلاقة.
T3008	توفير إرشادات من منظور الأمن السيبراني بشأن القوانين والأنظمة والسياسات والمعايير أو الإجراءات لصالح الإدارة أو العاملين أو العملاء.
T3009	المساعدة في تنفيذ القوانين أو الأنظمة أو الأوامر التنفيذية وما شابهها – سواء كانت جديدة أم محدثة - حسب علاقتها بسياسات الأمن السيبراني والوثائق الأخرى.
T3010	توفير الإرشاد من منظور الأمن السيبراني فيما يخص إعداد الوثائق القانونية والوثائق الأخرى ذات الصلة.
T3011	العمل مع المستشارين القانونيين بالمنظمة والأطراف الأخرى ذات العلاقة لضمان التزام كافة الخدمات مع متطلبات الخصوصية وأمن البيانات.
T3012	العمل مع المستشارين القانونيين والإداريين وأصحاب المصلحة بالمنظمة لضمان توفر توثيق ملائم للخصوصية والسرية بالمنظمة والمحافظة عليه.
T3013	العمل مع أصحاب المصلحة لتطوير العلاقات مع الجهات التنظيمية والإدارات الحكومية المعنية بقضايا الخصوصية وأمن البيانات.
T3014	ضمان تسجيل كافة مصادر البيانات ومصادر معالجتها لدى سلطات حماية خصوصية البيانات حسب اللزوم.
T3015	العمل مع فرق الأعمال والإدارة العليا لضمان التوعية بـأفضل الممارسات في مجال خصوصية المعلومات وأمن البيانات.
T3016	العمل مع الإدارة العليا بالمنظمة لتأسيس لجنة مراقبة لخصوصية البيانات.
T3017	توفير القيادة في اللجنة المسؤولة عن مراقبة خصوصية البيانات.
T3018	تطوير وتوثيق إجراءات بلاغات الإفصاح الذاتي عن أية أدلة على انتهاكات الخصوصية.
T3019	العمل كحلقة اتصال لخصوصية المعلومات لمستخدمي الأنظمة التقنية، والإبلاغ عن الخروقات للإدارة العليا.

رمز المهمة	وصف المهمة
T3020	تطوير مواد التدريب والاتصالات الأخرى لزيادة فهم الموظفين لسياسات الخصوصية بالشركة وممارسات معالجة البيانات والالتزامات القانونية.
T3021	الإشراف على التدريب والتعريف الأولي في مجال الخصوصية، وتوجيهه وضمان تقديمه لكل من الموظفين والمتطوعين والمقاولين والحلفاء وشركاء العمل وأيّ أطراف أخرى ذات صلة.
T3022	ضمان تقديم التدريب والتوعية بالخصوصية بصفة دورية.
T3023	العمل مع الشؤون الخارجية لتطوير العلاقات مع منظمات المستهلكين وغيرها من المنظمات غير الحكومية المهتمة بقضايا الخصوصية وأمن البيانات.
T3024	العمل مع إدارة المنظمة والمستشارين القانونيين والأطراف الأخرى ذات الصلة لتمثيل مصالح خصوصية المعلومات للمنظمة أمام الأطراف الخارجية.
T3025	تقديم التقارير الدورية عن الوضع الراهن لبرنامج الخصوصية لصالح الإدارة العليا أو المسؤولين أو اللجان الآخرين.
T3026	توفير القيادة لبرنامج الخصوصية بالمنظمة.
T3027	توجيه مسؤولي الخصوصية والإشراف على أعمالهم، وتنسيق برامج الخصوصية وأمن البيانات مع الإدارة العليا لضمان التناسق عبر المنظمة.
T3028	ضمان الالتزام بممارسات الخصوصية عبر المنظمة.
T3029	العمل مع فرق الموارد البشرية والقانونية لتطوير عقوبات مناسبة لعدم الالتزام بسياسات وإجراءات الخصوصية للمنظمة.
T3030	حلّ مزاعم عدم الالتزام بسياسات الخصوصية للمنظمة، أو ممارسات إبلاغ المعلومات، دون تأخر.
T3031	تطوير وحفظ إطار خصوصية لإدارة المخاطر وضمان الالتزام.
T3032	مراجعة مشاريع البيانات والخصوصية بالمنظمة وضمان التزامها بسياسات الخصوصية وأمن البيانات بالمنظمة.
T3033	إنشاء عملية لإدارة جميع جوانب الشكاوى المتعلقة بسياسات وإجراءات الخصوصية في المنظمة.
T3034	توفير القيادة في أعمال التخطيط والتصميم والتقييم للمشاريع ذات الصلة بالخصوصية والأمن السيبراني.
T3035	إنشاء ومتابعة برنامج تدقيق داخلي للخصوصية.
T3036	المراجعة الدورية لبرنامج الخصوصية وتحديثه ليشمل التغييرات في القوانين أو الأنظمة أو سياسة المنظمة.
T3037	تقديم إرشادات التطوير والمساعدة في ما يخص سياسات وإجراءات خصوصية المعلومات بالمنظمة.

رمز المهمة	وصف المهمة
T3038	ضمان أن استخدام التقنيات يحافظ على سُبل حماية الخصوصية، سواء عند الاستخدام أو الجمع أو الإفصاح عن المعلومات الشخصية، ولا يؤدي إلى تعريتها.
T3039	مراقبة تطوير النُظم وعملياتها لضمان التزامها بسياسات الخصوصية والأمن.
T3040	إجراء تقييمات للآثار المترتبة على الخصوصية جراء قواعد جديدة مقترحة في حق خصوصية المعلومات الشخصية .
T3041	مراجعة كافة خطط الأمن السيبراني لضمان المواءمة بين الأمن السيبراني وممارسات الخصوصية.
T3042	تطوير وإدارة إجراءات التمحيص وتدقيق الموردين للالتزام بالمتطلبات المناسبة في مجالات الخصوصية وأمن البيانات والمتطلبات القانونية والتنظيمية.
T3043	التأكد من أن كافة الشكاوى ذات العلاقة بسياسة الخصوصية للمنظمة والوثائق ذات العلاقة تتم معالجتها دون تأخر من خلال المورد المناسب.
T3044	تحديد وعلاج الفجوات في التزام المنظمة بمتطلبات الخصوصية.
T3045	التنسيق مع رئيس إدارة الأمن السيبراني أو من يقوم بعمله لضمان المواءمة بين ممارسات الأمن السيبراني وممارسات الخصوصية.
T3046	إعداد الاتصالات والتدريبات المناسبة لتحفيز وتعليم كافة الموظفين، بما فيهم القيادات العليا، فيما يخص الالتزام بالخصوصية وعواقب عدم الالتزام، والمداومة على ذلك.
T3047	ضمان أداء أنشطة مراقبة الالتزام بالخصوصية بصفة مستمرة.
T3048	ضمان تسخير التقنيات الملائمة لاستمرار التزام المنظمة بمتطلبات الخصوصية.
T3049	تطوير خطط استراتيجية مع الإدارة العليا لضمان معالجة المعلومات الشخصية وفقًا لمتطلبات الخصوصية المعمول بها.
T3050	تطوير إجراءات على مستوى المنظمة ومتابعتها لضمان تطوير المنتجات والخدمات الجديدة بما يتسق مع سياسات الخصوصية بالمنظمة والتزاماتها القانونية.
T3051	العمل مع رئيس إدارة الأمن السيبراني والمستشار القانوني والإدارة العليا لإدارة حوادث وانتهاكات الخصوصية وفقًا للمتطلبات القانونية والتنظيمية.
T3052	المحافظة على التوعية بقوانين الخصوصية وأنظمتها ومعايير الاعتماد المعمول بها.
T3053	إدارة مشاركة الشركة بالأحداث العامة ذات العلاقة بالخصوصية وأمن البيانات.
T3500	تطوير أدوات الدفاع السيبراني.
T3501	وصف وتحليل حركة المرور على الشبكة، لتحديد الأنشطة الشاذة والتهديدات المحتملة لموارد الشبكات.

رمز المهمة	وصف المهمة
T3502	الإدارة والإشراف على أعمال تحديث القواعد والتواقيع لتطبيقات الدفاع السيبراني.
T3503	التنسيق مع بقية طاقم عمل الدفاع السيبراني للتحقق من مصداقية التنبيهات الشبكية.
T3504	تقديم تقارير مُجملة يومية لأحداث الشبكات والأنشطة الأخرى ذات الصلة بالأمن السيبراني بما يتلاءم مع سياسات ومتطلبات المنظمة.
T3505	إعداد وتهيئة برامج وأجهزة الدفاع السيبراني المخصصة، وتثبيتها وتحديثها واختبارها.
T3506	المساعدة في تقييم أثر بناء وتشغيل بنية تحتية مخصصة للدفاع السيبراني.
T3507	إدارة منصات الاختبار، واختبار وتقييم التطبيقات وأجهزة البنية التحتية والقواعد والتوقيعات، وضوابط التحكم بالوصول وإعدادات المنصات التي يديرها مزودو الخدمات.
T3508	إنشاء قوائم التحكم بالوصول إلى الشبكات المخزنة بداخل نُظم الدفاع السيبراني المخصصة، وتعديلها وإدارتها.
T3509	تحديد التعارضات المحتملة جراء تنفيذ أي من أدوات الدفاع السيبراني، والإبلاغ عنها.
T3510	تنفيذ متطلبات إطار إدارة المخاطر والتقييم الأمني والتصريح لنُظم الدفاع السيبراني المخصصة داخل المنظمة، وتوثيق سجلاتها وحفظها.
T3511	انتقاء ضوابط الأمن السيبراني للنظام وتوثيق الوصف الوظيفي لتنفيذ الضوابط في الخطة الأمنية.
T3512	تنفيذ ضوابط الأمن السيبراني الواردة في الخطة الأمنية أو وثائق النُظم الأخرى.
T4000	تطبيق مبادئ المعمارية الأمنية الموجهة للخدمات لاستيفاء متطلبات المنظمة الخاصة بالسرية والسلامة والتوافر.
T4001	ضمان توثيق جميع عمليات أمن النُظم وأنشطة الصيانة على نحو ملائم، وتحديثها حسب الضرورة.
T4002	تطبيق التحديثات وحزم التحديثات الأمنية للمنتجات التجارية بما يتوافق مع الأطر الزمنية التي تمليها السلطة الإدارية فيما يخص بيئة التشغيل المعنية.
T4003	تنفيذ تدابير أمن سيبراني مضادة محددة للنظم والتطبيقات.
T4004	دمج القدرات المؤتمة المخصصة لتحديث أو عمل تحديثات إصلاح برمجيات النظام، حيثما أمكن ذلك عمليا.
T4005	ضمان اختبار الأمن السيبراني للتطبيقات والنظم بعد تطويرها.
T4006	توثيق وتحديث جميع الأنشطة المتعلقة بتنفيذ وتشغيل وصيانة أمن الأنظمة.
T4007	تقديم إرشادات بشأن الأمن السيبراني إلى القيادة.

رمز المهمة	وصف المهمة
T4008	الكشف عن البيانات المشفرة والمخفية وتحليلها.
T4009	تطوير واختبار إجراءات نقل عمليات النظام إلى موقع بديل.
T4010	تنفيذ إجراءات التعافي من الكوارث واستمرارية الأعمال.
T4011	تنفيذ تدابير أمنية على النظام أو مكونات النظام لمعالجة الثغرات وتقليل المخاطر، والتوصية بعمل تغييرات تتعلق بالأمن السيبراني.
T4012	تنفيذ التدابير والضوابط الأمنية للنظام وفقًا للإجراءات المعمول بها.
T4013	ضمان دمج وتنفيذ الحلول العابرة للنطاقات في بيئة آمنة.
T4014	رفع التوصيات للإدارة بعمل الإجراءات اللازمة للمعالجة والتصحيح أو بقبول المخاطر الناتجة عن جوانب القصور الأمني التي يتم اكتشافها عند الفحص.
T4015	التحقق من وجود الحد الأدنى من المتطلبات الأمنية لجميع التطبيقات.
T4016	العمل مع الفرق الأخرى لتصميم وتطوير وتأمين حلول لإدارة الهوية والوصول.
T4017	العمل مع معماري الأمن السيبراني لتطوير استراتيجية إدارة الهوية والوصول.
T4018	ضمان اتباع معايير وسياسات المنظمة عند تنفيذ حلول إدارة الهوية والوصول.
T4019	العمل مع أصحاب المصلحة لتحديد ومعالجة الثغرات عند تنفيذ حلول إدارة الهوية والوصول.
T4020	تقديم التوجيه والنصيحة إلى أعضاء الفريق بشأن نُظم إدارة الهوية والوصول وعملياتها.
T4021	تطوير خوارزميات التشفير وتصميمها وتنفيذها لتفي بمتطلبات المنظمة.
T4022	تحليل خوارزميات التشفير للكشف عن نقاط ضعفها وكسر الشفرات.
T4023	تطوير العمليات والإجراءات الخاصة بالتحديث وعمل تحديث الإصلاح اليدوي لبرمجيات النُظم بحسب متطلبات الجدول الزمني الحالي أو المتوقع لتطبيق حزم تحديثات الإصلاح على البيئة التشغيلية للنظام.
T4024	إعداد سياسات المجموعات وقوائم التحكم في الوصول لضمان التوافق مع المعايير التنظيمية وقواعد العمل والاحتياجات.
T4025	إدارة الحسابات وصلاحيات الشبكة والوصول إلى الأنظمة والمعدات.

رمز المهمة	وصف المهمة
T4026	تصميم وتطوير وظائف إدارة النظم والإشراف عليها للمستخدمين ذوي الصلاحيات الإضافية.
T4027	الإشراف على الحسابات وصلاحيات الشبكة والوصول إلى الأنظمة والمعدات.
T4028	إعداد عمليات وإجراءات التحكم في الوصول لأدوات وتقنيات المراقبة المستمرة.
T4029	ضمان أن تتم إدارة الوصول لأدوات وتقنيات المراقبة المستمرة بشكل مناسب.
T4500	إجراء أو دعم اختبارات الاختراق المصرحة للبنية التحتية والأصول.
T4501	إجراء المراجعات المطلوبة شاملة مراجعات التدابير الدفاعية حسب سياسات المنظمة.
T4502	تقديم التوصيات بخصوص الضوابط الأمنية ذات الكفاءة المالية لمعالجة المخاطر المكتشفة عن طريق الاختبار والمراجعة.
T4503	جمع المعلومات عن معمارية واستخدامات الشبكات من خلال التحليل التقني والبحث في المصادر المفتوحة وتوثيق النتائج.
T4504	محاكاة أساليب الهندسة الاجتماعية الضارة التي يستخدمها المعتدي في محاولته لخرق النظام للكشف عن الثغرات الأمنية ونقاط الضعف.
T4505	تحديد المنهجيات التي قد يستخدمها المعتدون لاستغلال نقاط الضعف في النُظم والشبكات.
T4506	أخذ الأعمال في الاعتبار وتضمينها في توصيات واستراتيجيات الأمن السيبراني.
T4507	مسح الثغرات على الأنظمة والأصول.
T4508	إعداد تقارير نتائج اختبارات الاختراق والتقييم لنقاط الضعف شاملا مستوى الخطر، واقتراحات المعالجة، وكافة التفاصيل التقنية اللازمة لإعادة توليد نتائج الاختبار.
T4509	مناقشة النتائج الأمنية مع الإدارة والقيادة وفرق تقنية المعلومات.
T4510	تصميم وتطوير عمليات اختبارات الاختراق.
T4511	إجراء اختبار عن بُعد للشبكة للكشف عن نقاط الضعف الأمنية.
T4512	تخطيط وإنشاء منهجيات وبرمجيات واختبارات الاختراق.
T4513	تصميم نماذج محاكاة للهجمات لتوضح الأثر على أعمال المنظمة والمستخدمين.
T4514	عرض نتائج الاختبارات والمخاطر والاستنتاجات على المتلقين التقنيين وغير التقنيين.

رمز المهمة	وصف المهمة
T4515	توضيح التبعات على الأعمال بسبب نقاط الضعف المكتشفة من خلال الاختبارات لإبراز أهمية معالجتها.
T4516	إجراء التقييمات الأمنية المادية للخوادم والنُظم وأجهزة الشبكات.
T4517	فحص الثغرات في التطبيقات على الشبكة العنكبوتية وتطبيقات العميل والتطبيقات النمطية.
T4518	استخدام الاختبارات الأمنية وأدوات مسح الشفرات لمراجعة الشفرات.
T5000	تحليل ملفات السجل والأدلة والمعلومات الأخرى لتحديد أفضل المنهجيات لمعرفة هوية المتسلل للشبكة.
T5001	عقد مقابلات مع الضحايا المحتملين للجريمة السيبرانية ومع الشهود.
T5002	تأكيد ما هو معلوم عن عملية التسلل والسعي لاكتشاف معلومات جديدة.
T5003	تقديم الدعم التقني من الخبراء لحل حوادث الدفاع السيبراني.
T5004	إنشاء نسخة مطابقة وسليمة من جانب الأدلة الشرعية بهدف استخدامها في عمليات استعادة البيانات وتحليلها، تمشيا مع السياسات المعنية سواء المؤسسية منها أو الوطنية حسب الساري.
T5005	تطوير خطة للتحقيق في الجريمة السيبرانية المزعومة أو المخالفة أو النشاط المشتبه به.
T5006	تقديم ملخص تقني للنتائج وفقًا لإجراءات الإبلاغ القائمة.
T5007	ضمان تتبع تسلسل العُهَد لجميع الوسائط الرقمية المستحوذ عليها وفقًا للقوانين الوطنية أو سياسات المنظمة المعمول بها.
T5008	دمج نتائج التحليل للشبكات وللبنية التحتية وللأدلة الرقمية مع النتائج من التحقيقات والعمليات الجنائية الأخرى.
T5009	تحديد ما إذا كان الحادث الأمني يُعد مخالفاً للقانون وبالتالي يتطلب اتخاذ إجراء قانوني محدد.
T5010	تحديد الأدلة الرقمية للفحص والتحليل.
T5011	تحديد الأدلة التي يمكن أن تثبت وقوع جريمة سيبرانية.
T5012	تحديد الأدلة النصية أو المادية المرتبطة بحوادث التسلل السيبرانية والتحقيقات والعمليات، وجمعها والاستحواذ عليها.
T5013	إجراء تحليل ديناميكي لتحميل "صورة" (نسخة طبق الأصل من البيانات) لمحرك الأقراص - سواء مع أو بدون وجود محرك الأقراص الأصلي- لرؤية التسلل كما قد يراه المستخدم في بيئة أصلية.
T5014	إجراء مقارنة البعثرة على قواعد البيانات حسب متطلبات سياسات المنظمة.

رمز المهمة	وصف المهمة
T5015	إجراء تحليل للوسائط غير القابلة للتغيير.
T5016	إجراء تحليل للبرمجيات الضارة على الرُتبة الأولى والثانية والثالثة.
T5017	ضمان سلامة البيانات عند إعداد الوسائط الرقمية للنسخ.
T5018	إدارة مسرح الجريمة.
T5019	تقديم مساعدة تقنية خلال عمليات جمع وحفظ ومعالجة أو تحليل الأدلة الرقمية.
T5020	التعرف على الوحدات الجنائية الأولية والإبلاغ عنها بما يتماشى مع سياسات الإبلاغ.
T5021	تأمين الأجهزة الإلكترونية ومصادر المعلومات المطلوبة للتحليل.
T5022	استخلاص البيانات من الأجهزة.
T5023	استخدام معدات وأساليب مخصصة للقيام بمهام التحقيق الجنائي الرقمي بما يتماشى مع السياسات.
T5024	إجراء تحليل سريع على مستوى الشفرات الثنائية.
T5025	أداء دور الخبير التقني لدعم السلطات القانونية التنفيذية وشرح تفاصيل حادث الأمن السيبراني والتحليل الجنائي، حسب المطلوب.
T5026	فحص الفيروسات على الوسائط الرقمية.
T5027	إجراء تحليل جنائي لأنظمة إدارة الملفات.
T5028	إجراء تحليل ثابت لتحميل "صورة" (نسخة طبق الأصل من البيانات) لقرص مع وجود القرص الأصلي أو بدونه.
T5029	إجراء تحليل ثابت للبرمجيات الضارة.
T5030	استخدام مجموعة الأدوات الجنائية القابلة للتطبيق الميداني لدعم العمليات.
T5031	التنسيق مع محللي معلومات التهديدات السيبرانية بهدف ربط بيانات تقييم التهديدات.
T5032	أخذ التدابير اللازمة لمعالجة أثر المخاطر المحتملة جراء الحادث، سواء على الأشخاص أو الأصول أو الموارد.
T5033	تقييم الأفعال والتصرفات ذات العلاقة بعمليات التحري مع الضحايا والشهود أو المشتبه بهم، ورفع تقارير بذلك.

رمز المهمة	وصف المهمة
T5034	تحديد نطاق تغطية التهديدات، والمخاطر الناجمة، وتقديم توصية بالأفعال أو التدابير المضادة لمعالجتها.
T5035	تقديم الدعم بخصوص التحقيقات الجنائية للسلطات القانونية خلال مجريات العملية القضائية.
T5036	معالجة نسخة البيانات بأدوات تناسب غايات التحقيق.
T5037	إجراء تحليل لسجل ويندوز المركزي.
T5038	مراقبة الملفات والسجل المركزي على نظام التشغيل الحي، بعد تحديد التسلل.
T5039	إدخال معلومات الوسائط الرقمية التي تمت حيازتها إلى قاعدة بيانات التتبع.
T5040	الإبلاغ عن الحوادث السيبرانية لإفادة الدفاع السيبراني.
T5041	بناء أدوات للحوادث السيبرانية القابلة للتطبيق الميداني.
T5042	تحليل المواد المتعلقة بحوادث الأمن السيبراني للحصول على أدلة على وجود طرف أجنبي عدائي أو نشاط إجرامي.
T5043	جمع وحفظ الأدلة التي يمكن استخدامها في مقاضاة مقترفي الجرائم السيبرانية.
T5044	استخدام نتائج تحليل آثار التسلل لإفادة التوصيات بشأن معالجة حوادث الدفاع السيبراني المحتملة.
T5045	تحليل ملفات السجلات، والأدلة، والمعلومات الأخرى لتحديد أفضل الأساليب للتعرف على مرتكبي عملية التسلل الشبكي أو الجرائم السيبرانية الأخرى.
T5046	تحديد وتطوير دلائل ومصادر معلومات للمساعدة في تحديد الأطراف المسؤولة عن الجرائم السيبرانية أو مقاضاتهم.
T5047	توثيق الحالة الأصلية للأدلة الرقمية والأدلة ذات الصلة بما يتوافق مع السياسات الوطنية وسياسات المنظمة.
T5048	تحليل نُظم تقنية المعلومات والوسائط الرقمية لحل الجرائم السيبرانية والتحقيق فيها، وللمقاضاة.
T5049	توثيق مجريات التحقيق وفقًا للمعايير والمتطلبات القانونية.
T5050	مراجعة النسخ طبق الأصل من البيانات الجنائية والبيانات العُرضة للتغيير وغيرها من مصادر البيانات لاستعادة المعلومات التي يُحتمل أن تكون ذات صلة.
T5051	تحرير ونشر التوصيات والتقارير عن مكتشفات الحوادث لصالح المجموعات المعنية.
T5052	مراجعة المعلومات المجموعة لتحديد مدى مصداقيتها وعلاقتها بالتحقيق بما يتوافق مع سياسات المنظمة.

رمز المهمة	وصف المهمة
T5053	إعادة بناء الشبكات بصيغ المخططات والتقارير.
T5054	تحديد وانتقاء موارد المعلومات الأكثر فاعلية للمساعدة في التحقيق في حادث الأمن السيبراني.
T5055	تنقيح التقارير لحماية بيانات أو منهجيات الممتلكات الخاصة، أو التجارية، أو الشخصية، أو غيرها من البيانات أو المنهجيات السرية أو الحساسة.
T5056	تتبع حالة طلبات المعلومات، بما يتوافق مع سياسات المنظمة.
T5057	توثيق الدروس المستفادة من مخرجات الأحداث والتمارين.
T5058	تحديد أيّ نشاط خبيث محتمَل من خلال تفريغ الذاكرة، أو السجلات، أو الحِزم الملتقطة.
T5059	فحص البيانات المستردة بحثًا عن معلومات ذات الصلة بالمشكلة محل النظر.
T5060	ابتكار أساليب وحلول إبداعية مخصصة للاستغلال لاكتشاف الثغرات ومدى عُرضة الأهداف لأعمال الاستغلال.
T5061	عقد المقابلات مع المشتبه بارتكابهم جرائم سيبرانية.
T5062	تحديد التسلل من خلال إجراء تحليل ديناميكي.
T5500	استخدام المراجعات للتوصية بتدابير جديدة أو محدثة لجوانب الأمن أو الصمود والموثوقية.
T5501	تحليل نتائج اختبارات البرمجيات والعتاد والاختبار البيني لتحديد تحسينات ذات كفاءة عالية للحد من المخاطر المكتشفة.
T5502	الإجابة عن طلبات المعلومات بما يتوافق مع سياسات المنظمة.
T5503	استخدام المعرفة بممثلي التهديد وبالأنشطة لبناء فهم مشترك عن حالة المخاطر الحالية للمنظمة.
T5504	استخدام المعرفة بممثلي التهديد وبالأنشطة لإفادة المنظمة في الاستجابة لحادث سيبراني.
T5505	تنسيق مصادر المعلومات الإستباقية لتهديدات الأمن السيبراني ونقاط التغذية، والتحقق من مصداقيتها وإدارتها.
T5506	تحديد الثغرات في المعلومات الإستباقية للتهديدات وتقييم آثارها على المنظمة.
T5507	إعداد وتقديم ملخصات عن تهديدات معينة للمنظمة.
T5508	التعاون ومشاركة المعلومات مع محللي معلومات التهديدات الذين يعملون في المجالات ذات الصلة.

رمز المهمة	وصف المهمة
T5509	استطلاع الشبكات وتحليل الثغرات للنُظم داخل الشبكة.
T5510	إجراء التحليل العقدي الشبكة.
T5511	الكشف عن حالات الاستغلال ضد الشبكات والمضيفات ذات الاهتمام لإفادة جهود محاولة فهم نشاط ممثل التهديد.
T5512	تحديد التقنيات المستخدمة من قبل ممثلي التهديد محل الاهتمام.
T5513	تطوير مصادر المعلومات لتعميق فهم ممثلي التهديد محل الاهتمام.
T5514	تطبيق الأساليب التحليلية للحصول على معلومات ممثلي التهديد محل الاهتمام.
T5515	تقييم عمليات صنع القرار بشأن التهديدات.
T5516	تحديد سلوكيات التهديد والثغرات.
T5517	تحديد التهديدات الأساسية للثغرات المعروفة بالمنظمة.
T5518	تقييم القدرات المتوفرة للتصدي لأنشطة التهديدات المحتملة وذلك لتقديم توصية بحلول فعّالة.
T5519	تحديد أساليب التهديد ومنهجياته.
T5520	تحديد وتقييم القدرات الحرجة للتهديدات، ومتطلباتها وثغراتها.
T5521	تحديد هيكلة ومكونات ممثل التهديد.
T5522	تحديد فجوات المعلومات الإستباقية وجوانب قصورها.
T5523	تقديم المدخلات أو تطوير مسارات العمل بناء على فهم التهديد.
T5524	المراقبة والإبلاغ عن التغيرات في ميول التهديدات وأنشطتها وأساليبها وقدراتها وغاياتها.
T5525	مراقبة أنشطة التهديد التي تمت مصادقتها والإبلاغ عنها.
T5526	مراقبة المواقع مفتوحة المصدر للمحتوى العدائي الموجه ضد مصالح المنظمة أو شركائها.
T5527	مراقبة أنشطة الجهات التي تمثل مصدر للتهديدات والإبلاغ عنها، لتحقيق متطلبات المنظمة المتعلقة بالمعلومات الإستباقية للتهديدات والبلاغات.

رمز المهمة	وصف المهمة
T5528	تسخير الخبرة حيال ممثلي التهديد لدعم أنشطة التخطيط والتطوير لاستراتيجية وموارد الأمن السيبراني للمنظمة.
T5529	توفير المعلومات والتقييمات عن ممثلي التهديد لدعم أصحاب المصلحة في تخطيط وتنفيذ أنشطة الأمن السيبراني.
T5530	تقديم التحليل والدعم الحي في مجال المعلومات الإستباقية للتهديدات خلال تمارين وحوادث الأمن السيبراني.
T5531	مراقبة مصادر التغذية للمعلومات الإستباقية للتهديدات والإبلاغ عن الأحداث الشبكية الكبيرة وحالات التسلل.
T5532	معالجة الحوادث، وفرز الأحداث حسب أولوياتها، وتحليل الشبكات، وكشف التهديدات، وتحليل التوجهات، وتطوير المقاييس، ونشر المعلومات عن الثغرات.
T5533	المساندة في تحليل التهديدات والثغرات وتقديم الخدمات والتوصيات الاستشارية في الأمن السيبراني.
T5534	القيام بتحليل البرمجيات الضارة ذات الرُتبة الأولى والثانية.
T5535	المحافظة على تصور مشترك للمعلومات الإستباقية.
T5536	القيام بأبحاث وعمليات تحليل متعمقة.
T5537	تطوير متطلبات المعلومات اللازمة للاستجابة لطلبات المعلومات ذات الأولوية.
T5538	إنشاء طلبات للمعلومات.
T5539	إصدار معلومات إستباقية مدمجة وفي الوقت المناسب من كافة مصادر العمليات السيبرانية ومن دلائل وتحذيرات منتجات المعلومات الإستباقية (مثل تقييمات التهديدات، والإيجازات، ودراسات المعلومات الإستباقية، ودراسات الدول).
T5540	توفير دعم المعلومات الإستباقية الآني لأصحاب المصلحة الداخليين والخارجيين المهمين، حسب الملائم.
T5541	توفير التقييم والتغذية الراجعة اللازمة لتحسين إنتاج المعلومات الإستباقية و تقاريرها عمليات و متطلبات جمعها.
T5542	توفير إخطارات آنية بالمقاصد أو الأنشطة الوشيكة أو العدائية، أو الأنشطة التي قد تؤثر على غايات المنظمة أو مواردها أو قدراتها.
T5543	العمل الوثيق مع المخططين ومحللي معلومات التهديدات ومديري التجميع؛ لضمان دقة وحداثة متطلبات المعلومات الإستباقية وخطط تجميعها.
T5544	تحديد أساليب ومنهجيات التهديد السيبراني.
T5545	تحديد مصطلحات اللغات الأجنبية بداخل برامج الحاسب (مثل الملاحظات وأسماء المتغيرات).

رمز المهمة	وصف المهمة
T6000	تحديد وترتيب أولويات قدرات النُظم أو وظائف الأعمال اللازمة لاستعادة النظام جزئيًا أو كليًا بعد وقوع عطل كارثي في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
T6001	تطوير ودمج تصاميم الأمن السيبراني للنُظم والشبكات والتي لها متطلبات أمن متعددة المستويات في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
T6002	توثيق ومعالجة متطلبات الأمن السيبراني لعمليات النظم، ومتطلبات هندسة الأمن للبُنى المعمارية والنُظم في كافة مراحل عمليات الشراء والاستحواذ في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
T6003	ضمان اتساق النُظم والبُنى المعمارية التي تمت حيازتها أو تطويرها مع إرشادات المنظمة لمعمارية الأمن السيبراني في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
T6004	ترجمة القدرات المقترحة إلى متطلبات تقنية في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
T6005	تحليل التقنيات المادية والتقنيات الرقمية المنطقية في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية لتحديد السبل المحتملة للوصول إليها.
T6006	بحث توجهات تقنيات الاتصالات الناشئة لإفادة سياسات التصاميم والأمن بالمنظمة في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
T6007	انتقاء ضوابط الأمن السيبراني للنظام وتوثيق الوصف الوظيفي لتنفيذ الضوابط في الخطة الأمنية في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
T6008	تنفيذ ضوابط الأمن السيبراني الواردة في الخطة الأمنية أو وثائق النُظم الأخرى في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
T6009	العمل مع أعضاء فريق التطوير المرن لتسريع إعداد نماذج أولية ودراسات الجدوى وتقييم التقنيات الحديثة في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
T6010	تصميم نُظم وحلول لدعم نجاح "حلول إثبات المبدأ" والمشاريع التجريبية في مجالات التقنيات الناشئة في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
T6011	قراءة وتفسير المخططات والمواصفات والرسومات والتصاميم الأولية والرسومات البيانية التخطيطية ذات العلاقة بالأنظمة والشبكات في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
T6012	فهم وإصلاح مواطن الخلل في أنظمة الاتصالات والأتمتة الصناعية.
T6013	تحديد وتوثيق الضوابط الأمنية للأنظمة والشبكات في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
T6014	تنسيق وتقديم الدعم الاستشاري التقني إلى فريق الأمن السيبراني بالمنظمة لحل حوادث الأمن السيبراني في بيئة أنظمة التحكم الصناعي والتقنيات التشغيلية.
T6015	تنفيذ مهام التعامل الفوري مع حوادث الأمن السيبراني في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية لدعم فريق الاستجابة للحوادث.
T6016	عمل تحليل المخاطر في بيئات أنظمة التحكم الصناعي والتقنيات التشغيلية كلما حدث تغيير في تطبيق أو نظام.

(جدول ١٠): أوصاف المعارف

رمز المعرفة	وصف المعرفة
K0001	معرفة بمكونات الشبكة وبتشغيلها وبضوابط ومنهجيات أمن الشبكة المناسبة.
K0002	معرفة وفهم بتقييم المخاطر وبمنهجيات المعالجة والإدارة.
K0003	معرفة بجوانب الأمن السيبراني لمتطلبات القوانين والأنظمة فيما يتعلق بالأخلاق والخصوصية.
K0004	معرفة بمبادئ الأمن السيبراني والخصوصية.
K0005	معرفة بالتهديدات والثغرات ذات العلاقة بالأمن السيبراني.
K0006	معرفة بالتبعات التشغيلية المتوقعة على المنظمة جراء الاختراقات الأمنية.
K0007	معرفة بمنهجيات الأمن السيبراني للتحقق والتصريح والتحكم بالوصول.
K0008	معرفة بممارسات الأعمال المطبقة بداخل المنظمة.
K0009	معرفة بثغرات التطبيقات وأثرها المرجح.
K0010	معرفة بمنهجيات الاتصالات للأمن السيبراني والمبادئ والمفاهيم الداعمة للبنية التحتية للشبكات.
K0011	معرفة بقدرات وتطبيقات معدات الشبكات.
K0012	معرفة بكيفية تحليل القدرات والمتطلبات.
K0013	معرفة بأدوات تقييم الثغرات والدفاع للأمن السيبراني، وبقدراتها.
K0014	معرفة بالخوارزميات الحاسوبية.
K0015	معرفة بمبادئ برمجة الحاسبات.
K0016	معرفة بخوارزميات التشفير ونقاط القوة والضعف النسبية ومعايير الاختيار المناسبة.
K0017	معرفة بمفاهيم التشفير وإدارة مفاتيح التشفير.
K0018	معرفة بسياسات إدارة البيانات وسياسات التوحيد القياسي لها.
K0019	معرفة بمنهجيات وحلول النسخ الاحتياطي واسترداد البيانات المناسبة، شاملا الاختبارات.
K0020	معرفة باعتبارات الأمن السيبراني لنُظم قواعد البيانات.
K0021	معرفة بجوانب الأمن السيبراني التابعة لخطط استمرارية الأعمال وعمليات التعافي من الكوارث، شاملا الاختبارات.
K0022	معرفة بمعمارية الأمن السيبراني بالمنظمة.

رمز المعرفة	وصف المعرفة
K0023	معرفة بالهندسة الكهربائية المطلوبة لمعمارية الحاسبات.
K0024	معرفة بآليات الاستضافة والتحكم في الوصول إلى الشبكة.
K0025	معرفة بآلية عمل خدمات الشبكات وبروتوكولاتها من أجل توفير الاتصالات الشبكية.
K0026	معرفة بكيفية تثبيت مكونات النظام ودمجها وتحسينها.
K0027	معرفة بمبادئ التفاعل بين الإنسان والحاسب.
K0028	معرفة بعمليات التصريح والتقييم للأمن السيبراني.
K0029	معرفة بمتطلبات الخصوصية وضوابط الأمن السيبراني المستخدمة لإدارة المخاطر ذات الصلة بالبيانات.
K0030	معرفة بمبادئ الأمن السيبراني والخصوصية، التي تنطبق على تطوير البرمجيات.
K0031	معرفة بمصادر المعلومات فيما يتعلق بتحديد ومعالجة الثغرات بفاعلية.
K0032	معرفة بفئات الحوادث والاستجابة لها والجداول الزمنية لتلك الاستجابات.
K0033	معرفة بأفضل الممارسات للاستجابة للحوادث السيبرانية وإدارتها.
K0034	معرفة بأفضل الممارسات في مجال مبادئ ومنهجيات التحليل.
K0035	معرفة بمبادئ الأمن السيبراني والخصوصية، وكذلك المتطلبات التنظيمية.
K0036	معرفة بمنهجيات وأساليب كشف التسلل، سواء المخصصة منها للاستضافة أو الشبكات.
K0037	معرفة بعمليات وإجراءات إدارة المخاطر في المنظمة.
K0038	معرفة بمبادئ ومنهجيات أمن تقنية المعلومات.
K0039	معرفة بلغات الحاسوب الأولية المطلوبة للدور.
K0040	معرفة بالرياضيات المطلوبة للدور.
K0041	معرفة بالمعالجات الدقيقة.

رمز المعرفة	وصف المعرفة
K0042	معرفة بإدارة صلاحيات الوصول على الشبكات، وإدارة الهويات وصلاحيات الوصول عموما.
K0043	معرفة بأفضل الممارسات لمنهجيات تحليل حركة المرور عبر الشبكات.
K0044	معرفة وفهم بالتقنيات والحلول الجديدة من منظور الأمن السيبراني.
K0045	معرفة بنُظم التشغيل.
K0046	معرفة ببروتوكولات حركة مرور البيانات عبر الشبكات، وبمنهجياتها وبإدارتها.
K0047	معرفة بالتحليل على مستوى الحزم.
K0048	معرفة بمفاهيم الحوسبة المتوازية والموزعة.
K0049	معرفة بضوابط التحكم بالوصول المبنية على السياسات، والتكيف مع المخاطر.
K0050	معرفة بكيفية تقييم التبعات على الخصوصية.
K0051	معرفة ببُنى لغات البرامج ومنطقها.
K0052	معرفة بتهديدات وثغرات أمن النُظم والتطبيقات.
K0053	معرفة بالمفاهيم الأساسية في الإدارة الأمنية.
K0054	معرفة بأدوات تصميم النُظم الأمنية، وبمنهجياتها وأساليبها.
K0055	معرفة بأدوات تشخيص النُظم القياسية للقطاع وأساليب التعرف على الأخطاء.
K0056	معرفة بجميع مبادئ إدارة دورة حياة النُظم.
K0057	معرفة بمنهجيات اختبار النُظم وتقييمها.
K0058	معرفة بمفاهيم الاتصال عن بعد المطلوبة للدور.
K0059	معرفة بقدرات ووظائف تقنيات تنظيم المعلومات وإدارتها.
K0060	معرفة بعملية الإبلاغ عن حوادث الأمن السيبراني.

رمز المعرفة	وصف المعرفة
K0061	معرفة باستراتيجية وغايات تقنية المعلومات بالمنظمة.
K0062	معرفة بعملية هندسة النُظم.
K0063	معرفة بأمن الشبكات الخاصة الافتراضية.
K0064	معرفة بمكونات الهجمة الشبكية وعلاقتها بالتهديدات والثغرات.
K0065	معرفة بأدوات المعالجة والإبلاغ والتحري ذات العلاقة بعمليات التحري عن التهديدات الداخلية، شاملا القوانين والتنظيمات ذات العلاقة.
K0066	معرفة بمكونات الحاسبات المادية، وبمعمارية ملحقاتها ووظائفها.
K0067	معرفة بالمعتدين ذوي الصلة بخطط المنظمة وأساليبها وإجراءاتها.
K0068	معرفة بأدوات الشبكات.
K0069	معرفة بمبادئ الدفاع الأمني متعدد المستويات ومعمارية أمن الشبكات.
K0070	معرفة بأنواع مختلفة من الاتصالات الشبكية.
K0071	معرفة بالتقنية القابلة للاستغلال.
K0072	معرفة بامتدادات الملفات.
K0073	معرفة بأفضل ممارسات إدارة مخاطر سلسلة الإمداد.
K0074	معرفة بمتطلبات ولوائح الأمن السيبراني الوطنية ذات الصلة بالمنظمة.
K0075	معرفة بأنواع البيانات الجنائية الرقمية وكيفية تمييزها.
K0076	معرفة بلغات الحوسبة المفسرة والمجمعة.
K0077	معرفة بمصادر المعلومات الاستباقية للتهديدات، وقدراتها وحدودها.
K0078	معرفة بكيفية جمع مصادر المعلومات الاستباقية للتهديدات للمعلومات الاستباقية.
K0079	معرفة بعمليات أعمال المنظمة الأساسية وكيفية تأثرها بالأمن السيبراني.

رمز المعرفة	وصف المعرفة
K0080	معرفة بتهديدات الأمن السيبراني، ومخاطره، والقضايا التي تثيرها كل من التقنيات الجديدة وأصحاب الأفعال العدوانية.
K0081	معرفة بضوابط تنظيمات الصادر والوارد ذات الصلة بأنشطة ومعارف وتقنيات إدارة مخاطر الأمن السيبراني.
K0082	معرفة بإجراءات المنظمة لإدارة المخاطر.
K0083	معرفة بضوابط إدارة مخاطر سلسلة الإمداد، وعملياتها وممارساتها من منظور الأمن السيبراني.
K0084	معرفة بسياسات الأمن السيبراني و إجراءاته وتنظيماته.
K0085	معرفة بسياسات أمن مستخدمي تقنية المعلومات بالمنظمة.
K0086	معرفة بأساليب الهجمات الشائعة على مستوى الشبكة.
K0087	معرفة بالفئات المختلفة للهجمات السيبرانية.
K0088	معرفة بأنواع المهاجمين السيبرانيين وقدراتهم وغاياتهم.
K0089	معرفة بمنهجيات تقييم المخاطر والتهديدات الفعالة.
K0090	معرفة بمنهجيات إدارة النُظم، وإدارة الشبكات، وتحصين نُظم التشغيل.
K0091	معرفة بالمتطلبات التشريعية والتنظيمية.
K0092	معرفة بأفضل ممارسات الأمن السيبراني لإدارة سلسلة الإمداد لتقنية المعلومات.
K0093	معرفة بنُظم المعلومات الحساسة التي تم تصميمها بقدر محدود من ضوابط الأمن السيبراني التقنيّة.
K0094	معرفة بأساليب الهندسة العكسية للأجهزة.
K0095	معرفة بالبرمجيات الوسيطة المرتبطة بالدور.
K0096	معرفة ببروتوكولات الشبكات.
K0097	معرفة بأساليب الهندسة العكسية للبرمجيات.
K0098	معرفة بمخططات لغة (XML).

رمز المعرفة	وصف المعرفة
K0099	معرفة بمراحل الهجوم السيبراني.
K0100	معرفة بمفاهيم معمارية أمن الشبكات وتشمل المعمارية والبروتوكولات والمكونات والمبادئ.
K0101	معرفة بمبادئ إدارة نُظم الشبكات ونماذجها ومنهجياتها وأدواتها.
K0102	معرفة بمنهجيات التشفير.
K0103	معرفة بأثر تنفيذ التوقيعات على الفيروسات والبرمجيات الضارة والهجمات.
K0104	معرفة بمنافذ وخدمات نظامي التشغيل ويندوز ويونكس.
K0105	معرفة بالخواص الأمنية المتقدمة بداخل قواعد المعلومات المخصصة لعلاج البيانات.
K0106	معرفة بتقنيات ومفاهيم إدارة المعرفة السحابية المعمول بها بحق الأمن والحوكمة والمشتريات والإدارة.
K0107	معرفة بمعايير تصنيف البيانات ومنهجياتها من جانب صلتها بإدارة مخاطر الأمن السيبراني.
K0108	معرفة بواجهات برمجة تطبيقات الوصول إلى قواعد البيانات.
K0109	معرفة بمفاهيم تحسين العمليات التنظيمية ونماذج نضوج العمليات.
K0110	معرفة بمفاهيم المعمارية الأمنية والنماذج المرجعية.
K0111	معرفة بمفاهيم إدارة الخدمات للشبكات والمعايير ذات الصلة.
K0112	معرفة بمفاهيم ووظائف جدران الحماية للتطبيقات.
K0113	معرفة بنماذج الأمن القياسية للقطاع وبكيفية تطبيقها بفاعلية.
K0114	معرفة بأساليب الاتصال الخفية.
K0115	معرفة بمفاهيم النسخ الاحتياطي للبيانات واسترجاعها.
K0116	معرفة بمتطلبات السرية والسلامة والتوافر.
K0117	معرفة بنموذج "ترابط الأنظمة المفتوحة" (OSI) والبروتوكولات الخاصة بشبكاتها.

رمز المعرفة	وصف المعرفة
K0118	معرفة بالقوانين والسلطات التشريعية والتنظيمات ذات العلاقة التي تحكم أنشطة الأمن السيبراني وتسري عليها.
K0119	معرفة بمفاهيم إدارة النُظم لأنظمة التشغيل المستخدمة من قبل المنظمة.
K0120	معرفة بالأنواع المختلفة لمعمارية الحاسبات ذات الصلة بالمنظمة.
K0121	معرفة بنماذج الخدمات السحابية وكيف يمكن لتلك النماذج أن تحدّ من الاستجابة للحوادث.
K0122	معرفة بجميع قدرات الأمن السيبراني الهجومية والدفاعية.
K0123	معرفة بمفاهيم تحليل البرمجيات الضارة ومنهجياته.
K0124	معرفة بمعايير أمن البيانات ذات العلاقة بمعلومات المعرفات الشخصية.
K0125	معرفة بمعايير أمن البيانات لقطاع بطاقات الدفع.
K0126	معرفة بمعايير أمان البيانات ذات العلاقة بالقطاع الذي تعمل فيه المنظمة.
K0127	معرفة بأفضل الممارسات لمنهجيات إدارة مخاطر تقنية المعلومات.
K0128	معرفة بالقوانين والأنظمة والمعايير الأخرى المعمول بها في مجال الأمن السيبراني للبنية التحتية الحساسة.
K0129	معرفة بأساليب إدارة الإعدادات.
K0130	معرفة بإدارة الأمن.
K0131	معرفة بمزايا تشفير البيانات الحالية والناشئة في قواعد البيانات.
K0132	معرفة بحالات الاستخدام ذات الصلة بالتعاون عبر المنصات ومزامنة المحتوى.
K0133	معرفة بمتطلبات المنظمة لتصنيف بيانات الأمن السيبراني.
K0134	معرفة بمنهجيات اختبار أمن النُظم وتقييمها.
K0135	معرفة بالثغرات المحتملة في كافة المعدات الشبكية وكيفية استخدامها.
K0136	معرفة بكيفية تصميم الإجراءات المضادة للمخاطر الأمنية المحددة.

رمز المعرفة	وصف المعرفة
K0137	معرفة بكيفية اكتشاف مكونات الشبكات وإعادة بناء مخططات الشبكات.
K0138	معرفة بالتحليل على مستوى الحِزم باستخدام الأدوات المناسبة.
K0139	معرفة باستخدام أدوات الشبكة الجزئية.
K0140	معرفة بعلم التشفير.
K0141	معرفة بالتقنيات الناشئة وقابليتها للاستغلال.
K0142	معرفة بتوجهات التقنية.
K0143	معرفة بثغرات الأمن السيبراني عبر نطاق واسع من تقنيات القطاع القياسية.
K0144	معرفة بالمنهجيات والإجراءات والأساليب الأساسية لجمع معلومات الأمن السيبراني وإعدادها ومشاركتها.
K0145	معرفة بأدوات واجهة أوامر نظام التشغيل.
K0146	معرفة بالنُظم المدمجة وكيفية تطبيق ضوابط الأمن السيبراني عليها.
K0147	معرفة بأدوات وتطبيقات نُظم كشف التسلل ومنعه.
K0148	معرفة ببروتوكولات الشبكات وخدمات الدليل.
K0149	معرفة بعمليات تصميم الشبكات، شاملا الغايات الأمنية والتشغيلية، والمفاضلات.
K0150	معرفة بتقنيات الأمن السيبراني الحالية والناشئة والتهديدات ذات العلاقة.
K0151	معرفة بمنهجيات توثيق عمليات الوصول.
K0152	معرفة بكيفية استخدام أدوات تحليل الشبكات لتحديد الثغرات.
K0153	معرفة بمبادئ اختبار الاختراق ومبادئ الفرق الحمراء، وأدواتهما وأساليبهما.
K0154	معرفة ببيئة التهديد للمنظمة.
K0155	معرفة بمصطلحات اتصالات البيانات.

رمز المعرفة	وصف المعرفة
K0156	معرفة بنظريات قواعد البيانات.
K0157	معرفة بخوارزميات التشفير.
K0158	معرفة بأمن الشبكات على صعيد الممارسين للمهنة.
K0159	معرفة بأمن عمليات تقنية المعلومات.
K0160	معرفة بغايات المنظمة وأولويات القيادة ومنهجيات إدارة المخاطر.
K0161	معرفة بأجهزة الشبكة المادية والمنطقية وكذلك البنية التحتية.
K0162	معرفة باستراتيجيات إدارة المخاطر للأمن السيبراني ومعالجتها.
K0163	معرفة بأساسيات أمن الشبكات.
K0164	معرفة ببروتوكولات التوجيه الشبكي وكيفية تفاعلها لتوفير اتصالات الشبكة.
K0165	معرفة بكل ما يمثل تهديدًا لأمن الشبكة.
K0166	معرفة بمبدأ تصنيف المخاطر كجزء من عملية إدارة المخاطر.
K0167	معرفة بمنهجيات تقييم المخاطر.
K0168	معرفة بالمصادر العامة التي تسرد تفاصيل مخاطر أمان التطبيق الشائعة وسبل ومعالجتها.
K0169	معرفة بإجراءات الإبلاغ عن انتهاك البيانات.
K0500	معرفة بالبرمجة النصية.
K0501	معرفة ببروتوكولات TCP/IP الشبكية.
K0502	معرفة بالتقنيات السحابية والأمن السحابي.
K0503	معرفة بأجهزة الشبكات ووظائفها.
K0504	معرفة بتقنيات الشبكات.

رمز المعرفة	وصف المعرفة
K0505	معرفة بإمكانيات وقيود منتجات الأمن السيبراني.
K0506	معرفة بأفضل الممارسات في منهجيات إدارة مخاطر الأمن السيبراني.
K0507	معرفة بالنُظم الأمنية متعددة المستويات والحلول المستخدمة في مجالات مختلفة.
K0508	معرفة بتدابير التخطيط لحماية النظام.
K0509	معرفة بمعمارية الشبكات متعددة الطبقات.
K0510	معرفة بالمفاهيم والأنماط المعمارية.
K0511	معرفة بدمج أهداف وغايات المنظمة في معمارية النظام.
K0512	معرفة بمعايير التقييم والمصادقة ذات العلاقة بالأمن السيبراني.
K0513	معرفة منهجيات تحمل العيوب بالنُظم.
K0514	معرفة المناطق الشبكية المعزولة.
K0515	معرفة بهيكل الشبكات الرقمية والهاتفية الحديثة، ومعماريتها وتصميمها.
K1000	معرفة بهياكل البيانات المعقدة.
K1001	معرفة بمبادئ التنقيب عن البيانات وتخزين البيانات.
K1002	معرفة بنُظم إدارة قواعد البيانات ولغات الاستعلام وعلاقات الجداول وطرق العرض.
K1003	معرفة بإدارة الحقوق الرقمية.
K1004	معرفة بمتطلبات المنظمة للتقييم والمصادقة فيما يتعلق بإدارة مخاطر الأمن السيبراني.
K1005	معرفة بنُظم المراسلات المؤسسية والبرمجيات ذات الصلة.
K1006	معرفة بكيفية استغلال مبدأ الصمود والأنظمة الرديفة لمعالجة مخاطر الأمن السيبراني.
K1007	معرفة بمبادئ هندسة نُظم الأمن السيبراني والمعايير المستخدمة من قبل المنظمة.

رمز المعرفة	وصف المعرفة
K1008	معرفة بمبادئ ومفاهيم الشبكات المحلية والشبكات واسعة النطاق، شاملا إدارة عرض النطاق.
K1009	معرفة بمفاهيم هندسة العمليات.
K1010	معرفة بلغات الاستعلام.
K1011	معرفة بأساليب إدارة الإعدادات الآمنة.
K1012	معرفة بمبادئ تصحيح الأخطاء بالبرمجيات.
K1013	معرفة بأدوات تصميم البرمجيات ومنهجياته وأساليبه.
K1014	معرفة بنماذج تطوير البرمجيات.
K1015	معرفة بهندسة البرمجيات.
K1016	معرفة بمصادر مجموعات البيانات بالمنظمة، وخصائصها واستخداماتها.
K1017	معرفة بمبادئ التحليل المنظم ومنهجياته.
K1018	معرفة بأدوات تصميم النُظم ومنهجياته وأساليبه، شاملا أدوات أتمتة عمليات تحليل وتصميم النُظم.
K1019	معرفة بخدمات الشبكة العنكبوتية.
K1020	معرفة بأدوات واجهة أوامر نظام التشغيل.
K1021	معرفة بأساليب البرمجة الآمنة.
K1022	معرفة بمبادئ ومنهجيات أمن تقنية المعلومات ذات العلاقة بالبرمجيات.
K1023	معرفة بعملية ضمان جودة البرمجيات.
K1024	معرفة بمنهجيات نشر البرمجيات الآمنة، وأدواتها وممارستها.
K1025	معرفة بالتطبيقات التي يمكنها تسجيل الأخطاء والاستثناءات وعيوب التطبيق.
K1026	معرفة بكيفية العمل مع والاستفادة من مخرجات مراكز البحث والتطوير ومجموعات الأفكار والأبحاث الأكاديمية والصناعية.

رمز المعرفة	وصف المعرفة
K1027	معرفة بكيفية استخدام التقنيات والأدوات لاستكشاف وتحليل وتمثيل البيانات.
K1028	معرفة بنظرية التعلّم الآلي ومبادئه.
K1029	معرفة بتحديد آثار الأدلة الجنائية.
K1030	معرفة بمعمارية الاتصالات المتنقلة.
K1031	معرفة بهياكل نُظم التشغيل ومكوناتها الداخلية.
K1032	معرفة بأدوات تحليل الشبكات المستخدمة للكشف عن الثغرات في اتصالات البرمجيات.
K1033	معرفة بنماذج الأمن القياسية في القطاع.
K1034	معرفة بمنهجيات الاختراق.
K1035	معرفة بالمفاهيم الهندسية المنطبقة على المعمارية الحاسوبية والأجهزة والبرمجيات الحاسوبية ذات الصلة.
K1036	معرفة بنظرية المعلومات.
K1037	معرفة بأساليب التحليل لكشف الأسباب الجذرية.
K1038	معرفة باستراتيجيات البحث وإدارة المعرفة.
K1039	معرفة بتطوير البرمجيات من خلال اللغات عالية المستوى.
K1040	معرفة بتطوير البرمجيات لنُظم يونكس أو لينكس.
K1041	معرفة بدمج مكونات البرامج أو اختبارها، شاملا تحليل وتنفيذ خطط وبرمجيات الاختبارات.
K1042	معرفة بالمنهجيات الإحصائية.
K1043	معرفة بمعالجة اللغات الطبيعية.
K1044	معرفة بتحليل السجلات المؤتمتة.
K1045	معرفة بخوارزميات التعلم الآلي.

رمز المعرفة	وصف المعرفة
K1046	معرفة بطرق تطوير الخوارزميات الأساسية.
K1047	معرفة بالتقنيات مفتوحة المصدر.
K1500	معرفة بمقاييس أو مؤشرات أداء النُظم وتوافرها.
K1501	معرفة بأفضل الممارسات لمبادئ وأساليب إدارة الموارد.
K1502	معرفة بأفضل الممارسات لإدارة الخوادم، ونظريات هندسة النُظم ومفاهيمها ومنهجياتها.
K1503	معرفة بنُظم التشغيل للخوادم ولأجهزة العملاء والأجهزة المتنقلة.
K1504	معرفة ببرمجيات النُظم ومعايير التصميم بالمنظمة وسياساتها ومنهجياتها.
K1505	معرفة بأفضل الممارسات لعمليات دمج التقنيات ذات العلاقة بالأمن السيبراني.
K1506	معرفة بأفضل الممارسات لمبادئ وأساليب إدارة البرامج وإدارة المشاريع.
K1507	معرفة بأفضل الممارسات لمنهجيات الاستجابة للحوادث، وللأدوار والمسؤوليات.
K1508	معرفة بتهديدات الأمن السيبراني الحالية والناشئة وعوامل التهديد.
K1509	معرفة بمتطلبات شراء تقنيات المعلومات الحساسة ذات العلاقة بالأمن السيبراني.
K1510	معرفة بتقنيات المراقبة المستمرة القياسية بالقطاع وأدواتها.
K1511	معرفة بضوابط الأمن السيبراني ذات العلاقة باستخدام البيانات ومعالجتها وتخزينها وبثها.
K2000	معرفة بالمجالات الإدراكية والأدوات والمنهجيات المعمول بها في التعلّم في كل مجال.
K2001	معرفة بتطوير وصيانة تقنيات المحاكاة والآلات الافتراضية.
K2002	معرفة بأساليب تقدير التعلم المختلفة واختباره وتقييمه وكيفية وتوقيت استخدامها.
K2003	معرفة بتطوير خدمات التدريب والتعلّم الإلكتروني على الحاسوب.
K2004	معرفة بنماذج التصميم والتقييم التعليمي.

رمز المعرفة	وصف المعرفة
K2005	معرفة بأفضل الممارسات التدريبية.
K2006	معرفة بمستويات التعلُّم.
K2007	معرفة بنُظم إدارة التعلُّم واستخداماتها.
K2008	معرفة بأنماط التعلُّم وكيفية تطوير التدريب لاستيعابهم.
K2009	معرفة بطرق التعلّم.
K2010	معرفة بنُظم التدريب المؤسسية.
K2011	معرفة بالإطار السعودي لكوادر الأمن السيبراني، والأدوار والمهام الوظيفية، والمعارف، والمهارات، والقدرات.
K2012	معرفة باستخدامات الوسائط المكتوبة والشفوية والبصرية لدعم التدريب وأساليب إنتاج تلك الوسائط وتوصيلها ونشرها.
K2013	معرفة بسياسات وعمليات وإجراءات الموارد البشرية بالمنظمة.
K2014	معرفة بسياسات التدريب والتعليم بالمنظمة، وعملياتها وإجراءاتها.
K2015	معرفة بمبادئ وعمليات إجراء تقييم احتياجات التدريب والتعليم.
K2016	معرفة بمفاهيم والإجراءات والبرمجيات والمعدات والتطبيقات التقنية ذات الصلة بتدريب الأمن السيبراني.
K2017	معرفة بعمليات الاختبار والتقييم للمتعلمين.
K2018	معرفة بمنهجيات تصميم المناهج والتدريس والتعليم للأفراد والجماعات.
K2019	معرفة بالجهات الخارجية والجهات الأكاديمية المتخصصة بالأمن السيبراني في التعليم والبحث والتطوير.
K2020	معرفة بقدرات بدائل التدريب التقنية للأمن السيبراني وحدود قدراتها.
K2021	معرفة بكيفية التقاط العلم وغيرها من التدريبات ذات الصلة بالأمن السيبراني التي تساعد في تحسين المهارات العملية.
K2500	معرفة بارتباطات الشبكات المحلية والشبكات واسعة النطاق بالمنظمة والمخاطر التي تشكلها على الأمن السيبراني.

رمز المعرفة	وصف المعرفة
K2501	معرفة بأفضل الممارسات لمراجعة وتحديد مدى ملاءمة الحلول التقنية لتلبية متطلبات الأمن السيبراني.
K2502	معرفة بمعمارية تقنية المعلومات المؤسسية للمنظمة والمخاطر التي تشكلها على الأمن السيبراني.
K2503	معرفة بالاستراتيجيات النظرية والتطبيقة المتعلقة بالأمن السيبراني.
K2504	معرفة بإجراءات إعداد التقارير من كافة المصادر ونشرها.
K2505	معرفة بأفضل الممارسات لإجراءات التدقيق والتسجيل.
K2506	معرفة بقوالب التقارير وبأفضل الممارسات لإعداد تقارير الالتزام للأمن السيبراني لصالح الشركاء الخارجيين.
K2507	معرفة بقوالب التقارير المعتمدة بالمنظمة للإدارة وللإبلاغ عن حالة الالتزام المتعلقة بمخاطر الأمن السيبراني، وحالات التأهب والتقدم المحرزة لتحقيق الخطط.
K2508	معرفة بهوية المخططين لاستراتيجيات المنظمة وسياساتها وخططها، وكيفية التواصل معهم، ومعرفة بتوقعاتهم.
K3000	معرفة بمفاهيم وممارسات معالجة البيانات الجنائية الرقمية لضمان قبولها كأدلة.
K3001	معرفة بمبادئ جمع المعلومات الاستباقية للتهديدات السيبرانية، وسياساته وإجراءاته، شاملا الصلاحيات والقيود القانونية.
K3002	معرفة بسياسات المنظمة وإجراءات التشغيل القياسية لها المتعلقة بالأمن السيبراني.
K3003	معرفة بسياسات الإفصاح الأجنبية وأنظمة تنظيم الاستيراد والتصدير فيما يتعلق بالأمن السيبراني.
K3004	معرفة بكيفية إنتاج إفصاحات الخصوصية لأمن المعلومات بموجب الأنظمة المعمول بها.
K3005	معرفة بتقنيات تعزيز الخصوصية شاملا قدرات تشغيلها وتقاريرها.
K3006	معرفة بالتفاعل بين الإنسان والحاسب ومبادئ التصميم القابل للاستخدام المتعلقة بالأمن السيبراني.
K3500	معرفة بأساليب التحصين للنُظم وللشبكات ولنُظام التشغيل.
K3501	معرفة بإجراءات الاختبار ومبادئه ومنهجياته ذات الصلة بتطوير ودمج قدرات الأمن السيبراني.
K3502	معرفة بتقنيات البث وأساليب التشويش التي تمكّن أو تمنع نقل المعلومات غير المرغوبة أو تمنع الأنظمة الحية من العمل بشكل صحيح والقوانين المتعلقة باستخدامها.

رمز المعرفة	وصف المعرفة
K3503	معرفة بتحليل تدفق البيانات بالشبكات، ومنهجياته وعملياته.
K3504	معرفة بأساسيات الشبكات واتصالات الإنترنت.
K3505	معرفة بكيفية تحليل صفحات توصيف بناء البنية التحتية، وقواعد بيانات إدارة الإعدادات، ومسوحات الثغرات، وقوائم التحكم بالوصول، ووثائق الموردين بغرض فهم سلوكيات البرمجيات وتفاعلاتها.
K4000	معرفة بمفاهيم تقنية الوصول عن بُعد والأدوات والقدرات وآثارها على الأمن السيبراني.
K4001	معرفة بالقدرات والوظائف ومخاطر الأمن السيبراني المرتبطة بتقنيات إنشاء المحتوى.
K4002	معرفة بقدرات ووظائف تقنيات العمل التعاوني وانعكاساتها على الأمن السيبراني.
K4003	معرفة بلوائح الاستيراد والتصدير المتعلقة بالتشفير.
K4004	معرفة بعلم التصنيف وعلم الدلالية.
K4005	معرفة بعمليات الوصول عن بُعد والأدوات والقدرات المتعلقة بدعم العملاء.
K4006	معرفة بكيفية تقييم مدى موثوقية الموردين والمنتجات شاملا الاستعانة باستشارات خارجية.
K4007	معرفة بفهارس خدمات تقنيات المعلومات.
K4008	معرفة بتطوير وتطبيق نظام إدارة بيانات اعتماد المستخدم.
K4009	معرفة بتنفيذ نُظم مستودعات المفتاح المؤسسية لدعم تشفير البيانات حال تخزينها.
K4010	معرفة بمبادئ السرية والسلامة والتوافر.
K4011	معرفة بأساليب إخفاء البيانات وكيفية تطبيقها أو نقضها من خلال التقنية.
K4012	معرفة بأساليب تنقيب البيانات.
K4013	معرفة بتوافر الأصول وقدراتها وحدودها.
K4014	معرفة بقدرات التشفير المنطقية وحدودها ومساهماتها في العمليات السيبرانية.
K4015	معرفة بخوارزميات التشفير وأدواته للشبكات المحلية اللاسلكية.
K4016	معرفة بعمليات التعريف وإعداد التقارير.

رمز المعرفة	وصف المعرفة
K4017	معرفة بأساليب التعتيم.
K4018	معرفة بمفاهيم إدارة نظم التشغيل لأنظمة التشغيل بالمنظمة.
K4500	معرفة بمنهجيات الاختراق.
K4501	معرفة بالبنية التحتية الداعمة لسلامة وأداء وموثوقية تقنية المعلومات.
K4502	معرفة بمبادئ اختبارات الاختراق وأساليبه وكيفية تطبيق أفضل ممارساته.
K4503	معرفة بمفاهيم البرمجة الحاسوبية، شاملا اللغات الحاسوبية والبرمجة والاختبار وتصحيح الأخطاء وأنواع الملفات.
K4504	معرفة باستخدام لغات البرمجة ذات الصلة بالأنظمة والبنية التحتية المطلوب اختبارها.
K4505	معرفة باستخدام أنظمة التشغيل، وأدواتها ذات الصلة بالأنظمة التي يجري اختبارها.
K4506	معرفة بكيفية محاكاة الهجمات التي سيستخدمها المهندس الاجتماعي لمحاولة خرق النظام.
K4507	معرفة بأدوات كسر التشفير أو كلمة المرور، وكذلك منهجيات الوصول عن بُعد.
K4508	معرفة باستخدام الخوادم الشبكية والأدوات الشبكية المستخدمة من قبل المؤسسة أو الأنظمة التي يجري اختبارها.
K4509	معرفة باستخدام واختيار الأدوات والمنتجات الأمنية.
K4510	معرفة باستخدام الأدوات والإطارات الأكثر شيوعا لدى المخترقين الساعين لمهاجمة المنظمة.
K5000	معرفة بأدوات تشخيص الخوادم وأساليب معرفة الأخطاء.
K5001	معرفة بأنواع الأجهزة الإلكترونية الرئيسية ونقاط ضعفها وكيفية تخزينها للبيانات.
K5002	معرفة بكيفية تنفيذ نُظم الملفات.
K5003	معرفة بعمليات احتجاز الأدلة الرقمية والحفاظ عليها.
K5004	معرفة بالتقنيات وأدوات المخترق.
K5005	معرفة بأساليب التحقيق اللازمة للأجهزة وأنظمة التشغيل وتقنيات الشبكة.

رمز المعرفة	وصف المعرفة
K5006	معرفة بالقوانين المعمول بها وسياسات وإجراءات المنظمة ذات العلاقة بجمع الأدلة الرقمية وتسجيلها.
K5007	معرفة بعمليات جمع الأدلة الإلكترونية، وتعبئتها ونقلها وتخزينها، مع الحفاظ خلال كل ذلك على تسلسل حجز الأدلة.
K5008	معرفة بأنواع البيانات المستديمة وكيفية جمعها.
K5009	معرفة بأدوات وأساليب جمع البريد الإلكتروني والبحث والتحليل.
K5010	معرفة بملفات النظام التي تحوي معلومات ذات صلة ومكان العثور عليها.
K5011	معرفة بكيفية إدارة عمليات البيانات الجنائية الميدانية والأدوات التي تدعمها.
K5012	معرفة بتقنيات الترشيح للشبكة العنكبوتية.
K5013	معرفة بالديناميكية الاجتماعية العالمية لأنواع التهديد السيبراني المختلفة.
K5014	معرفة بأدوات ربط الأحداث الأمنية.
K5015	معرفة بقانون الأدلة الإلكترونية.
K5016	معرفة بالإجراءات الوطنية أو المعمول بها في القضاء والمحاكم في قضايا الجرائم السيبرانية وجرائم الاحتيال.
K5017	معرفة بأدوات وأساليب استرجاع الملفات من بياناتها المتفرقة.
K5018	معرفة بمفاهيم الهندسة العكسية للبرمجيات الخبيثة.
K5019	معرفة بالخطط والأساليب والإجراءات المضادة للأدلة الجنائية.
K5020	معرفة بتطبيقات التصميم والإعداد والدعم للمختبرات الجنائية.
K5021	معرفة بإجراءات وأدوات تصحيح الأخطاء.
K5022	معرفة بأسباب عبث الخصوم بنوع الملفات وكيف يتم ذلك.
K5023	معرفة بأدوات تحليل البرمجيات الضارة.
K5024	معرفة بكيفية تفادي البرمجيات الضارة للكشف من قبل الآلات الافتراضية.

رمز المعرفة	وصف المعرفة
K5025	معرفة ببروتوكولات إدارة الأزمات وعملياتها وأساليبها ذات العلاقة بالأمن السيبراني بالمنظمة.
K5026	معرفة بالسلوكيات الجسدية والفسيولوجية التي قد تشير إلى نشاط مشبوه أو غير عادي.
K5027	معرفة بالعملية القضائية متضمنا عرض الحقائق والأدلة.
K5028	معرفة بالتحليل الثنائي.
K5029	معرفة بمفاهيم معمارية الشبكات، شاملا المعمارية والبروتوكولات والمكونات.
K5030	معرفة بمفاهيم وممارسات معالجة البيانات الجنائية الرقمية.
K5031	معرفة بالتصميم التشغيلي وفهمه.
K5032	معرفة بالتشريعات والقوانين والأنظمة والسياسات التي تحكم عمليات جمع البيانات من خلال أساليب الأمن السيبراني.
K5500	معرفة بمفاهيم ومصطلحات وعمليات وسائط الاتصال.
K5501	معرفة بأنواع مواقع الشبكة العنكبوتية وإدارتها ووظائفها، ونُظم إدارة المحتوى.
K5502	معرفة بمنهجيات الهجوم وأساليبه.
K5503	معرفة بمعايير وسياسات وإجراءات تصنيف ووسم المعلومات والوثائق على المستوى الوطني وعلى مستوى المنظمة.
K5504	معرفة بإصابات الحاسب والشبكات الشائعة ومنهجياتها.
K5505	معرفة بأساسيات شبكات الحاسبات.
K5506	معرفة بمجموعات التسلل الحاسوبية.
K5507	معرفة بمصادر المعلومات الاستباقية للتهديدات السيبرانية وقدرات كل منها.
K5508	معرفة بمفاهيم عمليات الأمن السيبراني ومصطلحاتها ومبادئها وقيودها وآثارها.
K5509	معرفة بتقنيات الاتصالات الناشئة والمتطورة وآثارها على الأمن السيبراني.
K5510	معرفة بمفاهيم العمليات السيبرانية الأساسية، ومصطلحاتها ومعاجمها (مثل إعداد البيئة، الهجوم السيبراني، الدفاع السيبراني)، ومبادئها وقدراتها وقيودها وآثارها.

رمز المعرفة	وصف المعرفة
K5511	معرفة بالمنتجات الأمنية المخصصة للاستضافة وكيفية تأثير هذه المنتجات في الحد من التعرض للاستغلال.
K5512	معرفة بطريقة عمل تطبيقات الاتصالات عبر الإنترنت.
K5513	معرفة بالمخاطر التي تمثلها الشبكات الهاتفية الرقمية الحديثة على أمن المنظمة السيبراني.
K5514	معرفة بالمخاطر التي تمثلها الشبكات اللاسلكية على أمن المنظمة السيبراني.
K5515	معرفة بكيفية استخلاص البيانات الوصفية المجملة، وكيفية تحليلها واستخدامها.
K5516	معرفة بمختلف أنواع المنظمات والفرق والأفراد المشاركين في جمع المعلومات الاستباقية عن التهديدات السيبرانية.
K5517	معرفة بكيفية استخدام المعلومات الاستباقية للتهديدات السيبرانية لإفادة التخطيط للأمن السيبراني في المنظمة.
K5518	معرفة بكيفية استخدام المعلومات الاستباقية للتهديدات السيبرانية لإفادة العمليات التشغيلية للأمن السيبراني في المنظمة.
K5519	معرفة بالخطط التي يمكن للمنظمة تسخيرها للتنبؤ بقدرات وأعمال المهاجمين وصدها.
K5520	معرفة بأسلوب عنونة شبكة الإنترنت.
K5521	معرفة بممثلي التهديدات السيبرانية للمنظمة.
K5522	معرفة ببيئة التهديد التي تعمل ضمنها المنظمة.
K5523	معرفة بالبرمجيات الضارة.
K5524	معرفة بقيادات المنظمة، وهيكلها الإداري، وإجراءات صنع القرار السيبراني.
K5525	معرفة ببُنى ممثلي التهديد على المنظمة، وقدراتهم الأساسية، وثغراتهم.
K5526	معرفة بخطط ممثلي التهديد على المنظمة وأساليبهم، وإجراءاتهم.
K5527	معرفة بأساسيات الاتصالات بعيدة المدى.
K5528	معرفة بالهيكل الأساسي للشبكات الرقمية والهاتفية الحديثة، ومعماريتها وتصميمها.
K5529	معرفة بعوامل التهديد التي يمكن أن تؤثر على عمليات الجمع.

رمز المعرفة	وصف المعرفة
K5530	معرفة بكيفية استخدام شبكة الإنترنت من قبل ممثلي التهديد على المنظمة، وما هي معلومات الاستهداف التي يمكنهم استخلاصها منها عن المنظمة.
K5531	معرفة بأنظمة التهديدات السيبرانية.
K5532	معرفة بمنتجات المحاكاة الافتراضية.
K5533	المعرفة بالهيكل الأساسي لأنظمة الاتصالات اللاسلكية الحديثة، ومعماريتها وتصميمها.
K5534	معرفة بالبدائل السياسية والقانونية والتجارية وغيرها من الخيارات ذات الصلة التي يمكن استخدامها لردع ممثلي التهديد الذين يهددون المنظمة.
K6000	معرفة بأجهزة الشبكات ووظائفها في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
K6001	معرفة بتقنيات الشبكات في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
K6002	معرفة بإمكانيات وقيود منتجات الأمن السيبراني في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
K6003	معرفة بأفضل الممارسات في منهجيات إدارة مخاطر الأمن السيبراني في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
K6004	معرفة بالنُظم الأمنية متعددة المستويات والحلول المستخدمة في مجالات مختلفة في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
K6005	معرفة بتدابير التخطيط لحماية النظام في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
K6006	معرفة بمعمارية الشبكات متعددة الطبقات في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
K6007	معرفة بالمفاهيم والأنماط المعمارية في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
K6008	معرفة بدمج أهداف وغايات المنظمة في معمارية النظام في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
K6009	معرفة بمعايير التقييم والمصادقة ذات العلاقة بالأمن السيبراني في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
K6010	معرفة منهجيات تحمل العيوب بالنُظم في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
K6011	معرفة المناطق الشبكية المعزولة في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.

رمز المعرفة	وصف المعرفة
K6012	معرفة بمكونات نُظم التحكم الإشرافي وحيازة البيانات.
K6013	معرفة بهيكل الشبكات الرقمية والهاتفية الحديثة، ومعماريتها وتصميمها في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
K6014	معرفة ببيئات تشغيل نظم التحكم الصناعي ووظائفها.
K6015	معرفة بمعمارية شبكات نظام التحكم الصناعي وبروتوكولات الاتصال التابعة لها.
K6016	معرفة بأجهزة نظام التحكم الصناعي ولغات البرمجة الصناعية.
K6017	معرفة بنطاق تهديدات نظم التحكم الصناعي.
K6018	معرفة بالتهديدات والثغرات في نُظم وبيئات التحكم الصناعي.
K6019	معرفة بمنهجيات وأساليب كشف التسلل لكشف حالات التسلل إلى نظم التحكم الصناعي.
K6020	معرفة بمنهجيات وأساليب أمن نظم التحكم الصناعي.

(جدول ١١): أوصاف المهارات

رمز المهارة	وصف المهارة
S0001	مهارة كفاءة أداء مسوحات للثغرات الأمنية ولتحديد الثغرات في النُظم الأمنية.
S0002	مهارة تحديد البرمجيات الضارة، واكتشافها، واحتوائها والإبلاغ عنها.
S0003	مهارة تطبيق ودمج تقنيات المعلومات في الحلول المقترحة.
S0004	مهارة تطبيق مبادئ الأمن السيبراني الأساسية.
S0005	مهارة تطبيق ضوابط الاستضافة والتحكم في الوصول إلى الشبكة.
S0006	مهارة تطوير ونشر التوقيعات.
S0007	مهارة تصميم التدابير المضادة للمخاطر الأمنية المحددة.
S0008	مهارة تصميم دمج حلول الأجهزة والبرمجيات.
S0009	مهارة تسخير تقنيات كشف التسلل لكشف عمليات التسلل ذات العلاقة بالاستضافة والشبكات.
S0010	مهارة تحديد الحالة التشغيلية العادية للأنظمة الأمنية وكيفية تأثر تلك الحالة جراء التغيير.
S0011	مهارة تطوير خطط الطوارئ والتعافي للبنية التحتية للشبكات، واختبارها وتطبيقها.
S0012	مهارة تقييم مدى كفاية التصاميم الأمنية.
S0013	مهارة الحفاظ على سلامة الأدلة وفقًا لإجراءات التشغيل القياسية أو المعايير الوطنية.
S0014	مهارة ضبط الحساسات.
S0015	مهارة استخدام محلّلات البروتوكولات.
S0016	مهارة استخدام أجهزة الشبكات الخاصة الافتراضية وتشفيرها.
S0017	مهارة كتابة البرامج بلغات برمجة مدعومة حاليا.
S0018	مهارة استخدام القواعد والمنهجيات العلمية لحل المشاكل.
S0019	مهارة استخدام الآلات الافتراضية.

رمز المهارة	وصف المهارة
S0020	مهارة إجراء التحليلات الجنائية في عدة بيئات لنُظم التشغيل.
S0021	مهارة معايرة واستخدام أدوات الحماية الحاسوبية.
S0022	مهارة تأمين اتصالات الشبكات.
S0023	مهارة كفاءة تحديد وتصنيف أنواع الثغرات والهجمات ذات الصلة.
S0024	مهارة حماية الشبكة ضد البرمجيات الضارة.
S0025	مهارة تقييم الأضرار.
S0026	مهارة استخدام أدوات تحليل الشبكات لتحديد الثغرات.
S0027	مهارة معايرة واستخدام مكونات حماية الشبكة.
S0028	مهارة إجراء التدقيقات أو المراجعات الأمنية للنُظم التقنية.
S0029	مهارة استخدام أدوات تحليل النصوص الثنائية.
S0030	مهارة استخدام وظائف الامتزاج أحادي الإتجاه.
S0031	مهارة قراءة البيانات الست عشرية.
S0032	مهارة تحديد الأساليب الشائعة للتشفير.
S0033	مهارة قراءة وتفسير التوقيعات.
S0034	مهارة انتقاء أو تطوير أنشطة التعلّم بهدف تأمين أكثر المواد ملاءمة للمتعلمين.
S0035	مهارة التحصين الأمني للنظام والشبكات ونظام التشغيل.
S0036	مهارة تصميم خطط مناسبة لاختبار الأمن السيبراني.
S0037	مهارة إجراء تقييمات لثغرات التطبيقات وفهم نتائجها.
S0038	مهارة استخدام قدرات التشفير والتوقيع للبنية التحتية للمفاتيح العامة في التطبيقات.

رمز المهارة	وصف المهارة
S0039	مهارة تطبيق النماذج الأمنية.
S0040	مهارة تقييم الضوابط الأمنية المستندة إلى مبادئ الأمن السيبراني.
S0041	مهارة إجراء تحليلات على مستوى الحِزم.
S0042	مهارة التعرف على ثغرات النُظم الأمنية.
S0043	مهارة إعداد واستخدام مكونات حماية شبكة الحاسبات.
S0044	مهارة إجراء تقييمات الأثر والخطر للأمن السيبراني.
S0045	مهارة تطبيق أساليب البرمجة الآمنة بفاعلية.
S0046	مهارة استخدام أدوات ربط الأحداث الأمنية بفاعلية.
S0047	مهارة استخدام أدوات تحليل الشفرات البرمجية بفاعلية.
S0048	مهارة إجراء تحليل الأسباب الجذرية لقضايا الأمن السيبراني.
S0049	مهارة إجراء البحث باستخدام الشبكة العنكبوتية العميقة بفاعلية وأمان.
S0050	مهارة تحليل النظام المستهدف بفاعلية.
S0051	مهارة إعداد وتقديم الملخصات بفاعلية ووضوح واختصار.
S0052	مهارة التعرف على نشاط الشبكة الضار بين حركة البيانات وتفسيرها.
S0053	مهارة الهندسة العكسية للبرمجيات الضارة.
S0054	مهارة تحليل الأدوات والتقنيات والإجراءات المستخدمة من قبل الخصوم عن بُعد لتحقيق الثبات داخل الهدف.
S0055	مهارة استخدام التغذية الراجعة لتحسين عمليات الأمن السيبراني ومنتجاته وخدماته.
S0056	مهارة تحليل مصادر التهديد ذات القوة والاندفاع.
S0057	مهارة التواصل للتعبير عن تأثير النقص في المعرفة الرقابية أو في المعلومات الاستباقية للتهديدات على فاعلية استراتيجية الأمن السيبراني.

رمز المهارة	وصف المهارة
S0058	مهارة التواصل مع جميع مستويات الموظفين.
S0059	مهارة تحديد تهديدات الأمن السيبراني الجديدة في حينه.
S0060	مهارة الاستجابة لحوادث الأمن السيبراني في بيئة الحوسبة السحابية.
S0061	مهارة تطبيق مبادئ الأمن السيبراني والخصوصية لاستيفاء متطلبات المنظمة.
S0062	مهارة استخدام تصنيفات المخاطر لتحقيق الأداء العالي والتكلفة الفعالة بهدف مساعدة المنظمة على إدارة مخاطر الأمن السيبراني.
S0063	مهارة استخدام مقدمي خدمات الأمن السيبراني بفعالية كجزء من قدرات المنظمة.
S0064	مهارة تحديد قضايا الخصوصية والأمن السيبراني المتعلقة بالتواصل مع الأطراف الداخلية والخارجية وسلسلة الإمداد الخاصة بهم.
S0065	مهارة تصميم التكامل بين العمليات التقنية والحلول بما فيها الأنظمة القديمة ولغات البرمجة الحديثة.
S0500	مهارة تأمين الأجهزة الافتراضية.
S0501	مهارة تصميم النماذج و إعداد حالات الاستخدام .
S0502	مهارة صياغة خطط الاختبار.
S0503	مهارة تصميم حلول أمنية متعددة المستويات عبر النطاقات.
S0504	مهارة استخدام منهجيات التصميم.
S0505	مهارة ترجمة المتطلبات التشغيلية إلى احتياجات الحماية.
S0506	مهارة إعداد شبكات فرعية مادية أو منطقية تفصل شبكة الاتصال الموثوقة عن الشبكات غير الموثوقة.
S1000	مهارة إجراء الاستعلامات وتطوير الخوارزميات لتحليل هياكل البيانات.
S1001	مهارة تصحيح أخطاء البرمجيات.
S1002	مهارة إنشاء واستخدام النماذج الرياضية أو الإحصائية.
S1003	مهارة صناعة البرامج التي تصادق وتحلل مدخلات متعددة ومنها مدخلات واجهة أوامر نظام التشغيل ومتغيرات البيئة والمدخلات المتدفقة.

رمز المهارة	وصف المهارة
S1004	مهارة تصميم الضوابط الأمنية المستندة إلى مبادئ ومفاهيم الأمن السيبراني.
S1005	مهارة تطوير قواميس البيانات.
S1006	مهارة تطوير نماذج البيانات.
S1007	مهارة تطوير وتطبيق ضوابط التحكم بالوصول للنُظم الأمنية.
S1008	مهارة تحديد احتياجات التحكم الأمني لنُظم المعلومات والشبكات.
S1009	مهارة تطوير الاستعلامات والتقارير.
S1010	مهارة دمج أدوات اختبار أمن الصندوق الأسود في عملية ضمان الجودة لإصدارات البرمجيات.
S1011	مهارة تقييم قوة التنبؤ لنموذج محدد، وبالتالي قابلية تعميمه.
S1012	مهارة المعالجة المسبقة للبيانات.
S1013	مهارة تحديد الأنماط المخفية أو العلاقات.
S1014	مهارة إجراء تحويلات على التنسيق من أجل إنشاء تمثيل موحد للبيانات.
S1015	مهارة إجراء تحليل للحساسية.
S1016	مهارة تطوير علم أدلة تفهمه الآلات.
S1017	مهارة تطبيق أساليب تحليل الانحدار.
S1018	مهارة تطبيق أساليب تحليل التحول.
S1019	مهارة استخدام الإحصاءات والأساليب الوصفية الأساسية.
S1020	مهارة استخدام أدوات تحليل البيانات.
S1021	مهارة استخدام أدوات تخطيط البيانات.
S1022	مهارة معرفة القيم الشاذة وأساليب التخلص منها.

رمز المهارة	وصف المهارة
S1023	مهارة كتابة البرامج النصية لأتمتة عمليات المنظمة.
S1024	مهارة تطبيق عملية هندسة النُظم بالمنظمة.
S1025	مهارة تصميم تكامل العمليات والحلول التقنية، شاملا النُظم القديمة ولغات البرمجة المعاصرة.
S1026	مهارة تطوير التطبيقات التي يمكنها تسجيل الأخطاء والاستثناءات وعيوب التطبيق والتسجيل، والتعامل معها.
S1027	مهارة استخدام نمذجة التصاميم.
S1028	مهارة إجراء البحث باستخدام جميع المصادر المتوفرة.
S1029	مهارة استخدام أساليب التنقيب عن البيانات وتحليلها.
S1030	مهارة تحديد مصادر أصول بيانات المنظمة، وخصائصها واستخداماتها.
S1031	مهارة تصميم وتطوير النُظم المبنية على الكائنات (object-oriented).
S1032	مهارة استخدام أنظمة التحكم بالإصدارات.
S1033	مهارة نمذجة النشاط لالتقاط المعرفة.
S1034	مهارة تصميم وتطوير البرمجيات والتقنيات والخوارزميات التحليلية المؤتمتة.
S1035	مهارة إجراء البحوث.
S1036	مهارة استخدام أطر تعلم الآلة.
S1037	مهارة استخدام لغات البرمجة الكمية لاستعلامات قاعدة البيانات، ولنمذجة البيانات ولأدوات العرض المرئي.
S1500	مهارة تطوير السياسات التي تعكس غايات المنظمة الاستراتيجية للأعمال و الأمن السيبراني.
S1501	مهارة تقييم صلاحية ومشروعية الموردين والمنتجات.
S1502	مهارة تحديد التقنيات الجديدة باستمرار وتأثيرها المحتمل على متطلبات الأمن السيبراني.
S1503	مهارة استخدام التفكير النقدي للتعرف على التحديات والعلاقات التنظيمية.

رمز المهارة	وصف المهارة
S2000	مهارة تحليل سعة تدفق البيانات عبر الشبكات وخصائص الأداء.
S2001	مهارة استخدام تقنيات إدارة المعرفة.
S2002	مهارة استخدام أدوات إدارة الشبكات لتحليل أنماط حركة مرور البيانات عبر الشبكات.
S2003	مهارة تطوير وتنفيذ برامج ومناهج التدريب التقني.
S2004	مهارة تحديد الثغرات في القدرات التقنية.
S2005	مهارة التحدث مع الآخرين لتوصيل المعلومات بفاعلية.
S2006	مهارة استخدام التقنيات لأغراض تعليمية.
S2007	مهارة تطوير القدرات التقنية من خلال التدريب والتمارين.
S2008	مهارة تطوير معايير التأهيل للأدوار والتخصص للكوادر.
S2009	مهارة تحديد الثغرات في القدرات التقنية.
S2010	مهارة توثيق الحقائق والأفكار بطريقة واضحة ومقنعة ومنظمة.
S2500	مهارة تحديد مقاييس أو مؤشرات أداء النُظم وتنفيذ الإجراءات اللازمة لتحسين أو تصحيح الأداء حسب الحاجة.
S2501	مهارة تطبيق ضوابط الأمن السيبراني المناسبة.
S2502	مهارة تحديد متطلبات البنية التحتية للاختبار والتقييم.
S2503	مهارة التواصل مع العملاء.
S2504	مهارة إدارة أصول الاختبارات ومواردها لضمان إنجاز أحداث الاختبار بكفاءة.
S2505	مهارة إعداد تقارير الاختبار والتقييم.
S2506	مهارة مراجعة السجلات لتحديد أدلة التسلل والاختراق والأنشطة المشبوهة الأخرى.
S2507	مهارة تشخيص ومعالجة الحالات غير الطبيعية في البنية التحتية للدفاع السيبراني وتحديد أسبابها الجذرية.

رمز المهارة	وصف المهارة
S2508	مهارة استخدام نُظم تقنيات المعلومات للموارد البشرية.
S2509	مهارة إجراء مراجعات الأمن السيبراني للنُظم.
S2510	مهارة فهم مبادئ إدارة نظم الشبكات ونماذجه وأساليبه وأدواته.
S2511	مهارة تقييم تصاميم الأمن السيبراني للنُظم.
S2512	مهارة تطوير السياسات التي تحقق أهداف الأمن السيبراني لأنظمة المنظمة، وتطبيقها وتحقيق تكاملها.
S2513	مهارة تخطيط وتنفيذ الأنشطة الإدارية المتعلقة بالأمن السيبراني.
S2514	مهارة تحليل شبكات اتصالات المنظمة من خلال وجهة نظر المهاجم.
S2515	مهارة تحليل حركة البيانات للتعرف على أجهزة الشبكة.
S2516	مهارة تدقيق جدران الحماية والموجهات الشبكية وأنظمة كشف التسلل.
S2517	مهارة تحديد الثغرات والقيود في توفير المعلومات الاستباقية للتهديدات السيبرانية.
S2518	مهارة تحديد مشاكل الأمن السيبراني التي قد يكون لها تأثير على غايات المنظمة.
S2519	مهارة تحديد دلائل محتملة قد تساعد في التحقيق في جرائم الأمن السيبراني.
S2520	مهارة تحديد اللغات واللهجات الإقليمية لمصادر التهديدات.
S2521	مهارة تحديد الأجهزة، التي تعمل ضمن كل مستوى من نماذج البروتوكولات.
S2522	مهارة استخدام تقنيات التحليل الجغرافي المكاني لتحديد مصادر التهديدات وتحديد مكانها.
S2523	مهارة تحديد أولويات المعلومات أثناء عملية الأمن السيبراني.
S2524	مهارة تفسير لغات البرمجة المُجمَّعة والتفسيرية.
S2525	مهارة تفسير البيانات الوصفية المجملة بفعالية وكفاءة.
S2526	مهارة تفسير نتائج أدوات تحليل الشبكة وإعادة بنائها، بفعالية وكفاءة.

رمز المهارة	وصف المهارة
S2527	مهارة تفسير نتائج عملية مسح الثغرات لتحديد ثغرات المنظمة ومستوى حساسيتها.
S2528	مهارة إدارة المعرفة، شاملا أساليب التوثيق التقني.
S2529	مهارة إدارة العلاقات مع العملاء.
S2530	مهارة إعداد الخطط والوثائق ذات الصلة.
S2531	مهارة تحديد أولويات المواد اللغوية الأجنبية المؤمنة أو التي تم الحصول عليها لدعم التحقيق السيبراني.
S2532	مهارة تحديد ومعالجة البيانات وإعدادها لمزيد من التحليل.
S2533	مهارة تحليل التقارير والتوصية بالإجراءات الواجب اتخاذها.
S2534	مهارة مراجعة وتحرير منتجات تقييم الأمن السيبراني.
S2535	مهارة مراجعة وتحرير الخطط المتعلقة بالأمن السيبراني.
S2536	مهارة تفصيل التحليل إلى المستويات اللازمة بناءً على السياسات التنظيمية المتعلقة بالتعامل مع البيانات وتصنيف المواد الحساسة وتوزيعها.
S2537	مهارة جمع المعلومات الاستباقية للتهديدات.
S2538	مهارة تحديد الشواذ الشبكية.
S2539	مهارة كتابة الوثائق التقنية بوضوح وإيجاز.
S2540	مهارة الوصول إلى المعلومات المتعلقة بموارد الأمن السيبراني الداخلية والخارجية الحالية واستخداماتها الحالية وأولوياتها.
S2541	مهارة الوصول إلى قواعد البيانات التي تحوي الوثائق المطلوبة.
S2542	مهارة مراجعة استراتيجيات الشركات أو الوثائق القانونية أو التنظيمية أو السياسة المعمول بها لتحديد القضايا التي تتطلب توضيح أو إجراء.
S2543	مهارة تطوير المتطلبات المناسبة والفعالة لإفادة عملية انتقاء مصادر المعلومات الاستباقية للتهديدات السيبرانية أو نشاط المراقبة.
S2544	مهارة تفسير تقارير مستوى الجاهزية، وعلاقتها بالعمليات التشغيلية، وتأثيرها على جمع المعلومات الاستباقية.

رمز المهارة	وصف المهارة
S2545	مهارة إعداد تقارير واضحة وموجزة، وعروض تقديمية وملخصات.
S2546	مهارة تحليل وتقييم تقارير الشركاء الداخليين والخارجيين.
S3000	مهارة إنشاء وحفظ سياسات الأمن السيبراني بما يتماشى مع غايات الخصوصية بالمنظمة.
S3001	مهارة التفاوض بشأن اتفاقيات المُوَرِّدين.
S3002	مهارة تقييم ممارسات الخصوصية لدى المورد.
S3500	مهارة استخدام منهجيات معالجة الحوادث.
S3501	مهارة جمع البيانات من مجموعة متنوعة من مصادر الأمن السيبراني.
S3502	مهارة تحليل التوجهات.
S4000	مهارة البحث عن المعلومات.
S4001	مهارة تقييم تطبيق معايير التشفير.
S4002	مهارة تحليل قوة التشفير وكسر الشفرات.
S4003	مهارة استخدام خوارزميات وطرق التشفير لحماية البيانات والأنظمة والشبكات.
S4500	مهارة تقييم متانة النُظم والتصاميم الأمنية.
S4501	مهارة تطوير سيناريوهات الاختبار المبنية على العمليات.
S4502	مهارة محاكاة سلوكيات التهديد.
S4503	مهارة اختبار أمن الأنظمة المتكاملة.
S4504	مهارة استخدام أدوات وأساليب اختبار الاختراق.
S4505	مهارة استخدام أساليب الهندسة الاجتماعية.
S4506	مهارة تنفيذ واختبار خطط الطوارئ واستمرارية الأعمال للبنية التحتية للشبكات.

رمز المهارة	وصف المهارة
S4507	مهارة تطوير رؤى متعلقة ببيئة التهديد للمنظمة.
S4508	مهارة استخدام الأدوات والأساليب وإجراءات الاستغلال عن بعد لتحقيق الثبات بداخل الهدف.
S4509	مهارة كتابة جمل برمجية لتجنب الضوابط الأمنية.
S4510	مهارة تنفيذ الخطط والأساليب والإجراءات المضادة.
S4511	مهارة تنفيذ عمليات اختراق وعمليات دفاعية لأغراض التمارين وتقييم واكتشاف الثغرات.
S5000	مهارة تحليل تفريغات الذاكرة لاستخلاص المعلومات.
S5001	مهارة تحديد واستخلاص البيانات المهمة للتحليل الجنائي من وسائط متنوعة.
S5002	مهارة تحديد مكونات النُظم ذات الصلة، وتعديلها والتصرف بها.
S5003	مهارة جمع الأدلة الإلكترونية ومعالجتها وتعبئتها ونقلها وتخزينها؛ لتجنب تبديل البيانات أو فقدانها أو الإضرار المادي بها أو تدميرها.
S5004	مهارة إنشاء محطة عمل للتحليل الجنائي.
S5005	مهارة استخدام أطقم الأدوات الجنائية.
S5006	مهارة التفكيك المادي للحاسبات الشخصية.
S5007	مهارة التحليل المتعمق للشفرات الضارة المستحوذة.
S5008	مهارة تحليل الشفرات غير المألوفة وتصنيفها كضارة أو سليمة.
S5009	مهارة تحليل البيانات غير المستقرة.
S5010	مهارة تحديد أساليب التعتيم.
S5011	مهارة تفسير نتائج برامج كشف الأخطاء البرمجية للتحقق من خطط المعتدي وأساليبه وإجراءاته.
S5012	مهارة تحليل البرمجيات الضارة.
S5013	مهارة إجراء تحليلات على مستوى "البت" (الأرقام الثنائية).

رمز المهارة	وصف المهارة
S5014	مهارة معالجة الدليل الرقمي ويشمل ذلك حمايته وعمل نسخ سليمة قانونيا لاستخدامها كأدلة.
S5015	مهارة استخدام لغة البرمجة C ولغة التجميع منخفضة المستوى ولغة نظام تشغيل لينكس.
S5016	مهارة لغات البرمجة المبنية على النصوص البرمجية.
S5017	مهارة الهندسة العكسية لمعرفة وظيفة وملكية الأدوات التي تعمل عن بُعد.
S5500	مهارة إجراء بحوث غير محددة المرجعية.
S5501	مهارة تحديد وتوصيف جوانب البيئة التشغيلية ذات العلاقة باستراتيجية الأمن السيبراني.
S5502	مهارة التطوير أو التوصية بمناهج تحليلية في المواقف التي تكون فيها المعلومات غير كاملة، أو التي لا توجد لها سابقة.
S5503	مهارة تقييم مصادر محتملة للمعلومات وقيمتها لعملية التحقيق في الأمن السيبراني.
S5504	مهارة تقييم المعلومات للتأكد من موثوقيتها ومصداقيتها وملاءمتها.
S5505	مهارة تقييم أهمية وأولوية المعلومات ومدى الحاجة للاستعجال في استعمالها.
S5506	مهارة تحديد خصائص الشبكة من وجهة نظر المهاجم.
S5507	مهارة تحديد التفسيرات التحليلية البديلة لتقليل النتائج غير المتوقعة.
S5508	مهارة تحديد عناصر التهديد الحساسة.
S5509	مهارة تحديد التهديدات السيبرانية التي تعرض مصالح المنظمة أو أصحاب المصلحة بها للخطر.
S5510	مهارة تحديد وتحليل العلاقات المادية، والوظائفية أو السلوكية لتطوير الفهم للمهاجمين وغاياتهم.
S5511	مهارة التعرف على أساليب الخداع وقطع الخدمة عند استخدامها من قبل المهاجمين أو مرتكبي الجرائم السيبرانية.
S5512	مهارة معرفة الفرص والمعلومات التي تساعد في تطوير استراتيجية الأمن السيبراني أو عمليات التحقيق.
S5513	مهارة معرفة أهمية المعلومات لاستراتيجية الأمن السيبراني أو للتحقيق.
S5514	مهارة معرفة التغييرات المهمة التي تطرأ على أنماط اتصالات المهاجم أو المجرم السيبراني.

رمز المهارة	وصف المهارة
S5515	مهارة مراجعة وتحرير نواتج المعلومات الاستباقية للتهديدات من مصادر مختلفة لدعم اتخاذ القرار في شؤون الأمن السيبراني.
S5516	مهارة صياغة الاستعلامات البسيطة والمعقدة.
S5517	مهارة استخدام أدوات تحليلية متعددة وقواعد البيانات والأساليب.
S5518	مهارة استخدام العديد من محركات البحث والأدوات لإجراء عمليات البحث مفتوحة المصدر.
S5519	مهارة استخدام أدوات تحليل وإعادة بناء الشبكات، وتفسير نتائجها.
S5520	مهارة استخدام مساحات العمل التعاوني الافتراضية وأدواتها بما يتوافق مع سياسات الأمن السيبراني للمنظمة.
S5521	مهارة كتابة منتجات التقييم للأمن السيبراني، ومراجعتها وتحريرها، باستخدام معلومات مستخلصة من مصادر متعددة.
S5522	مهارة وضع الأولويات لسد الفجوات في المعرفة في المنظمة بما يتوافق مع استراتيجية الأمن السيبراني لها، ومع نقاط الضعف والتهديدات الأساسية.
S5523	مهارة مراقبة التهديد أو حالة الثغرات والعوامل البيئية.
S5524	مهارة دقة تقييم آثار الهجمات الناجحة على الأطراف الأخرى بمن فيهم الموردون وغيرهم ممن لديهم بيئات وحلول مشابهه للأمن السيبراني.
S6000	مهارة تصميم النماذج و إعداد حالات الاستخدام في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
S6001	مهارة صياغة خطط الاختبار في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
S6002	مهارة تصميم حلول أمنية متعددة المستويات عبر النطاقات في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
S6003	مهارة استخدام منهجيات التصميم في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
S6004	مهارة ترجمة المتطلبات التشغيلية إلى احتياجات الحماية في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
S6005	مهارة إعداد شبكات فرعية مادية أو منطقية تفصل شبكة الاتصال الموثوقة عن الشبكات غير الموثوقة في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
S6006	مهارة تقييم ضوابط الأمن السيبراني الخاصة ببيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
S6007	مهارة حماية بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية ضد التهديدات السيبرانية.

(جدول ١٢): أوصاف القدرات

رمز القدرة	وصف القدرة
A0001	القدرة على تحليل الثغرات وإعدادات البيانات لتحديد قضايا الأمن السيبراني.
A0002	القدرة على توصيل مفاهيم وممارسات الأمن لاسيبراني بطريقة فعالة.
A0003	القدرة على أداء مسوحات للثغرات ومن ثم تحديد الثغرات من النتائج.
A0004	القدرة على إعداد وتقديم إيجازات خاصة بالأمن السيبراني للمدراء وبقية الموظفين.
A0005	القدرة على إعداد وتوثيق المحتوى التقني بالمستوى المناسب للمتلقين.
A0006	القدرة على تطوير الاستراتيجية والسياسة والوثائق ذات العلاقة لدعم استراتيجية الأعمال والحفاظ على الالتزام للقوانين والتنظيمات والتزامات العقود.
A0007	القدرة على تطوير وتحديث الوثائق الخاصة بالأمن السيبراني وحفظها.
A0008	القدرة على تحديد عيوب البرمجة الأساسية الشائعة ذات العلاقة بالأمن السيبراني على مستوى عالٍ.
A0009	القدرة على تطبيق مفاهيم معمارية أمن الشبكات، شاملا المعمارية والبروتوكولات والمكونات والمبادئ.
A0010	القدرة على تطبيق أدوات تصميم النُظم الآمنة، ومنهجياتها وأساليبها.
A0011	القدرة على تطبيق أدوات تحليل وتصميم النُظم المؤتمتة.
A0012	القدرة على ضمان تطبيق ممارسات الأمن السيبراني عبر كافة مراحل عملية الحيازة أو التصفية.
A0013	القدرة على تصميم الأطر والبنى المعمارية للنظم بما يتوافق مع السياسات الأمنية.
A0014	القدرة على الحصول على البيانات المستخدمة في أنشطة جمع المعلومات الإستباقية للتهديدات السيبرانية والتقييم والتخطيط من مصادرها.
A0015	القدرة على البرهنة على استيعاب المحتوى الحساس للوثائق.
A0016	القدرة على تحديد مدى موثوقية المعلومات وصحتها وصلتها بالموضوع محل الدراسة.
A0017	القدرة على استخدام الخبرة لفهم السياسات المكتوبة بشكل ضعيف.
A0018	القدرة على تركيز جهود البحث لتلبية متطلبات الأمن السيبراني وحاجات صناع القرار بالمنظمة.
A0019	القدرة على العمل في بيئة تعاونية للاستفادة من الخبرات التحليلية والتقنية.

رمز القدرة	وصف القدرة
A0020	القدرة على تحديد النقص في جمع المعلومات الإستباقية للتهديدات وغيرها من معلومات الأمن السيبراني.
A0021	القدرة على فهم وتطبيق الأنظمة واللوائح والسياسات والإرشادات المتعلقة بغايات المنظمة السيبرانية.
A0022	القدرة على إدراك محاولات التدليس في المعلومات التي تم الحصول عليها ومعالجة أثرها وتقديم التقارير والتحليلات المناسبة.
A0023	القدرة على اختيار أساليب المعالجة المناسبة في سياق أهداف وسياسات المنظمة.
A0024	القدرة على إيصال المعلومات التقنية والتخطيطية بحيث تلائم مستوى فهم العميل.
A0025	القدرة على تطبيق التفكير النقدي.
A0026	القدرة على استخدام الوعي بالتغييرات في أنظمة خصوصية المعلومات للتأثير على حركة تكيّف والتزام المنظمة بها.
A0027	القدرة على المحافظة على الوعي بالتغييرات في تقنيات خصوصية المعلومات للتأثير على حركة تكيّف والتزام المنظمة بها.
A0028	القدرة على تطوير المناهج ذات العلاقة وفق المستوى المناسب للمتلقي المستهدف، أو تحديدها أو شراؤها.
A0029	القدرة على تحديد أولويات موارد الأمن السيبراني بكفاءة وفعالية.
A0030	القدرة على المواءمة بين استراتيجيات الأعمال والأمن السيبراني فيما يصب في مصلحة المنظمة.
A0031	القدرة على إدراك التحديات للمنظمة في منظور الأعمال أو المنظور الإداري أو التقني.
A0032	القدرة على ربط مفاهيم الأمن السيبراني الأساسية بآثارها المحتملة على المنظمة.
A0033	القدرة على التواصل الفعال لتقديم رؤى حول بيئة التهديدات للمنظمة، بما يساهم في تحسين وضع إدارة المخاطر لديها.
A0034	القدرة على التقييم والتصدي بفاعلية للحوادث السيبرانية في البيئة السحابية.
A0035	القدرة على تطبيق مبادئ الأمن السيبراني والخصوصية لاستيفاء متطلبات المنظمة.
A0036	القدرة على تطبيق تقنيات الكشف عن التسلل لاكتشاف حالات التسلل الخاصة بالاستضافة أو الشبكة.
A0037	القدرة على العمل مع قيادة المنظمة لتقديم نهج شامل على مستوى المنظمة لمعالجة مخاطر الأمن السيبراني.
A0038	القدرة على العمل مع قيادة المنظمة لإعداد استراتيجية لإدارة المخاطر تتم من خلالها معالجة المخاطر السيبرانية.

رمز القدرة	وصف القدرة
A0039	القدرة على العمل مع قيادة المنظمة لمشاركة المعلومات المتعلقة بمخاطر الأمن السيبراني.
A0040	القدرة على التنسيق مع قيادة المنظمة لتوفير خدمات الإشراف على جميع الأنشطة المتعلقة بإدارة المخاطر.
A0041	القدرة على ضم كافة أصحاب المصلحة على نطاق المنظمة في مجموعة موحدة لمناقشة مخاطر الأمن السيبراني التي يمكن أن تؤثر على المنظمة.
A0042	القدرة على العمل مع قيادة المنظمة لتحديد وضع مخاطر الأمن السيبراني لها بناءً على المخاطر الكلية الناتجة عن تشغيل واستخدام الأنظمة بالمنظمة.
A0043	القدرة على العمل مع موظفي الأمن السيبراني لتقديم المشورة الفعالة والإرشاد لقيادة المنظمة في العديد من شؤون الأمن السيبراني.
A0044	القدرة على تحديد أنظمة المعلومات الحساسة والتي لا تمتلك سوى ضوابط تقنية محدودة للأمن السيبراني.
A0045	القدرة على إدراك أثر التغييرات في الأنظمة أو البيئة أو ضوابط الأمن السيبراني على حجم المخاطر التي تبقى دون معالجة، وعلاقتها بقابلية المنظمة لتحمل المخاطر.
A0046	القدرة على إجراء تحليل متقدم وهندسة عكسية لنصوص الترميز البرمجية المشتبه بمصدرها.
A0500	القدرة على تطبيق الإطار المنتقى من قبل المنظمة لوصف وتحليل وتوثيق معمارية البنية التحتية.
A0501	القدرة على تطبيق أفضل الممارسات عند تنفيذ ضوابط الأمن السيبراني داخل النظام.
A0502	القدرة على تطوير المعمارية لدعم أهداف وغايات المنظمة، والمحافظة عليها.
A0503	القدرة على تحسين النُظم لتلبية متطلبات أداء المنظمة.
A0504	القدرة على العمل مع المهندسين المعماريين للمنظمة، ومهندسي أمن النظم، ومالكي النظم، ومالكي الضوابط، ومسؤولي أمن النظم لتطبيق الضوابط الأمنية كضوابط مشتركة، أو مختلطة أو مخصصة للنظم.
A1000	القدرة على مواءمة تحليل الشفرات البرمجية لتقييم القضايا ذات العلاقة بتطبيق محدد.
A1001	القدرة على استخدام وفهم المفاهيم الرياضية المعقدة.
A1002	القدرة على بناء هياكل بيانات معقدة ولغات البرمجة عالية المستوى.
A1003	القدرة على استخدام أدوات العرض المرئي للبيانات.
A1004	القدرة على تطوير برامج آمنة وفقًا لمنهجيات إطلاق البرامج الآمنة وأدواتها وممارساتها.

رمز القدرة	وصف القدرة
A1005	القدرة على التعاون بفاعلية مع الآخرين.
A1006	القدرة على تطوير نماذج التعلّم الإحصائية والآلية.
A1007	القدرة على تطوير خوارزميات لتحليل البيانات النصية.
A1008	القدرة على تصميم وتطوير النظم المبنية على الكائنات.
A1500	القدرة على دمج عمليات إدارة الأمن السيبراني مع العمليات الاستراتيجية والتشغيلية للأعمال.
A1501	القدرة على التنسيق مع قيادة المنظمة لضمان تطبيق ضوابط الأمن السيبراني في المجالات الخاضعة لسيطرتهم.
A1502	القدرة على دمج متطلبات الأمن السيبراني في عمليات الشراء.
A2000	القدرة على تطوير منهج يدرس كافة المواضيع على المستوى المناسب للفئة المستهدفة.
A2001	القدرة على إعداد وتقديم التدريب لضمان إدراك المستخدمين لسبب الحاجة إلى التزامهم بسياسات وإجراءات أمن النُظم.
A2002	القدرة على تقدير مستوى الفهم ومستوى المعرفة للمتدربين.
A2003	القدرة على تأمين تغذية راجعة فعّالة للطلاب لتحسين تعلُّمهم.
A2004	القدرة على تطبيق مبادئ تعلُّم البالغين.
A2005	القدرة على تطوير مواد تعليمية واضحة ومختصرة وفعالة.
A2006	القدرة على تقييم متطلبات الكوادر والتنبؤ بها لتلبية غايات المنظمة.
A2007	القدرة على تطوير المناهج للاستخدام بداخل بيئة افتراضية.
A2008	القدرة على تطوير المسارات المهنية حسب حاجات المنظمة.
A2009	القدرة على تحديد مدى مصداقية بيانات توجهات القوى العاملة.
A2010	القدرة على تصميم التدريب بما يتوافق مع معايير وسياسات المنظمة.
A2011	القدرة على تشغيل أدوات الشبكة الشائعة.

رمز القدرة	وصف القدرة
A2012	القدرة على تنظيم المناهج التي تغطي مواضيع الأمن السيبراني بالمستوى المناسب للفئة المستهدفة.
A2013	القدرة على تنفيذ أوامر واجهة نظام التشغيل.
A2014	القدرة على تشغيل نُظُم ومنهجيات الاتصال الإلكتروني المختلفة.
A2015	القدرة على القيام بتقييم احتياجات التدريب والتعليم.
A2500	القدرة على تحديد صلاحية بيانات التوجهات التقنية.
A2501	القدرة على تطبيق ضوابط إدارة مخاطر سلسلة الإمداد.
A2502	القدرة على الإجابة عن الأسئلة ذات العلاقة بالأمن السيبراني بصفة واضحة وموجزة.
A2503	القدرة على طرح الأسئلة لاستيضاح القضايا ذات العلاقة بالأمن السيبراني.
A2504	القدرة على توصيل المعلومات ذات العلاقة بالأمن السيبراني بوضوح واختصار عند الكتابة.
A2505	القدرة على تنسيق المناقشات الجماعية الصغيرة بكفاءة وفاعلية.
A2506	القدرة على تصميم تقييمات للأمن السيبراني ذات مصداقية.
A2507	القدرة على تحليل بيانات الاختبارات للأمن السيبراني بأهلية تامة.
A2508	القدرة على جمع بيانات الاختبار والتأكد منها والتحقق من مصداقيتها.
A2509	القدرة على تحديد العلاقات بين اثنين فأكثر من مصادر بيانات الأمن السيبراني والتي قد تبدو للوهلة الأولى أنها غير متصلة.
A2510	القدرة على الاستفادة من أفضل الممارسات من الجهات الخارجية عند التعامل مع حوادث الأمن السيبراني.
A2511	القدرة على تحديد علاقة ومعنى البيانات ونتائج اختبارات الأمن السيبراني.
A2512	القدرة على التعاون بشكل فعال مع الزملاء والشركاء والموردين.
A2513	القدرة على التعاون بفاعلية عبر الفرق الافتراضية والهياكل الإدارية المصفوفية.
A2514	القدرة على تقييم وتحليل وتحويل كميات كبيرة من البيانات إلى تقارير مدمجة وعالية الجودة.

رمز القدرة	وصف القدرة
A2515	القدرة على استهداف وتوسيع نطاق الوصول الشبكي عن طريق إجراء تحليل مناسب وجمع البيانات المعنية.
A2516	القدرة على العمل بفاعلية في بيئة ديناميكية سريعة الوتيرة وكثيرة التغير.
A2517	القدرة على تحديد الشركاء الخارجيين ذوي المصلحة المشتركة بالأمن السيبراني.
A2518	القدرة على تحديد ووصف ثغرات الأمن السيبراني بالمنظمة.
A2519	القدرة على تحديد الأدوات والمنهجيات التي يمكن من خلالها استهداف ثغرات المنظمة.
A2520	القدرة على فهم وترجمة متطلبات أصحاب المصلحة للأمن السيبراني إلى ضوابط وأنشطة تشغيلية.
A2521	القدرة على تفسير وفهم البيئات المعقدة سريعة التطور.
A2522	القدرة على المشاركة كعضو من فرق افتراضية حسب الحاجة.
A2523	القدرة على معرفة التحيزات الفكرية، التي قد تؤثر على التحليل، ومعالجتها.
A2524	القدرة على فهم غايات المنظمة وآثار ضوابط الأمن السيبراني على تلك الغايات.
A2525	القدرة على استخدام مصادر معلومات متعددة لإفادة جهود الأنشطة ذات العلاقة بالأمن السيبراني.
A2526	القدرة على العمل عبر الإدارات ووحدات الأعمال لتنفيذ مبادئ وبرامج الخصوصية في المنظمة.
A2527	القدرة على العمل عبر الإدارات ووحدات الأعمال لضمان المواءمة بين غايات المنظمة للخصوصية وللأمن السيبراني.
A2528	القدرة على ضمان تقديم تقارير عن نشاطات الأمن السيبراني إلى أصحاب المصلحة المناسبين في المنظمة.
A2529	القدرة على إدراك وشرح أهمية التدقيق في تطبيق سياسات الأمن السيبراني.
A2530	القدرة على إيصال المشاكل التقنية المعقدة من منظور الأمن السيبراني.
A3000	القدرة على مراقبة وتقييم التأثير المحتمل للتقنيات الناشئة على التشريعات واللوائح وسياسات الأمن السيبراني والوثائق ذات العلاقة.
A3001	القدرة على تحديد ما إذا كان حادث أمن سيبراني قد انتهك مبدأ الخصوصية أو القانون، مما يتطلب اتخاذ إجراءات قانونية محددة.
A3002	القدرة على تأليف بيان خصوصية مناسب بناءً على القوانين الحالية.

رمز القدرة	وصف القدرة
A3500	القدرة على تحليل البرمجيات الضارة.
A3501	القدرة على تفسير المعلومات التي تم جمعها من خلال أدوات الشبكة.
A4000	القدرة على تنفيذ أساليب وطرق وإجراءات التجميع الشبكي.
A4001	القدرة على تنفيذ إجراءات التجميع اللاسلكية.
A4002	القدرة على ضمان اتخاذ كافة العوامل اللازمة للنجاح في قرارات عمليات الأمن السيبراني المتخذة من قبل قيادة المنظمة.
A4003	القدرة على ضمان مشاركة أصحاب المصلحة عندما تتخذ قيادة المنظمة قرارات تشغيلية ذات علاقة بالأمن السيبراني.
A4500	القدرة على تطبيق هياكل لغات البرمجة شاملا مراجعة نصوص الشفرات البرمجية المصدرية ومنطقها.
A4501	القدرة على إعداد اختبارات الاختراق وتقييم الثغرات وفقًا لدور المنظمة وعملياتها التشغيلية وهيكلها والتهديدات السيبرانية التي تتعرض لها.
A4502	القدرة على حل المشاكل التقنية المعقدة والتعبير عنها لغير موظفي تقنية المعلومات.
A4503	القدرة على تقديم تقييم تقني فعّال لمخاطر جميع التقنيات المعمول بها بالمنظمة محل التقييم أو الاختبار.
A4504	القدرة على إجراء اختبار الاختراق بما يتماشى مع أفضل الممارسات وسياسات المنظمة.
A4505	القدرة على كتابة التقارير التقنية التي تشمل تقييم للمخاطر التشغيلية والحلول المقترحة لمجالات المشاكل المعرفة.
A5000	القدرة على فك تشفير تجميعات البيانات الرقمية.
A5001	القدرة على إجراء التحليلات الجنائية في جميع أنظمة التشغيل المستخدمة في المنظمة.
A5002	القدرة على إيجاد وتصفح الشبكة العنكبوتية المظلمة لتحديد مواقع الأسواق والمنتديات بها.
A5003	القدرة على فحص الوسائط الرقمية على كافة منصات نُظم التشغيل المستخدمة في المنظمة.
A5004	القدرة على قراءة وفهم شفرات لغة التجميع.

رمز القدرة	وصف القدرة
A5500	القدرة على التعبير بوضوح عن متطلبات المعلومات الاستباقية لتهديدات الأمن السيبراني على هيئة أسئلة بحثية جيدة الصياغة ومتغيرات تتّبُع البيانات لأغراض تتبع الاستعلامات.
A5501	القدرة على تطوير مناهج وحلول قائمة على التحليل للمشكلات التي تكون فيها المعلومات غير مكتملة أو تلك التي لم يحدث مثيل لها سابقاً.
A5502	القدرة على التفكير كممثلي التهديدات.
A6000	القدرة على تطوير المعمارية لدعم أهداف وغايات المنظمة، والمحافظة عليها في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
A6001	القدرة على تحسين النُظم لتلبية متطلبات أداء المنظمة في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
A6002	القدرة على العمل مع المهندسين المعماريين للمنظمة، ومهندسي أمن النظم، ومالكي النظم، ومالكي الضوابط، ومسؤولي أمن النظم لتطبيق الضوابط الأمنية كضوابط مشتركة، أو مختلطة أو مخصصة للنظم في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
A6003	القدرة على إعداد شبكات فرعية مادية أو منطقية تفصل الشبكات الموثوقة عن الشبكات الأخرى غير الموثوقة في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
A6004	القدرة على تطبيق الأساليب والأدوات في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية ضد التهديدات السيبرانية.
A6005	القدرة على تطبيق الأساليب والأدوات للكشف عن الاختراقات في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.
A6006	القدرة على تطبيق الأساليب والأدوات للتصدي لحوادث الأمن السيبراني في بيئات تقنية المعلومات وأنظمة التحكم الصناعي والتقنيات التشغيلية.

الهيئة الوطنية للأمن السيبـراني
National Cybersecurity Authority