الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الإطار السعودي لكوادر الأمن السيبراني (سيوف)

THE SAUDI CYBERSECURITY WORKFORCE FRAMEWORK

(SCyWF – 1.5: 2026)

إشارة المشاركة: شفاف
تصنيف الوثيقة: عام

بسم الله الرحمن الرحيم

بروتوكول الإشارة الضوئية (TLP):

يستخدم هذا البروتوكول 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 أكان ذلك من داخل الجهة أم خارجها؛ خارج النطاق المحدد للاستلام.

برتقالي + مشدد (مشاركة في نفس الجهة)

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب.

برتقالي (مشاركة محدودة)

المستلم يمكنه مشاركة المعلومات في الجهة نفسها مع الأشخاص المعنيين فحسب. ومن يتطلب الأمر منه اتخاذ إجراء يخص المعلومة.

أخضر (مشاركة في نفس المجتمع)

المستلم يمكنه مشاركة المعلومات مع آخرين في الجهة نفسها، أو جهة أخرى على علاقة معهم أو في القطاع نفسه؛ ولا يسمح بتبادلها أو نشرها من خلال القنوات العامة.

شفاف (غير محدود)

قائمة المحتويات

قائمة الرسوم التوضيحيّة

قائمة الجداول

١. المقدّمة

تعمل الهيئة الوطنية للأمن السيبراني على حماية الفضاء السيبراني للمملكة، ويتطلب ذلك كوادر وطنية مؤهلة في مجال الأمن السيبراني يكونون قادرين على تنفيذ جميع أعمال الأمن السيبراني. وبموجب الأمر الملكي الكريم ذو الرقم ٦٨٠١، والتاريخ ٣١ أكتوبر ٢٠١٧، الذي تضمن اختصاصات الهيئة الوطنية للأمن السيبراني نص على: 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. لهذا طورت الهيئة الوطنية للأمن السيبراني الإطار السعودي لكوادر الأمن السيبراني (سيوف) ليكون مرجعًا أساسيًا في هذا الجانب.

١,١ نظرة عامة

يُعنى 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 المهمات والمعارف والمهارات. ويتمثل الهدف الرئيسي من هذا الإطار تقديم دليل مرجعي لإعداد كوادر الأمن السيبراني وتطويرها، واستقطابها وإدارتها، ويقدم الإطار مرجعًا موحدًا لتحسين التواصل، وتطوير المحتوى في أنشطة تأهيل وإدارة الكوادر. ويساعد أيضاً في ربط مخرجات التعلم لبرامج التعليم والتدريب، بالمعارف والمهارات المطلوبة، للأدوار الوظيفية المختلفة في مجال الأمن السيبراني.

وتوصي الهيئة كافة الجهات، بتبني هذا الإطار واستخدامه؛ لضمان مواءمة هياكل الكوادر، والأنشطة الخاصة بها 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.

ونظرًا لطبيعة الأمن السيبراني المتغيرة والمتطورة باستمرار، فسوف يجري مراجعة محتويات هذا الإطار وتحديثه بصفة دورية.

٢,١ المنهجية والهيكل

جرى تطوير الإطار السعودي لكوادر الأمن السيبراني، استناداً إلى أفضل الممارسات العالمية والمعايير الدولية الرصينة، بما يعزز من كفاءته وجودته في التطبيق وبما يتلاءم مع احتياج كوادر الأمن السيبراني في المملكة العربية السعودية. ويُنظم هذا الإطار أعمال الأمن السيبراني، بشكل هرمي يتكون من فئات، ومجالات تخصص، وأدوار وظيفية، وفيما يلي تعريف للأدوار الوظيفية، ومجالات الاختصاص، والفئات ضمن هيكل هذا الإطار:

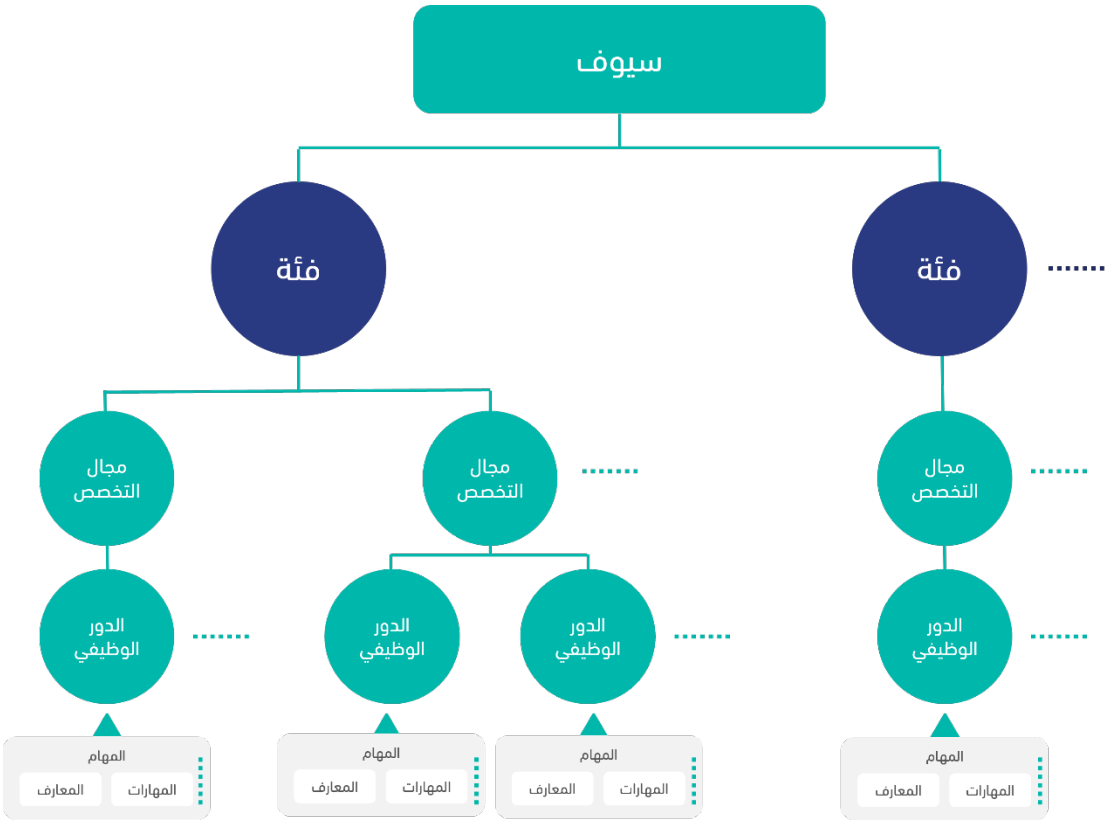
الدور الوظيفي: هو مجموعة من مهمات الأمن السيبراني، المطلوب أداؤها في وظيفة أمن سيبراني محددة. يجري تعريف الدور الوظيفي من خلال مجموعة من المهمات المطلوب أداؤها في سياق هذا الدور الوظيفي، وكذلك قائمة المعارف والمهارات المطلوبة لهذا الدور. ويحوي ("الملحق أ") قائمة بجميع الأدوار الوظيفية في الإطار السعودي لكوادر الأمن السيبراني.

مجال التخصص: هو مجموعة من الأدوار الوظيفية، التي تخدم وظيفة محددة في مجال الأمن السيبراني، وتتشارك في المهمات والمعارف والمهارات المطلوبة.

الفئة: هي مجموعة من مجالات التخصص، والأدوار الوظيفية المرتبطة بها، والتي تخدم مجموعة من وظائف الأمن السيبراني المرتبطة 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 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، قدرًا مناسبًا من الوعي بمخاطر الأمن السيبراني وممارساته المثلى.

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



شكل ١: هيكل الإطار السعودي لكوادر الأمن السيبراني

٢ تصنيف الإطار السعودي لكوادر الأمن السيبراني

١,٢ الفئات ومجالات التخصص في الإطار السعودي لكوادر الأمن السيبراني

يعمل الإطار على تصنيف عمل كوادر الأمن السيبراني في خمس فئات، واثني عشر مجال تخصص، وأربعين دورًا وظيفيًا. ويضمن هذا التصنيف اتباع نهج منظم ومتسق؛ لتحديد وإدارة وظائف الأمن السيبراني في مختلف المجالات، وتمثل كل فئة ومجال تخصص مجموعة من المسؤوليات، والوظائف ذات الصلة بالأمن السيبراني، المصممة لمواءمة الأدوار الوظيفية، مع احتياجات المنظمة، والاحتياجات الوطنية المحددة للأمن السيبراني.

يبين (الشكل ٢) كل الفئات ومجالات التخصص والأدوار الوظيفية في الإطار السعودي لكوادر الأمن السيبراني.

شكل ٢: تصنيف الإطار السعودي لكوادر الأمن السيبراني

الجدول ١ يصف فئات الإطار السعودي لكوادر الأمن السيبراني. ويلحظ أن كل فئة لديها مُعرّف فريد، يتكون من الأحرف الأولى من اسم الفئة باللغة الإنجليزية (مثال: يشير الرمز PD 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".

الفئة	الوصف
معمارية الأمن السيبراني والبحث والتطوير (CARD)	تنفيذ أعمال التصميم والمعمارية والبحث والتطوير في مجال الأمن السيبراني.
القيادة وتطوير الكوادر (LWD)	قيادة فرق عمل الأمن السيبراني وأعمالها وتطويرها، وتطوير كوادر الأمن السيبراني.
الحوكمة والمخاطر والالتزام والقوانين (GRCL)	تطوير سياسات الأمن السيبراني للمنظمة، وحوكمة هياكله وعملياته، وإدارة مخاطره، وضمان الالتزام بمتطلبات إدارة مخاطر الأمن السيبراني للمنظمة، والمتطلبات القانونية ذات الصلة.
الحماية والدفاع (PD)	تحديد تهديدات شبكات تقنية المعلومات وثغرات نظمها وتحليلها ومراقبتها والحد منها، وإدارتها، واستخدام التدابير الدفاعية، والمعلومات التي جرى الحصول عليها من مصادر متنوعة؛ للإبلاغ عن الأحداث والاستجابة للحوادث.
نظم التحكم الصناعية والتقنيات التشغيلية (ICS/OT)	تنفيذ أعمال الأمن السيبراني لنظم التحكم الصناعية، والتقنيات التشغيلية.

جدول ١: فئات الإطار السعودي لكوادر الأمن السيبراني

الجدول ٢ يصف 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 ("الملحق أ").

الفئة	مجال التخصص	الوصف
معمارية الأمن السيبراني والبحث والتطوير (CARD)	معمارية الأمن السيبراني (CA)	تصميم نظم الأمن السيبراني ومكوناته التابعة لنُظم 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 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 لجميع نظم 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 والنُظم والشبكات من التهديدات السيبرانية.
	تقييم الثغرات (VA)	اختبار نظم وشبكات تقنية المعلومات، وتقييم التهديدات والثغرات ذات الصلة.
	الاستجابة للحوادث (IR)	التحقيق في الحوادث السيبرانية وتحليلها والاستجابة لها.
	إدارة التهديدات (TM)	جمع وتحليل المعلومات عن التهديدات والبحث عن التهديدات غير المكتشفة، وتقديم رؤى قابلة للتطبيق لدعم اتخاذ القرار في الأمن السيبراني.
نظم التحكم الصناعية والتقنيات التشغيلية (ICS/OT)	نظم التحكم الصناعية والتقنيات التشغيلية (ICS/OT)	القيام بأعمال الأمن السيبراني المتعلقة بالحوكمة وإدارة المخاطر، ومتابعة الالتزام، والتصميم والتطوير، وتنفيذ عمليات التشغيل والإدارة، والحماية والدفاع في نظم التقنيات التشغيلية التي تشمل نظم التحكم الصناعية (ICS) ونُظم التحكم الإشرافي ونُظم حيازة البيانات (SCADA).

جدول ٢: مجالات التخصص للإطار السعودي لكوادر الأمن السيبراني

٢,٢ المهمات والمعارف والمهارات ومجالات الكفاءة في الإطار السعودي لكوادر الأمن السيبراني

يحدد الإطار العناصر الأساسية لكل دور وظيفي من حيث المهمات والمعارف والمهارات:

- **المهمة:** مجموعة من الأنشطة التي يجب إتمامها كجزء من دور وظيفي محدد.
- **المعرفة:** مجموعة البيانات والحقائق والمعلومات والنظريات والمفاهيم والقضايا المتعلقة بموضوع معين.
- **المهارة:** القدرة على تطبيق المعرفة واستخدام الأدوات والأساليب اللازمة لتنفيذ المهمة.

جرى إعداد نصوص بيانات المهمات والمعارف والمهارات في الإطار السعودي لكوادر الأمن السيبراني استنادًا إلى أفضل الممارسات العالمية وجرى تنقيحها لتتلاءم مع احتياجات كوادر الأمن السيبراني في المملكة العربية السعودية؛ ويحتوي "الملحق ب" على قائمة كاملة ببيانات المهمات والمعارف والمهارات في الإطار السعودي لكوادر الأمن السيبراني.

كما يقدم هذا الإصدار من الإطار السعودي لكوادر الأمن السيبراني مجالات الكفاءات لتحسين الإطار من خلال معالجة مجالات الأمن السيبراني المهمة.

- **مجال الكفاءة:** مجموعة من المعارف والمهارات ذات الصلة، وتمثل القدرة على أداء المهمات ضمن مجال معين.

تركز مجالات الكفاءة على مواءمة قدرات الكوادر مع تحديات الواقع، وضمان قدرة المنظمات والمختصين على الاستجابة بفاعلية لاحتياجات الأمن السيبراني المتغيرة. كما ستساعد مجالات الكفاءة المؤسسات على:

- التركيز على المجالات المتخصصة لمعالجة التحديات الفريدة للأمن السيبراني
- مواءمة برامج تدريب الكوادر والشهادات التأهيلية مع متطلبات القطاع
- دعم التطور في المسار الوظيفي من خلال تقديم مسارات منظمة للتطور الوظيفي

على الرغم من أن مجالات الكفاءة تثري تصنيف الإطار السعودي لكوادر الأمن السيبراني، إلا أنه ليس من الضروري أن يتقن المختصون في الأمن السيبراني جميع التفاصيل في كل مجال من مجالات الكفاءة المرتبطة بأدوارهم، وستكون هذه المجالات بمثابة إطار إرشادي للتركيز على الخبرات ذات الصلة. يمكن الاطلاع على وصف مفصل لمجالات الكفاءة والأدوار الوظيفية المرتبطة بها في "الملحق ج"

٣,٢ الأدوار الوظيفية في فئة معمارية الأمن السيبراني والبحث والتطوير (CARD)

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

الرقم	مجال التخصص	الدور الوظيفي	معرّف الدور الوظيفي	الوصف
١	معمارية الأمن السيبراني (CA)	مصمم معمارية الأمن السيبراني	CARD-CA-001	تصميم نظم وشبكات الأمن السيبراني، والإشراف على إعداداتها، وتطويرها وتنفيذها.
٢		أخصائي الحوسبة السحابية الآمنة	CARD-CA-002	تصميم نظم 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 نظم المعلومات، وتطويره، واختباره، وتقييمه في جميع مراحل تطوير تلك النُظم.
٤		مطور الأمن السيبراني	CARD-CRD-002	تطوير برمجيات الأمن السيبراني، وتطبيقاته، ونظمه، ومنتجاته.
٥		مُقيّم البرمجيات الآمنة	CARD-CRD-003	تقييم أمن تطبيقات الحاسب، أو برمجياته، أو شفراته، أو برامجه؛ مع تقديم نتائج قابلة للتنفيذ.
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 خوارزميات ونظم لاستخلاص استنتاجات ومعارف الأمن السيبراني وتنفيذها، وذلك من مصادر متعددة، لمجموعة بيانات واسعة النطاق.
٨		أخصائي الذكاء الاصطناعي للأمن السيبراني	CARD-CRD-006	استخدام نماذج الذكاء الاصطناعي، وتقنياته (شاملاً أساليب التعلم الآلي) لتصميم خوارزميات ونظم لأتمتة مهمات الأمن السيبراني وتنفيذها، وتحسين كفاءتها، وفاعليتها.

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

٤,٢ الأدوار الوظيفية في فئة القيادة وتطوير الكوادر (LWD)

الجدول ٤ يصف الأدوار الوظيفية في فئة القيادة وتطوير الكوادر.

الرقم	مجال التخصص	الدور الوظيفي	معرّف 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، والإستراتيجيات 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 أكان ذلك على مستوى فريق، أم على مستوى وحدة أو وظيفة على المستوى المؤسسي.
١١		مستشار الأمن السيبراني	LWD-L-003	تقديم الرأي والمشورة لقيادة المنظمة، وقادة الأمن السيبراني وفرقه في موضوعات الأمن السيبراني.
١٢	تطوير الكوادر (WD)	مدير الموارد البشرية للأمن السيبراني	LWD-WD-001	تطوير الخطط والإستراتيجيات والإرشادات داخل المنظمة؛ لدعم تطوير كوادر الأمن السيبراني وإدارتها.
١٣		مُطوّر المناهج التعليمية للأمن السيبراني	LWD-WD-002	تطوير برامج التعليم والتدريب والوعي بالأمن السيبراني، وتخطيطها مع تنسيقها وتقييمها، بما في ذلك الدورات، والمحتوى، وأساليب تقديمها، وتقنيات ذلك؛ حسب الاحتياجات التدريبية والتعليمية.
١٤		مدرب الأمن السيبراني	LWD-WD-003	تعليم الأفراد وتدريبهم، وتطويرهم، واختبارهم في موضوعات الأمن السيبراني، وزيادة وعيهم بشأنها؛ لتشجيعهم على اتباع سلوكيات آمنة.

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

٥,٢ الأدوار الوظيفية في فئة الحوكمة والمخاطر والالتزام والقوانين(GRCL)

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

الرقم	مجال التخصص	الدور الوظيفي	معرّف 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 المنظمة وإجراءاتها، وكذلك وفقا للقوانين 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		مُدقّق الأمن السيبراني	GRCL-GRC-005	تصميم عمليات التدقيق الخاصة بالأمن السيبراني وتنفيذها، وإدارتها؛ لتقييم مدى امتثال 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 بقوانين وأنظمة الأمن السيبراني.
٢١		أخصائي حماية البيانات	GRCL-LDP-002	تحليل مخاطر حماية البيانات، وضمان الامتثال للأنظمة والتشريعات ذات الصلة، والإشراف على تنفيذ السياسات والإجراءات الخاصة بحماية البيانات، ودعم استجابة المنظمة للحوادث المتعلقة بحماية البيانات.

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

٦,٢ الأدوار الوظيفية في فئة الحماية والدفاع (PD)

الجدول ٦ يصف الأدوار الوظيفية في فئة الحماية والدفاع.

الرقم	مجال التخصص	الدور الوظيفي	معرّف الدور الوظيفي	الوصف
٢٢	الدفاع (D)	محلل دفاع الأمن السيبراني	PD-D-001	استخدام البيانات التي جرى 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 الأجهزة والبرمجيات المستخدمة للدفاع وحماية النُظم والشبكات من التهديدات السيبرانية، وتنصيبها، وصيانتها، وتشغيلها، والإشراف عليها.
٢٤		أخصائي الأمن السيبراني	PD-D-003	تقديم الدعم العام للأمن السيبراني، والمساعدة في مهمات الأمن السيبراني.
٢٥	الحماية (P)	أخصائي التشفير	PD-P-001	تطوير نظم التشفير وخوارزمياته، وتقييمها، وتحليلها، وتحديد ثغراتها، وسبل تحسينها؛ بما في ذلك التقنيات الكمية.
٢٦		أخصائي إدارة الهوية والوصول	PD-P-002	إدارة هوية الأفراد والجهات، وصلاحيات وصولهم إلى الموارد؛ من خلال تطبيق نظم وعمليات التعريف والتحقق والتصريح.
٢٧		محلل أمن النُظم	PD-P-003	تطوير أمن النُظم، واختباره، وصيانته، وتحليل أمن العمليات، والنُظم المتكاملة.
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 المستويات، ضد الثغرات المعروفة.
٢٩		أخصائي اختبار الاختراقات	PD-VA-002	أداء محاولات اختراق مصرح لها، لنظم 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		أخصائيّ 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 بشأن تقنيات الوقاية منها، والاستجابة للحوادث الناتجة عنها.
٣٤	إدارة التهديدات (TM)	محلّل معلومات التهديدات السيبرانية	PD-TM-001	جمع معلومات عن التهديدات السيبرانية، من مصادر مختلفة، وتحليلها؛ لتكوين فهم وإدراك عميقين، للتهديدات السيبرانية، والخطط، والأساليب، والإجراءات، التي يتّبعها المخترقون؛ لاستنباط المؤشرات وتوثيقها، التي 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.

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

٧,٢ الأدوار الوظيفية في فئة نظم التحكم الصناعية والتقنيات التشغيلية (ICS/OT)

الجدول ٧ يصف الأدوار الوظيفية في فئة نظم التحكم الصناعية والتقنيات التشغيلية.

الرقم	مجال التخصص	الدور الوظيفي	معرّف الدور الوظيفي	الوصف
٣٦	نظم التحكم الصناعية والتقنيات التشغيلية (ICS/OT)	مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية	ICSOT-ICSOT-001	تصميم نظم الأمن السيبراني وشبكاته في بيئة نظم التحكم الصناعية والتقنيات التشغيلية، والإشراف على ضبط إعداداتها، وتطويرها وتنفيذها.
٣٧		أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية	ICSOT-ICSOT-002	فحص الأجهزة والبرمجيات المستخدمة للدفاع وحماية النُظم والشبكات من التهديدات السيبرانية، في بيئة نظم التحكم الصناعية والتقنيات التشغيلية، وتنصيبها، وصيانتها، وتشغيلها، والإشراف عليها.
٣٨		محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية	ICSOT-ICSOT-003	استخدام البيانات التي جرى جمعها من مجموعة متنوعة، من أدوات الأمن السيبراني؛ لتحليل الأحداث الواقعة في بيئة نظم التحكم الصناعية، والتقنيات التشغيلية؛ بهدف الكشف عن تهديدات الأمن السيبراني، والتعامل معها.
٣٩		أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية	ICSOT-ICSOT-004	تحديد مخاطر الأمن السيبراني وتقييمها وإدارتها في بيئة نظم التحكم الصناعية، والتقنيات التشغيلية، وتقييم فاعلية ضوابط الأمن السيبراني القائمة وتحليلها، وتقديم الملحوظات والتوصيات بشأنها؛ بناءً على تلك التقييمات.
٤٠		أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية	ICSOT-ICSOT-005	مباشرة حوادث الأمن السيبراني، وتحليلها والاستجابة لها، في بيئة نظم التحكم الصناعية والتقنيات التشغيلية.

جدول ٧: الأدوار الوظيفية في فئة نظم التحكم الصناعية والتقنيات التشغيلية (ICS/OT)

للاطلاع على المعارف والمهارات المطلوبة لكل دور وظيفي، المهمات المرتبطة به يُرجى الاطلاع على "الملحق أ".

٣ الملاحق

١,٣ الملحق أ: تفاصيل الدور الوظيفي

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

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مصمم معمارية الأمن السيبراني
معرّف الدور الوظيفي	CARD-CA-001
الفئة	معمارية الأمن السيبراني والبحث والتطوير
مجال التخصص	معمارية الأمن السيبراني
وصف الدور الوظيفي	تصميم نظم وشبكات الأمن السيبراني، والإشراف على إعداداتها وتطويرها وتنفيذها.
مجالات الكفاءة	تصميم معمارية الأمن السيبراني (CA017)
المهمات	T0036, T0037, T0043, T0134, T0507, T0508, T0511, T0512, T0514, T0515, T0516, T0517, T0518, T0519, T0520, T0523, T0524, T0525, T0526, T0527, T0529, T0530, T0534, T0535, T0540, T0541, T1052, T2511, T4502
المعارف	K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0014, K0016, K0017, K0020, K0021, K0022, K0025, K0027, K0028, K0034, K0035, K0042, K0053, K0057, K0058, K0062, K0074, K0093, K0101, K0109, K0111, K0112, K0120, K0121, K0146, K0149, K0175, K0176, K0177, K0185, K0186, K0187, K0188, K0189, K0190, K0191, K0504, K0507, K0509, K0510, K0512, K0513, K0514, K0516, K0517, K0518, K1015, K1036, K1505, K4000, K4030, K5503
المهارات	S0001, S0003, S0008, S0016, S0021, S0023, S0027, S0038, S0039, S0040, S0051, S0058, S0061, S0064, S0071, S0072, S0074, S0075, S0082, S0092, S0501, S0503, S0504, S0505, S1004, S1008, S1034, S1046, S1060, S1504, S1506, S2010, S2501, S2556

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي الحوسبة السحابية الآمنة
معرّف الدور الوظيفي	CARD-CA-002
الفئة	معمارية الأمن السيبراني والبحث والتطوير
مجال التخصص	معمارية الأمن السيبراني
وصف الدور الوظيفي	تصميم نظم الحوسبة السحابية الآمنة، وتنفيذها وتشغيلها؛ مع تطوير سياسات السحابة الآمنة.
مجالات الكفاءة	إدارة الهوية والتحكم بالوصول (CA001)، أمن الحوسبة السحابية (CA002)، أمن الاتصالات (CA003)، أمن أنظمة التشغيل (CA005)، أمن البيانات وإدارتها (CA007)
المهمات	T0003, T0004, T0005, T0011, T0013, T0014, T0015, T0040, T0103, T0107, T0134, T0139, T0500, T0502, T0503, T0504, T0505, T0511, T0524, T0526, T0527, T0532, T0533, T0536, T0542, T0543, T1007, T1016, T1017, T1049, T1050, T1112, T1529, T4011, T4509
المعارف	K0001, K0003, K0004, K0005, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0014, K0019, K0025, K0035, K0042, K0044, K0045, K0046, K0048, K0054, K0056, K0061, K0062, K0084, K0085, K0106, K0113, K0121, K0124, K0126, K0128, K0132, K0136, K0178, K0180, K0188, K0189, K0190, K0191, K0207, K0208, K0500, K0516, K0517, K0518, K0519, K0521, K2001, K2511, K3008, K3009, K5524, K5532
المهارات	S0003, S0004, S0012, S0018, S0019, S0021, S0039, S0040, S0055, S0058, S0060, S0061, S0062, S0064, S0065, S0071, S0073, S0077, S0078, S0085, S0086, S0088, S0106, S0504, S1505, S2010, S2501, S2512, S2533, S2546, S2550

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي تطوير أمن النُظم
معرّف الدور الوظيفي	CARD-CRD-001
الفئة	معمارية الأمن السيبراني والبحث والتطوير
مجال التخصص	البحث والتطوير في الأمن السيبراني
وصف الدور الوظيفي	تصميم أمن نظم المعلومات، وتطويره، واختباره، وتقييمه في جميع مراحل تطوير تلك النُظم.
مجالات الكفاءة	تطوير البرمجيات الآمنة (CA014)، اختبار الأمن السيبراني (CA024)
المهمات	T0004, T0013, T0014, T0022, T0040, T0089, T0096, T0103, T0107, T0138, T0158, T0507, T0508, T0511, T0524, T0526,T0527, T0534, T0536, T1004, T1007, T1008, T1015, T1016, T1026, T1027, T1029, T1031, T1033, T1034, T1038, T1042, T1044, T1048, T1049, T1050, T1079, T1081, T1087, T1088, T1089, T1090, T1091, T1102, T1104, T1105, T1111, T1112, T1126
المعارف	K0001, K0002, K0003, K0004, K0005, K0014, K0016, K0020, K0022, K0024, K0027, K0035, K0042, K0045, K0046, K0048, K0049, K0054, K0056, K0057, K0058, K0061, K0062, K0063, K0076, K0080, K0092, K0093, K0095, K0097, K0100, K0101, K0111, K0113, K0124, K0125, K0149, K0170, K0172, K0173, K0176, K0178, K0180, K0182, K0183, K0185, K0186, K0187, K0205, K0210, K0516, K0517, K0518, K0520, K1005, K1006, K1007, K1008, K1009, K1011, K1024, K1036, K1041, K1047, K1048, K1050, K1051, K1052, K1053, K1057, K1064, K1068, K3508, K4008, K4027, K5012, K5040, K5503, K5524, K5536, K6012
المهارات	S0001, S0003, S0004, S0008, S0012, S0018, S0023, S0028, S0039, S0040, S0053, S0055, S0058, S0061, S0062, S0064, S0065, S0066, S0068, S0070, S0071, S0072, S0073, S0074, S0083, S0084, S0086, S0091, S0092, S0106, S0504, S0505, S0508, S0509, S1000, S1004, S1041, S1049, S1052, S1053, S1060, S1504, S1505, S2010, S2512, S2533, S2546, S2550, S5503

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مطور الأمن السيبراني
معرّف 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 ونظمه ومنتجاته.
مجالات الكفاءة	تطوير البرمجيات الآمنة (CA014)
المهمات	T0013, T0014, T0035, T0039, T0040, T0089, T0091, T0107, T0511, T0527, T0536, T1002, T1003, T1005, T1006, T1009, T1010, T1011, T1013, T1014, T105, T1023, T1029, T1031, T1049, T1050, T1051, T1052, T1054, T1055, T1058, T1062, T1071, T1075, T1078, T1081, T1085, T1091, T1092, T1102, T1104, T1105, T1108, T1109, T1110, T1115, T1116, T1123, T5060
المعارف	K0001, K0002, K0003, K0004, K0005, K0015, K0022, K0024, K0030, K0035, K0039, K0042, K0045, K0051, K0054, K0056, K0063, K0069, K0074, K0076, K0080, K0083, K0093, K0095, K0124, K0125, K0126, K0128, K0136, K0146, K0147, K0170, K0171, K0172, K0173, K0174, K0175, K0178, K0180, K0182, K0183, K0185, K0186, K0187, K0188, K0189, K0194, K0205, K0518, K1000, K1005, K1008, K1011, K1012, K1013, K1014, K1015, K1017, K1021, K1023, K1048, K1050, K1053, K1057, K1059, K1064, K1068, K1504, K1514, K3008, K3009, K3508, K6012
المهارات	S0001, S0003, S0004, S0017, S0018, S0036, S0038, S0039, S0040, S0045, S0047, S0048, S0053, S0055, S0058, S0061, S0064, S0065, S0066, S0067, S0068, S0070, S0073, S0077, S0106, S0504, S0505, S0508, S1000, S1001, S1002, S1003, S1004, S1007, S1008, S1010, S1047, S1052, S1055, S1056, S1057, S1059, S1060, S1504, S1505, S2010, S2018, S2533, S2546, S2550

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مُقيّم البرمجيات الآمنة
معرّف 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، أو برمجياته، أو شفراته، أو برامجه؛ مع تقديم نتائج قابلة للتنفيذ.
مجالات الكفاءة	إدارة الهوية والتحكم بالوصول (CA001)، تطوير البرمجيات الآمنة (CA014)، اختبار الأمن السيبراني (CA024)
المهمات	T0013, T0014, T0039, T0040, T0107, T0138, T0511, T0527, T0536, T1005, T1006, T1009, T1012, T1013, T1016, T1024, T1025, T1029, T1031, T1035, T1040, T1041, T1043, T1046, T1049, T1050, T1054, T1055, T1076, T1078, T1081, T1092, T1104, T1105, T1115, T1116, T1123, T1127, T1131, T1133, T1134, T4011
المعارف	K0003, K0004, K0005, K0015, K0022, K0030, K0035, K0039, K0042, K0045, K0051, K0054, K0056, K0062, K0069, K0074, K0076, K0080, K0083, K0093, K0100, K0112, K0113, K0117, K0136, K0146, K0153, K0171, K0175, K0186, K0187, K0188, K0189, K0205, K0213, K0214, K1012, K1013, K1014, K1015, K1017, K1021, K1023, K1024, K1037, K1047, K1048, K1050, K3008, K3009, K5503
المهارات	S0001, S0003, S0004, S0018, S0036, S0038, S0040, S0047, S0048, S0055, S0058, S0061, S0062, S0065, S0066, S0067, S0068, S0070, S0073, S0077, S0078, S0082, S0086, S0091, S0092, S0106, S0504, S0505, S1004, S1007, S1008, S1010, S1039, S1053, S1056, S1057, S1504, S2547, S2549, S2550, S5526

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	باحث الأمن السيبراني
معرّف 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.
مجالات الكفاءة	جميع الكفاءات ذات الصلة بمجالات البحث.
المهمات	T0009, T0013, T0040, T0052, T0068, T0089, T0090, T0103, T0107, T0163, T0164, T0529, T1007, T1016, T1019, T1045, T1050, T1051, T1057, T1058, T1073, T1074, T1091, T1093, T1128, T1129, T1135, T5500, T6006, T6010
المعارف	K0003, K0004, K0005, K0009, K0017, K0035, K0042, K0044, K0054, K0056, K0069, K0073, K0074, K0080, K0092, K0093, K0094, K0095, K0096, K0097, K0098, K0100, K0112, K0113, K0135, K0136, K0153, K0159, K0170, K0174, K0175, K0181, K0185, K0186, K0187, K0188, K0214, K1030, K1031, K1032, K1034, K1035, K1038, K1047, K1058, K1060, K1062, K1063, K1514, K3008, K3009, K5524
المهارات	S0001, S0003, S0004, S0018, S0039, S0040, S0045, S0049, S0051, S0055, S0058, S0061, S0077, S0078, S0082, S0086, S0090, S0092, S0504, S1002, S1007, S1024, S1028, S0068, S1504, S2010, S2512, S2533, S2546, S2550, S5500

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي علم البيانات للأمن السيبراني
معرّف 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 خوارزميات ونظم لاستخلاص استنتاجات ومعارف الأمن السيبراني وتنفيذها، وذلك من مصادر متعددة، لمجموعة بيانات واسعة النطاق.
مجالات الكفاءة	أمن البيانات وإدارتها (CA007)، أمن الذكاء الاصطناعي (CA015)
المهمات	T0009, T0068, T0080, T0083, T0084, T1000, T1001, T1020, T1034, T1039, T1059, T1060, T1083, T1098, T1100, T1101, T1106, T1061, T1062, T1064, T1066, T1069, T1070, T1071, T1072, T1502, T5031
المعارف	K0003, K0004, K0005, K0014, K0015, K0018, K0019, K0020, K0035, K0039, K0042, K0045, K0049, K0051, K0054, K0059, K0069, K0074, K0075, K0076, K0080, K0105, K0107, K0108, K0113, K0124, K0126, K0133, K0156, K0169, K0170, K0186, K0187, K0188, K0189, K0193, K0197, K1000, K1001, K1002, K1003, K1005, K1010, K1016, K1021, K1025, K1027, K1028, K1036, K1045, K1047, K1049, K1052, K1054, K1064, K1065, K1066, K1067, K1069, K1511, K3000, K3001, K3008, K3009, K3010, K3011, K3012, K4009, K4011, K4012, K5008, K5017, K5034, K5503
المهارات	S0017, S0018, S0026, S0029, S0030, S0031, S0032, S0045, S0055, S0058, S0066, S0067, S0069, S0070, S0077, S0078, S0086, S0091, S0100, S1000, S1002, S1005, S1006, S1009, S1017, S1018, S1019, S1020, S1021, S1022, S1023, S1029, S1030, S1034, S1042, S1043, S1053, S1054, S1055, S1056, S1057, S1058, S1060, S1504, S2522, S2525, S2541, S2546, S3501, S4006, S5503, S5516, S5517, S5525, S5527

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي الذكاء الاصطناعي للأمن السيبراني
معرّف 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 (شاملاً أساليب التعلم الآلي) لتصميم خوارزميات ونظم لأتمتة مهمات الأمن السيبراني وتنفيذها، وتحسين كفاءتها، وفاعليتها.
مجالات الكفاءة	أمن الذكاء الاصطناعي (CA015)
المهمات	T0083, T0134, T1060, T1061, T1064, T1071, T1072, T1094, T1096, T1098, T1099, T1100, T1101, T1130, T3033
المعارف	K0001, K0002, K0003, K0004, K0005, K0014, K0015, K0018, K0030, K0035, K0051, K0059, K0074, K0119, K0186, K0187, K0188, K0189, K1021, K1028, K1039, K1040, K1041, K1043, K1058, K3009, K3010, K5503
المهارات	S0017, S0058, S0066, S0067, S1000, S1002, S1020, S1023, S1031, S1032, S1034, S1035, S1036, S1055, S1059, S1060

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

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	رئيس إدارة الأمن السيبراني
معرّف 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، والإستراتيجيات والموارد والأنشطة ذات العلاقة، وتقديم المرئيات لقيادة المنظمة؛ حيال أساليب الإدارة الفعّالة لمخاطر الأمن السيبراني للمنظمة.
مجالات الكفاءة*	إدارة برامج الأمن السيبراني (CA012) ، استمرارية الأعمال والتعافي من الكوارث (CA023)
المهمات	T0001, T0002, T0011, T0017, T0042, T0043, T0053, T0061, T0085, T0095, T0105, T0108, T0112, T0127, T0128, T0130, T0137, T0140, T0153, T0165, T1501, T1503, T1511, T1513, T1528, T1529, T1531, T1534, T1535, T1541, T1546, T1547, T1548, T1549, T2000, T2003, T2007, T2008, T2009, T2060, T2526, T4509
المعارف	K0001, K0003, K0004, K0005, K0008, K0009, K0021, K0029, K0034, K0035, K0037, K0044, K0054, K0061, K0064, K0069, K0073, K0074, K0080, K0092, K0093, K0100, K0113, K0128, K0205, K0213, K0214, K1506, K1509, K1515, K2013, K2014, K2021, K2022, K2023, K2024, K5503, K5524
المهارات	S0004, S0018, S0051, S0055, S0058, S0059, S0077, S0078, S0079, S0080, S0082, S0086, S0088, S0505, S1500, S1501, S1502, S1504, S1506, S1507, S1510, S2501, S2512, S0087, S2542, S2546, S2550, S2555

* بالإضافة إلى الحد الأدنى من الفهم والإلمام في جميع مجالات الكفاءة الأخرى

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مدير الأمن السيبراني
معرّف 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 أكان ذلك على مستوى فريق، أم على مستوى وحدة أو وظيفة على المستوى المؤسسي.
مجالات الكفاءة	جميع الكفاءات ذات الصلة، بالمجال الذي يتولّون إدارته.
المهمات	T0001, T0002, T0011, T0016, T0017, T0023, T0042, T0048, T0053, T0059, T0061, T0063, T0074, T0108, T0112, T0128, T0130, T0137, T0140, T0153, T1502, T1503, T1504, T1505, T1513, T1516, T1518, T1520, T1521, T1522, T1523, T1524, T1525, T1526, T1527, T1528, T1542, T1543, T1545, T1546, T1550, T1551, T1552, T1553, T1554, T2000, T2007, T2008, T4509
المعارف	K0001, K0003, K0004, K0005, K0008, K0019, K0021, K0024, K0029, K0031, K0034, K0035, K0037, K0043, K0044, K0046, K0056, K0061, K0064, K0069, K0073, K0074, K0090, K0092, K0113, K0124, K0125, K0126, K0128, K0133, K0159, K0169, K0176, K0186, K0187, K0188, K1500, K1501, K1504, K1505, K1506, K1509, K1511, K1512, K1513, K1514, K1515, K2013, K2027, K2030, K2501, K2511, K2513, K3009, K5503, K5524
المهارات	S0004, S0009, S0040, S0077, S0078, S0079, S0080, S0082, S0085, S0086, S1007, S1500, S2555, S3001 S1501, S1504, S1505, S1506, S1507, S1510, S1511, S2555, S3001

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مستشار الأمن السيبراني
معرّف الدور الوظيفي	LWD-L-003
الفئة	القيادة وتطوير الكوادر
مجال التخصص	القيادة
وصف الدور الوظيفي	تقديم الرأي والمشورة لقيادة المنظمة، وقادة الأمن السيبراني وفرقه في موضوعات الأمن السيبراني.
مجالات الكفاءة	جميع الكفاءات ذات الصلة بالمجال، الذي يقدمون المشورة بشأنه.
المهمات	T0001, T0002, T0003, T0011, T0016, T0017, T0042, T0048, T0053, T0112, T0128, T0130, T0138, T0139, T0140, T1501, T1503, T1511, T1525, T1528, T1529, T1537, T1538, T1539, T1555, T1556, T1557, T2003, T2526, T4509
المعارف	K0001, K0002, K0003, K0004, K0005, K0008, K0016, K0019, K0021, K0029, K0031, K0034, K0035, K0037, K0044, K0046, K0056, K0061, K0064, K0069, K0073, K0090, K0092, K0093, K0124, K0128, K0133, K0159, K0169, K0176, K0186, K0187, K0188, K0189, K0205, K0214, K1505, K1506, K1509, K1510, K1511, K1512, K1513, K1514, K1515, K2027, K2511, K2513, K3009, K5524
المهارات	S0004, S0018, S0051, S0055, S0058, S0075, S0077, S0078, S0079, S0080, S0082, S0085, S0086, S0087, S0088, S0090, S0505, S1048, S1049, S1500, S1501, S1502, S1504, S1506, S2546, S2548, S2550, S2555

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مدير الموارد البشرية للأمن السيبراني
معرّف الدور الوظيفي	LWD-WD-001
الفئة	القيادة وتطوير الكوادر
مجال التخصص	تطوير الكوادر
وصف الدور الوظيفي	تطوير الخطط والإستراتيجيات والإرشادات داخل المنظمة؛ لدعم تطوير كوادر الأمن السيبراني وإدارتها.
مجالات الكفاءة	التدريب والتوعية بشأن الأمن السيبراني (CA020)
المهمات	T0002, T0017, T0046, T0078, T0082, T0085, T0086, T0088, T0095, T0103, T0108, T0109, T0112, T0140, T0160, T0161, T0162, T0163, T0164, T0165, T1503, T1510, T1511, T1516, T1527, T1528, T1529, T1530, T1535, T1541, T1542, T1543, T2003, T2006, T2007, T2009, T2026, T2027, T2028, T2031, T2032, T2033, T2034, T2035, T2038, T2039, T2040, T2047, T2059, T2062, T2063, T2065, T2069
المعارف	K0001, K0003, K0004, K0005, K0035, K0058, K0061, K0074, K0080, K0092, K0186, K0187, K0188, K0189, K0215, K0216, K1501, K2002, K2011, K2013, K2014, K2022, K2023, K2024, K2025, K2026, K2027, K2029, K2030, K2031, K2032
المهارات	S0018, S0055, S0058, S0077, S0078, S0087, S0088, S1500, S1504, S2008, S2015, S2016, S2017, S2512, S2546, S2549, S2550

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مُطوّر المناهج التعليمية للأمن السيبراني
معرّف الدور الوظيفي	LWD-WD-002
الفئة	القيادة وتطوير الكوادر
مجال التخصص	تطوير الكوادر
وصف الدور الوظيفي	تطوير برامج التعليم والتدريب والوعي بالأمن السيبراني، وتخطيطها مع تنسيقها وتقييمها، بما في ذلك الدورات، والمحتوى، وأساليب تقديمها، وتقنيات ذلك؛ حسب الاحتياجات التدريبية والتعليمية.
مجالات الكفاءة*	التدريب والتوعية بشأن الأمن السيبراني (CA020)
المهمات	T0052, T0082, T0085, T0163, T0165, T1528, T2004, T2005, T2010, T2011, T2012, T2013, T2014, T2015, T2016, T2017, T 2018, T2019, T2020, T2021, T2022, T2024, T2028, T2029, T2049, T2050, T2051, T2053, T2054, T2055, T2056, T2057, T2058, T2061, T2064, T2066, T2070, T2072, T2073, T2075, T2076
المعارف	K0001, K0002, K0003, K0004, K0005, K0035, K0044, K0061, K0074, K0080, K0186, K0187, K0188, K0189, K1061, K2000, K2002, K2004, K2005, K2007, K2009, K2011, K2012, K2013, K2023, K2024, K2025, K2026, K2027, K2028, K2034, K2036, K2037
المهارات	S0001, S0004, S0018, S0023, S0026, S0034, S0051, S0055, S0058, S0069, S0075, S0077, S0078, S0086, S0092, S1504, S2001, S2003, S2004, S2006, S2010, S2012, S2014, S2017, S2026, S2028, S2029, S2542, S2546, S2550, S5503

* بالإضافة إلى مجالات الكفاءة المتعلقة بالمناهج الدراسية التي يقومون بتطويرها

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مدرب الأمن السيبراني
معرّف 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، وزيادة وعيهم بشأنها؛ لتشجيعهم على اتباع سلوكيات آمنة.
مجالات الكفاءة*	التدريب والتوعية بشأن الأمن السيبراني (CA020)
المهمات	T0083, T0084, T1528, T2002, T2005, T2010, T2011, T2012, T2013, T2014, T2015, T2016, T2017, T2018,T2019, T2020, T2022, T2024, T2028, T2029, T2036, T2040,T2042, T2044, T2046,T2048, T2049, T2050, T2051, T2054,T2055, T2061, T2064, T2066, T2067, T2068, T2071, T2074, T2075, T2077
المعارف	K0001, K0002, K0003, K0004, K0005, K0007, K0035, K0044, K0074, K0080, K0133, K0186, K0187, K0188, K0189, K0190, K2000, K2001, K2002, K2004, K2005, K2007, K2009, K2010, K2020, K2021, K2028, K2033, K2034, K2035, K2036, K2037
المهارات	S0001, S0004, S0017, S0018, S0019, S0021, S0023, S0026, S0027, S0034, S0041, S0051, S0055, S0058, S0069, S0077, S0086, S0092, S1502, S1504, S2001, S2002, S2003, S2006, S2018, S2019, S2020, S2021, S202 S2023, S2024, S2025, S2027, S2028, S2501, S2542, S2546, S2549, S2550, S3501, S4504, S4505, S5012, S5503

* بالإضافة إلى مجالات الكفاءة المتعلقة بموضوع التدريب الذي يقدمونه

٣.١.٣ مجموعة الفئة: الحوكمة والمخاطر والالتزام والقوانين (GRCL)

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي مخاطر الأمن السيبراني
معرّف 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 المنظمة وإجراءاتها، وكذلك وفقا للقوانين والأنظمة ذات العلاقة.
مجالات الكفاءة	تحليل المخاطر الأمنية (CA008) ، أمن سلسلة الإمداد (CA006)، استمرارية الأعمال والتعافي من الكوارث (CA023)
المهمات	T0001, T0003, T0006, T0011, T0012, T0013, T0014, T0015, T0017, T0037, T0039, T0042, T0043, T0053, T0105, T0107, T0108, T0127, T0128, T0130, T0132, T0133, T0138, T0139, T0140, T0146, T1524, T1529, T1545, T2000, T2060, T2500, T2507, T2513, T2526, T2528, T2529, T2530, T2536, T4509
المعارف	K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0009, K0021, K0029, K0035, K0037, K0073, K0074, K0080, K0081, K0083, K0092, K0107, K0160, K0166, K0167, K0186, K0187, K0188, K0189, K5503, K6005
المهارات	S0012, S0018, S0040, S0044, S0055, S0056, S0057, S0058, S0062, S0075, S0077, S0078, S0079, S0080, S0081, S0082, S0088, S0089, S0091, S1007, S1504, S1506, S1507, S2546, S2550, S2553, S2555, S4507

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي الالتزام في الأمن السيبراني
معرّف 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.
مجالات الكفاءة	تنظيمات الأمن السيبراني والالتزام (CA021)، حماية البيانات (CA022)
المهمات	T0003, T0019, T0022, T0023, T0063, T0082, T0111, T0139, T2500, T2501, T2504, T2506, T2509, T2514, T2515, T2519, T2522, T2523, T2524, T2525, T2527, T2529, T2530, T2534, T2542, T2543, T2544, T3031, T3039, T3052, T3056
المعارف	K0001, K0002, K0003, K0004, K0005, K0008, K0035, K0074, K0186, K0187, K0188, K0189, K0190, K2506, K2507, K2509, K2510, K2512, K5503
المهارات	S0018, S0051, S0055, S0058, S0061, S0062, S0073, S0077, S0078, S0087, S0088, S1500, S1504, S1506, S1507, S2014, S2512, S2542, S2546, S2550

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي سياسات الأمن السيبراني
معرّف 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.
مجالات الكفاءة	تنظيمات الأمن السيبراني والالتزام (CA021)، حماية البيانات (CA022)
المهمات	T0011, T0017, T0046, T0082, T0085, T0086, T0088, T0095, T0103, T0108, T0109, T0140, T0160 , T0161, T0162, T0163, T0164, T0165, T1020, T1525, T1546, T2006, T2028, T2510, T3005, T3007, T3008, T3037
المعارف	K0001, K0002, K0003, K0004, K0005, K0008, K0018, K0019, K0021, K0029, K0037, K0074, K0092, K0169, K0186, K0187, K0188, K0189, K0195, K0200, K1514, K2013, K2014, K2024, K2516, K3010, K3011, K4016, K4513,K5003, K5006, K5007, K5037, K5503
المهارات	S0075, S0077, S0081, S0087, S0088, S1500, S1504, S1506, S1507, S2512, S2513, S2530, S3000, S5503

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مُقيّم ضوابط الأمن السيبراني
معرّف الدور الوظيفي	GRCL-GRC-004
الفئة	الحوكمة، والمخاطر، والالتزام، والقوانين
مجال التخصص	الحوكمة، والمخاطر، والالتزام
وصف الدور الوظيفي	تحليل ضوابط الأمن السيبراني، وتقييم فاعليتها.
مجالات الكفاءة	تحليل المخاطر الأمنية (CA008)
المهمات	T0036, T0037, T0039, T0043, T0050, T0053, T0061, T0074, T0079, T0136, T0146, T0153, T2503, T2505, T2507, T2508, T2509, T2511, T2512, T2514, T2516, T2521, T2531, T2532, T2533, T2535
المعارف	K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0009, K0010, K0011, K0013, K0016, K0017, K0019, K0020, K0021, K0022, K0028, K0029, K0031, K0035, K0037, K0042, K0044, K0074,K0080, K0084, K0085, K0086, K0092, K0093, K0100, K0113, K0124, K0125, K0126, K0147, K0153, K0169, K0176, K0180, K0183, K0185, K0186, K0187, K0188, K0189, K0190, K0213, K0214, K1017, K1511, K2501, K2502, K2509, K2514, K2515, K5503, K5536
المهارات	S0001, S0004, S0018, S0023, S0026, S0036, S0037, S0040, S0044, S0045, S0046, S0047, S0048, S0050, S0051, S0055, S0058, S0061, S0064, S0068, S0070, S0073, S0077, S0078, S0096, S0102, S0103, S0505, S1008, S1009, S1020, S1029, S1058, S1500, S1502, S1504, S2502, S2504, S2506, S2507, S2509, S2512, S2513, S2517, S2521, S2523, S2524, S2525, S2541, S2542, S2543, S2544, S2546, S2547, S2548, S2549, S2550, S2551, S2552, S2554, S5526

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مُدقّق الأمن السيبراني
معرّف الدور الوظيفي	GRCL-GRC-005
الفئة	الحوكمة، والمخاطر، والالتزام، والقوانين
مجال التخصص	الحوكمة، والمخاطر، والالتزام
وصف الدور الوظيفي	تصميم عمليات التدقيق الخاصة بالأمن السيبراني، وتنفيذها وإدارتها؛ بهدف تقييم مدى التزام المنظمة بالمتطلبات، والسياسات، والمعايير، والضوابط المعمول بها، وإعداد تقارير التدقيق، وتقديمها للأطراف ذات الصلاحية.
مجالات الكفاءة	تحليل المخاطر الأمنية (CA008)
المهمات	T0024, T0037, T0039, T0041, T0043, T0048, T0053, T0060, T0061, T0074, T0109, T0136, T0147, T0153, T0160, T0161,T0162, T0163, T0164, T2505, T2508, T2509, T2510, T2511, T2535, T3057
المعارف	K0011, K0013, K0021, K0022, K0028, K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0074, K0080, K0084, K0085, K0086, K0109, K0029, K0035, K0037, K0042, K0044, K0056, K0069, K0187, K0188, K0189, K0113, K0124, K0125, K0126, K0128, K0133, K0134, K0144, K0186, K5503 K2516, K0205, K0209, K0211, K2501, K2505, K2506, K2507, K2509,K5503
المهارات	S0001, S0004, S0019, S0023, S0026, S0028, S0036, S0040, S0048, S0051, S0055, S0058, S0061, S0064, S0068, S0073, S0076, S0077, S0078, S0082, S0086, S0092, S0096, S0103, S1058, S1500, S1504, S1505, S2003, S2010, S2023, S2024, S2501, S2502, S2504, S2506, S2526, S2527, S2533, S2537, S2540, S2541, S2542, S2543, S2546, S2548, S2549, S2525, S2557, S2558, S3000, S5503

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي قانون الأمن السيبراني
معرّف 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 بقوانين وأنظمة الأمن السيبراني.
مجالات الكفاءة	تنظيمات الأمن السيبراني والالتزام (CA021)
المهمات	T0003, T0019, T0063, T0088, T0147, T1501, T2514, T2526, T2544, T3001, T3002, T3004, T3005, T3007, T3008, T3010, T3052, T5009
المعارف	K0002, K0003, K0004, K0005, K0044, K0065, K0074, K0081, K0084, K0125, K0126, K0128, K0187, K0188, K0189, K0198, K0199, K0200, K0201, K0202, K2509, K2510, K2513, K3000, K3012, K3509, K5015, K5032, K5503
المهارات	S0058, S0077, S0088, S1504, S3003, S3004, S3005

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي حماية البيانات
معرّف الدور الوظيفي	GRCL-LDP-002
الفئة	الحوكمة، والمخاطر، والالتزام، والقوانين
مجال التخصص	القوانين وحماية البيانات
وصف الدور الوظيفي	تحليل مخاطر حماية البيانات، وضمان الامتثال للأنظمة والتشريعات ذات الصلة، والإشراف على تنفيذ السياسات والإجراءات الخاصة بحماية البيانات، ودعم استجابة المنظمة للحوادث المتعلقة بحماية البيانات.
مجالات الكفاءة	حماية البيانات (CA022)
المهمات	T0019, T0023, T0063, T0127, T2514, T2521, T2522, T3013, T3014, T3019, T3023, T3025, T3026, T3029, T3030, T3031, T3033, T3036, T3037, T3038, T3039, T3041, T3042, T3049, T3057
المعارف	K0002, K0003, K0004, K0005, K0008, K0029, K0035, K0074, K0187, K0188, K0189, K2506, K2507, K2509, K2512, K3005, K3008, K3009, K3010, K5503
المهارات	S0018, S0055, S0058, S0061, S0064, S0077, S0078, S0087, S0088, S1504, S2546, S2550, S3000, S3002

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

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	محلل دفاع الأمن السيبراني
معرّف الدور الوظيفي	PD-D-001
الفئة	الحماية والدفاع
مجال التخصص	الدفاع
وصف الدور الوظيفي	استخدام البيانات التي جرى استخلاصها من مجموعة أدوات الدفاع السيبراني؛ لتحليل الأحداث الواقعة، داخل المنظمة، بهدف الكشف عن التهديدات، والتعامل معها.
مجالات الكفاءة	إدارة الهوية والتحكم بالوصول (CA001)، أمن الاتصالات (CA003)، أمن البيانات وإدارتها (CA٠٠٧)، إدارة الثغرات الأمنية (CA013)، المعلومات الاستباقية للتهديدات السيبرانية (CA019)، اختبار الأمن السيبراني (CA024)
المهمات	T0009, T0015, T0025, T0028, T0029, T0037, T0040, T0044, T0054, T0055, T0056, T0064, T0067, T0068, T0069, T0070, T0071, T0072, T0073, T0075, T0076, T0097, T0098, T0100, T0101, T0102, T0107, T0111, T0122, T0138, T0141, T0151, T0152, T0155, T0156, T0157, T3503, T3504, T5057
المعارف	K0001, K0002, K0003, K0004, K0005, K0007, K0013, K0014, K0016, K0017, K0020, K0024, K0031, K0035, K0042, K0043, K0044, K0045, K0046, K0049, K0053, K0054, K0058, K0063, K0064, K0065, K0068, K0069, K0070, K0072, K0074, K0076, K0077, K0078, K0084, K0086, K0087, K0101, K0102, K0103, K0104, K0113, K0117, K0124, K0125, K0126, K0134, K0136, K0137, K0159, K0176, K0177, K0179, K0184, K0186, K0187, K0188, K0189, K0190, K0191, K0192, K0198, K0199, K0200, K0201, K0202, K0205, K0206, K0212, K0213, K0214, K3506, K3507, K3508, K5503
المهارات	S0001, S0006, S0009, S0012, S0015, S0023, S0033, S0040, S0041, S0046, S0048, S0056, S0057, S0061, S0063, S0069, S0092, S0097, S0101, S0104, S1506, S1508, S1509, S2002, S2520, S2522, S3501, S3502, S4006, S5012, S5018, S5026, S5503, S5524, S5525, S5532

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي البنية التحتية للأمن السيبراني
معرّف الدور الوظيفي	PD-D-002
الفئة	الحماية والدفاع
مجال التخصص	الدفاع
وصف الدور الوظيفي	فحص الأجهزة والبرمجيات المستخدمة للدفاع وحماية النُظم والشبكات من التهديدات السيبرانية، وتنصيبها، وصيانتها، وتشغيلها، والإشراف عليها.
مجالات الكفاءة	أمن الحوسبة السحابية (CA002)، أمن الاتصالات (CA003)، أمن أنظمة التشغيل (CA005)، أمن الأجهزة والبرمجيات الثابتة (CA016)
المهمات	T0005, T0038, T0057, T0147, T1543, T3502, T3506, T3507, T3508, T3511, T4023
المعارف	K0001, K0002, K0003, K0004, K0005, K0017, K0019, K0024, K0035, K0043, K0046, K0063, K0064, K0074, K0084, K0100, K0104, K0119, K0147, K0159, K0177, K0179, K0184, K0186, K0187, K0188, K0206, K0212, K0519, K1052, K3502, K3509, K5012
المهارات	S0001, S0005, S0008, S0009, S0014, S0016, S0021, S0022, S0035, S0038, S0040, S0061, S0065, S0068, S0069, S0071, S0082, S0085, S0092, S0096, S0106, S0506, S1007, S1047, S2011, S2507, S3500, S4006, S5526, S5532

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي الأمن السيبراني
معرّف الدور الوظيفي	PD-D-003
الفئة	الحماية والدفاع
مجال التخصص	الدفاع
وصف الدور الوظيفي	تقديم الدعم العام للأمن السيبراني، والمساعدة في مهمات الأمن السيبراني.
مجالات الكفاءة	إدارة الهوية والتحكم بالوصول (CA001)، أمن الاتصالات (CA003)، أمن أنظمة التشغيل (CA005)، أمن البيانات وإدارتها (CA007)
المهمات	T0005, T0009, T0026, T0028, T0102, T0113, T0142, T3500, T3503, T3504
المعارف	K0001, K0004, K0005, K0007, K0009, K0013, K0014, K0017, K0019, K0020, K0024, K0031, K0035, K0043, K0045, K0051, K0053, K0063, K0068, K0074, K0084, K0104, K0119, K0159, K0188, K0189, K0190, K0191, K0192, K0193, K0194, K0206, K5536
المهارات	S0001, S0002, S0009, S0012, S0019, S0021, S0022, S0023, S0027, S0028, S0035, S0062, S0068, S0083, S0084, S0085, S0092, S0093, S0094, S0095, S0104, S1052, S2011, S2526, S3501, S3502, S4006, S5025, S5532

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي التشفير
معرّف الدور الوظيفي	PD-P-001
الفئة	الحماية والدفاع
مجال التخصص	الحماية
وصف الدور الوظيفي	تطوير نظم التشفير وخوارزمياته، وتقييمها، وتحليلها، وتحديد ثغراتها، وسبل تحسينها؛ بما في ذلك التقنيات الكمية.
مجالات الكفاءة	إدارة الهوية والتحكم بالوصول (CA001)، التشفير (CA004)، أمن البيانات وإدارتها (CA007)
المهمات	T0010, T0016, T0091, T0096, T0158, T4000, T4008, T4021, T4022, T4034
المعارف	K0001, K0002, K0003, K0004, K0005, K0007, K0010, K0014, K0015, K0016, K0017, K0018, K0024, K0028, K0029, K0030, K0035, K0039, K0042, K0044, K0046, K0051, K0053, K0074, K0175, K0176, K0186, K0187, K0188, K0189, K0190, K0192, K0194, K1000, K1011, K1060, K4017, K4020, K4030
المهارات	S0004, S0016, S0038, S0039, S0061, S0066, S0067, S1002, S1055, S1056, S1057, S4001, S4002, S4003, S4006, S4009, S5022

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي إدارة الهوية والوصول
معرّف الدور الوظيفي	PD-P-002
الفئة	الحماية والدفاع
مجال التخصص	الحماية
وصف الدور الوظيفي	إدارة هوية الأفراد والجهات، وصلاحيات وصولهم إلى الموارد؛ من خلال تطبيق نظم وعمليات التعريف والتحقق والتصريح.
مجالات الكفاءة	إدارة الهوية والتحكم بالوصول (CA001)
المهمات	T0100, T1049, T3508, T4016, T4017, T4018, T4019, T4024, T4025, T4026, T4027, T4028, T4029, T4035, T4036
المعارف	K0001, K0002, K0003, K0004, K0005, K0007, K0013, K0024, K0028, K0035, K0042, K0049, K0059, K0074, K0085, K0106, K0107, K0112, K0124, K0125, K0126, K0133, K0144, K0156, K0190, K0191, K0194, K0197, K0207, K0208, K0211, K4000, K4001, K4002, K4004, K4016, K4028, K4029, K4030, K5503
المهارات	S0005, S0061, S0096, S1007, S1504, S4000, S4005, S4007, S4008, S5025

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	محلل أمن النُظم
معرّف الدور الوظيفي	PD-P-003
الفئة	الحماية والدفاع
مجال التخصص	الحماية
وصف الدور الوظيفي	تطوير أمن النُظم، واختباره، وصيانته، وتحليل أمن العمليات، والنُظم المتكاملة.
مجالات الكفاءة	إدارة الهوية والتحكم بالوصول (CA001)، أمن الاتصالات (CA003)، التشفير (CA004)، أمن أنظمة التشغيل (CA005)، أمن البيانات وإدارتها (CA007)، إدارة الثغرات الأمنية (CA013)، اختبار الأمن السيبراني (CA024)
المهمات	T0004, T0005, T0015, T0036, T0040, T0043, T0050, T0074, T0079, T0097, T0098, T0100, T0102, T0107, T0111, T0122, T0138, T0146, T0159, T1025, T1026, T4000, T4001, T4002, T4004, T4005, T4011, T4013, T4014, T4015, T4023, T4030, T4031, T4032, T4033
المعارف	K0001, K0002, K0003, K0004, K0005, K0014, K0016, K0017, K0020, K0031, K0035, K0042, K0045, K0046, K0048, K0054, K0058, K0062, K0074, K0100, K0101, K0111, K0113, K0120, K0133, K0134, K0136, K0146, K0149, K0159, K0171, K0176, K0179, K0184, K0186, K0187, K1015, K4006, K4007, K4008, K4009, K4019, K5503
المهارات	S0001, S0008, S0012, S0017, S0023, S0040, S0061, S0072, S0083, S0084, S0092, S1007, S1052, S4007, S4008, S5025, S5526, S5532

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي تقييم الثغرات
معرّف 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 المستويات، ضد الثغرات المعروفة.
مجالات الكفاءة	إدارة الثغرات الأمنية (CA013)
المهمات	T0003, T0009, T0024, T0041, T0113, T0133, T0138, T0139, T4500, T4501, T4502, T4507
المعارف	K0001, K0002, K0003, K0004, K0005, K0009, K0017, K0019, K0024, K0035, K0042, K0046, K0051, K0064, K0074, K0076, K0087, K0088, K0090, K0099, K0100, K0113, K0119, K0133, K0186, K0187, K0188, K0189, K0192, K0194, K0205, K0213, K0214, K4514, K5503
المهارات	S0001, S0009, S0026, S0037, S0044, S0056, S0061, S0068, S0085, S0092, S0102, S1023, S1508, S1509, S2506, S2527, S2557, S4502, S4504, S4505, S4507, S5025, S5532

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي اختبار الاختراقات
معرّف الدور الوظيفي	PD-VA-002
الفئة	الحماية والدفاع
مجال التخصص	تقييم الثغرات
وصف الدور الوظيفي	أداء محاولات اختراق مصرح لها، لنظم الحاسبات أو الشبكات، والمنشآت المادية؛ باستخدام أساليب تهديد واقعية؛ لتقييم حالتها الأمنية، وكشف الثغرات المحتملة.
مجالات الكفاءة	اختبار الاختراق (CA010)، إدارة الثغرات الأمنية (CA013)
المهمات	T4503, T4504, T4505, T4507, T4508, T4509, T4510, T4511, T4512, T4513, T4514, T4515, T4516, T4517
المعارف	K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0009, K0010, K0011, K0054, K0057, K0074, K0075, K0080, K0134, K0153, K0159, K0170, K0171, K0184, K0186, K0187, K0188, K0214, K1013, K4504, K4505, K4506, K4508, K4511, K4512, K4513, K4514, K5503
المهارات	S0001, S0011, S0023, S0027, S0044, S0045, S0068, S0070, S0092, S0098, S0099, S2010, S4501, S4503, S4504, S4505, S4506, S4509, S4510, S4512, S502, S5015, S5025, S5502, S5532

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي استجابة للحوادث السيبرانية
معرّف الدور الوظيفي	PD-IR-001
الفئة	الحماية والدفاع
مجال التخصص	الاستجابة للحوادث
وصف الدور الوظيفي	مباشرة الحوادث المتعلقة بالأمن السيبراني، وتحليلها، والاستجابة لها.
مجالات الكفاءة	إدارة الحوادث (CA011)
المهمات	T0009, T0026, T0027, T0028, T0031, T0044, T0047, T0051, T0058, T0062, T0087, T0101, T0106, T0138, T0142, T0143, T0144, T0145, T0148, T0150, T0154, T5003, T5025, T5031, T5040, T5057, T5066
المعارف	K0001, K0002, K0003, K0004, K0005, K0019, K0021, K0024, K0025, K0032, K0043, K0047, K0064, K0074, K0084, K0087, K0088, K0090, K0099, K0100, K0117, K0121, K0123, K0133, K0186, K0187, K0188, K0189, K0194, K0195, K0196, K0205, K3507, K4511, K4512, K4513, K4514, K5503
المهارات	S0002, S0004, S0006, S0009, S0011, S0012, S0013, S0014, S0015, S0018, S0019, S0020, S0022, S0023, S0025, S0026, S0027, S0033, S0035, S0041, S0044, S0046, S0048, S0051, S0093, S0094, S0095, S0097, S0098, S0099, S0101, S0103, S0104, S1022, S1023, S1034, S2533, S2557, S3500, S3501, S5000, S5001, S5002, S5003, S5004, S5005, S5006, S5008, S5511, S5532, S5534, S5025, S5030, S5031, S5032, S5033, S5034, S5501, S5502, S5503, S5504

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي التحليل الجنائي الرقمي
معرّف 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.
مجالات الكفاءة	التحليل الجنائي الرقمي (CA009)
المهمات	T0010, T0030, T0032, T0033, T0049, T0149, T5000, T5002, T5004, T5006, T5007, T5010, T5013, T5014, T5015, T5016, T5017, T5019, T5020, T5022, T5023, T5024, T5025, T5026, T5036, T5037, T5038, T5039, T5040, T5041, T5045, T5057, T5062, T5063, T5064, T5065
المعارف	K0001, K0002, K0003, K0004, K0005, K0016, K0019, K0045, K0066, K0074, K0075, K0090, K0100, K0119, K0171, K0176, K0186, K0187, K0188, K0189, K0203, K0205, K1503, K1513, K5007, K5008, K5009, K5010, K5011, K5014, K5015, K5016, K5017, K5019, K5020, K5021, K5033, K5034, K5035, K5036, K5037, K5038, K5039, K5040, K5503
المهارات	S0013, S0020, S0029, S0030, S0041, S0068, S0069, S0085, S0098, S0099, S0100, S1038, S1039, S5000, S5001, S5002, S5003, S5004, S5005, S5006, S5008, S5009, S5010, S5011, S5021, S5022, S5024, S5025, S5026, S5027, S5029, S5030, S5031, S5032, S5033, S5034, S5527

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي تحقيقات الجرائم السيبرانية
معرّف 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.
مجالات الكفاءة	التحليل الجنائي الرقمي (CA009)
المهمات	T0018, T0021, T5001, T5005, T5008, T5009, T5010, T5012, T5018, T5023, T5034, T5035, T5040, T5042, T5043, T5046, T5047, T5049, T5057, T5061, T5067
المعارف	K0001, K0002, K0003, K0004, K0005, K0065, K0074, K0170, K0171, K0179, K0186, K0187, K0188, K0189, K0198, K0199, K0200, K0201, K0202, K5001, K5003, K5006, K5007, K5008, K5032, K5033, K5034, K5036, K5041, K5042, K5503
المهارات	S0013, S0018, S0068, S0069, S1038, S1039, S1501, S1510, S5003, S5019, S5020, S5021, S5023, S5024, S5025, S5031, S5032, S5033, S5527

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائيّ الهندسة العكسية، للبرمجيات الضارة
معرّف 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 بشأن تقنيات الوقاية منها، والاستجابة للحوادث الناتجة عنها.
مجالات الكفاءة	التحليل الجنائي الرقمي (CA009)، إدارة الحوادث (CA011)، أمن الأجهزة والبرمجيات الثابتة (CA016)
المهمات	T0089, T5016, T5052, T5055, T5057, T5058, T5510, T5519, T5525, T5535, T5537, T5538, T5539, T5547
المعارف	K0001, K0002, K0003, K0004, K0005, K0014, K0016, K0039, K0043, K0047, K0074, K0094, K0095, K0096, K0097, K0098, K0099, K0100, K0101, K0102, K0103, K0104, K0105, K0170, K0186, K0187, K0188, K0189, K0204, K0205, K0206, K5017, K5019, K5020, K5021, K5022, K5023, K5024, K5040
المهارات	S0001, S0029, S0030, S0031, S0032, S0048, S0049, S0052, S0053, S0066, S0067, S0068, S0077, S0092, S0100, S0104, S1039, S4502, S5008, S5009, S5010, S5011, S5012, S5013, S5028, S5034, S5527, S5529, S5531

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	محلّل معلومات التهديدات السيبرانية
معرّف 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، والخطط، والأساليب، والإجراءات، التي يتّبعها المخترقون؛ لاستنباط المؤشرات وتوثيقها، التي من شأنها مساعدة المنظمات في الكشف عن الحوادث السيبرانية، والتنبؤ بها، وحماية النُظم والشبكات من التهديدات السيبرانية.
مجالات الكفاءة	المعلومات الاستباقية للتهديدات السيبرانية (CA019)
المهمات	T5056, T5502, T5504, T5505, T5507, T5515, T5517, T5519, T5524, T5525, T5526, T5527, T5530, T5531, T5535, T5537, T5538, T5539, T5541, T5543, T5546, T5547, T5548, T5549, T5550
المعارف	K0001, K0002, K0003, K0004, K0005, K0027, K0043, K0066, K0074, K0099, K0159, K0177, K0184, K0186, K0187, K0188, K0189, K0203, K5501, K5502, K5503, K5505, K5510, K5511, K5519, K5520, K5523, K5524, K5529, K5531, K5532, K5535, K5536
المهارات	S0049, S0051, S0055, S0056, S0058, S0076, S0077, S0086, S0103, S0505, S1009, S1020, S1502, S1504, S2517, S2520, S2522, S2537, S2542, S2543, S2550, S2552, S2554, S3501, S5503, S5504, S5516, S5517, S5518, S5520, S5525, S5528, S5530, S5531, S5532

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي اكتشاف التهديدات السيبرانية
معرّف 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.
مجالات الكفاءة	المعلومات الاستباقية للتهديدات السيبرانية (CA019)
المهمات	T0009, T0017, T0018, T0021, T0026, T0027, T0028, T0030, T0032, T0033, T0035, T0049, T0054, T0055, T0056, T0057, T0060, T0069, T0080, T0089, T0109, T0140, T0142, T0143, T0152, T0156, T0160, T0161, T0162, T0163, T0164, T1528, T5010, T5016, T5023, T5500, T5514, T5515, T5517, T5519, T5520, T5521, T5523, T5524, T5525, T5532, T5546, T5547
المعارف	K0001, K0002, K0003, K0004, K0005, K0013, K0014, K0016, K0028, K0031, K0032, K0034, K0035, K0043, K0044, K0047, K0064, K0065, K0068, K0074, K0086, K0088, K0107, K0176, K0191, K0195, K0196, K0198, K0199, K0200, K0201, K0202, K5503, K5505, K5510, K5519, K5526, K5529, K5531, K5535, K5537
المهارات	S0001, S0029, S0030, S0031, S0032, S0050, S0051, S0052, S0053, S0056, S0059, S0062, S0068, S0069, S0070, S0076, S0077, S0092, S0100, S0103, S0104, S2520, S2522, S2525, S5008, S5009, S5010, S5011, S5012, S5018, S5022, S5025, S5503, S5511, S5515, S5519, S5534

٥,١,٣ مجموعة الفئة: نظم التحكم الصناعية والتقنيات التشغيلية (ICS/OT)

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	مصمم معمارية الأمن السيبراني، لنظم التحكم الصناعية والتقنيات التشغيلية
معرّف الدور الوظيفي	ICSOT- ICSOT-001
الفئة	نظم التحكم الصناعية، والتقنيات التشغيلية
مجال التخصص	نظم التحكم الصناعية، والتقنيات التشغيلية
وصف الدور الوظيفي	تصميم نظم الأمن السيبراني وشبكاته في بيئة نظم التحكم الصناعية والتقنيات التشغيلية، والإشراف على ضبط إعداداتها، وتطويرها وتنفيذها.
مجالات الكفاءة	تصميم معمارية الأمن السيبراني (CA017)، الأمن السيبراني الصناعي وأمن إنترنت الأشياء (CA018)
المهمات	T0036, T0043, T0146, T0507, T0508, T0511, T0512, T0514, T0515, T0516, T0517, T0518, T0519, T0520, T0534, T0535, T0536, T0537, T0538, T0539, T1543, T2511, T4502, T6000, T6006, T6009, T6010, T6012, T6017, T6018
المعارف	K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0009, K0010, K0011, K0012, K0013, K0014, K0016, K0017, K0020, K0021, K0022, K0025, K0027, K0028, K0034, K0035, K0042, K0048, K0053, K0057 , K0058, K0062, K0074, K0093, K0101, K0111, K0112, K0120, K0121, K0133, K0146, K0149, K0175, K0176, K0186, K0187, K0188, K0189, K0190, K0191, K0192, K1015, K1036, K1505, K4000, K4030, K5503, K6002, K6003, K6004, K6005, K6006, K6007, K6014, K6015, K6016, K6017, K6019, K6020, K6021, K6022, K6023
المهارات	S0001, S0003, S0008, S0016, S0021, S0023, S0027, S0038, S0039, S0040, S0051, S0058, S0061, S0064, S0071, S0072, S0074, S0075, S0082, S0092, S0507, S0508, S0509, S1004, S1008, S1034, S1046, S1060, S1504, S1506, S2010, S2501, S6000, S6001, S6002, S6003, S6004, S6005, S6006, S6007, S6008, S6012, S6013

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي البنية التحتية للأمن السيبراني، لنظم التحكم الصناعية والتقنيات التشغيلية
معرّف الدور الوظيفي	ICSOT- ICSOT-002
الفئة	نظم التحكم الصناعية، والتقنيات التشغيلية
مجال التخصص	نظم التحكم الصناعية، والتقنيات التشغيلية
وصف الدور الوظيفي	فحص الأجهزة والبرمجيات المستخدمة للدفاع وحماية النُظم والشبكات من التهديدات السيبرانية، في بيئة نظم التحكم الصناعية والتقنيات التشغيلية، وتنصيبها، وصيانتها، وتشغيلها، والإشراف عليها.
مجالات الكفاءة	أمن الاتصالات (CA003)، أمن أنظمة التشغيل (CA005)، أمن الأجهزة والبرمجيات الثابتة (CA016)، الأمن السيبراني الصناعي وأمن إنترنت الأشياء (CA018)
المهمات	T0038, T0057, T0147, T1543, T3502, T3506, T3507, T3508, T4023, T6005, T6007, T6008, T6012, T6019
المعارف	K0001, K0002, K0003, K0004, K0005, K0017, K0019, K0024, K0035, K0043, K0046, K0063, K0064 , K0074, K0084, K0100, K0119, K0147, K0186, K0187, K0188, K0189, K0192, K0194, K1052, K3502, K3509, K5012, K6012, K6014, K6015, K6016, K6017, K6019, K6020, K6022, K6023
المهارات	S0001, S0005, S0008, S0009, S0014, S0016, S0021, S0022, S0035, S0038, S0040, S0061, S0065, S0068, S0069, S0071, S0082, S0085, S0092, S0096, S0106, S1007, S2507, S3500,S4006, S6007,S6008, S6009, S6011

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	محلل دفاع الأمن السيبراني، لنظم التحكم الصناعية والتقنيات التشغيلية
معرّف الدور الوظيفي	ICSOT- ICSOT-003
الفئة	نظم التحكم الصناعية والتقنيات التشغيلية
مجال التخصص	نظم التحكم الصناعية والتقنيات التشغيلية
وصف الدور الوظيفي	استخدام البيانات التي جرى جمعها من مجموعة متنوعة، من أدوات الأمن السيبراني؛ لتحليل الأحداث الواقعة في بيئة نظم التحكم الصناعية، والتقنيات التشغيلية؛ بهدف الكشف عن تهديدات الأمن السيبراني، والتعامل معها.
مجالات الكفاءة	إدارة الهوية والتحكم بالوصول (CA001)، أمن الاتصالات (CA003)، أمن أنظمة التشغيل (CA005)، إدارة الثغرات الأمنية (CA013)، الأمن السيبراني الصناعي وأمن إنترنت الأشياء (CA018)، المعلومات الاستباقية للتهديدات السيبرانية (CA019)، اختبار الأمن السيبراني (CA024)
المهمات	T0009, T0015, T0025, T0028, T0029, T0037, T0040, T0044, T0054, T0055, T0056, T0058, T0064, T0067, T0068, T0069, T0070, T0071, T0072, T0073, T0075, T0076, T0097, T0098, T0111, T0122, T0138, T0141, T0151,T0152, T0155, T0156, T0157, T0159, T1543, T3500, T3503, T3504, T6005
المعارف	K0001, K0002, K0003, K0004, K0005, K0007, K0013, K0014, K0016, K0017, K0020, K0024, K0031, K0035, K0042, K0043, K0044, K0045, K0046, K0049, K0053, K0054, K0058, K0063, K0070, K0074, K0076, K0077, K0078, K0084, K0086, K0087, K0088, K0090, K0099, K0100, K0125, K0126, K0134, K0136, K0137, K0139, K0145, K0146, K0147, K0153, K0176, K0177, K0192, K0193, K0194, K0197, K0198, K0199, K0200, K0201, K0202, K0205, K0206, K0212, K6014, K6015, K6016, K6017, K6019, K6020, K6022, K6023
المهارات	S0001, S0006, S0009, S0012, S0015, S0023, S0033, S0040, S0041, S0046, S0048, S0056, S0057, S0061, S0063, S0069, S0092, S0097, S0101, S0104, S2002, S2520, S2522, S2526, S3500, S3501, S5503, S5525, S6004, S6005, S6006, S6007, S6009

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية
معرّف الدور الوظيفي	ICSOT- ICSOT-004
الفئة	نظم التحكم الصناعية، والتقنيات التشغيلية
مجال التخصص	نظم التحكم الصناعية، والتقنيات التشغيلية
وصف الدور الوظيفي	تحديد مخاطر الأمن السيبراني وتقييمها وإدارتها في بيئة نظم التحكم الصناعية، والتقنيات التشغيلية، وتقييم فاعلية ضوابط الأمن السيبراني القائمة وتحليلها، وتقديم الملحوظات والتوصيات بشأنها؛ بناءً على تلك التقييمات.
مجالات الكفاءة	تحليل المخاطر الأمنية (CA008)، الأمن السيبراني الصناعي وأمن إنترنت الأشياء (CA018)
المهمات	T0001, T0006, T0012, T0013, T0014, T0039, T0043, T0053, T0105, T0109, T0128, T0130, T0132, T0133, T0160, T0161, T0162, T0163, T0164, T2500, T2529, T6014, T6016, T6020
المعارف	K0001, K0002, K0003, K0004, K0005, K0007, K0008, K0009, K0029, K0037, K0073, K0074, K0080, K0081, K0083, K0092, K0107, K0160, K0166, K0167, K0186, K0187, K0188, K0189, K0190, K2511, K5503, K6003, K6005, K6012, K6014, K6015, K6016, K6017, K6019, K6020, K6022, K6023
المهارات	S0012, S0040, S0044, S0056, S0057, S0062, S0075, S0077, S0079, S0080, S0081, S0082, S0089, S0091, S1007, S1504, S2553, S4507, S6006, S6007, S6009

تفاصيل الدور الوظيفي	
مسمى الدور الوظيفي	أخصائي استجابة للحوادث السيبرانية، لنظم التحكم الصناعية، والتقنيات التشغيلية
معرّف الدور الوظيفي	ICSOT- ICSOT-005
الفئة	نظم التحكم الصناعية، والتقنيات التشغيلية
مجال التخصص	نظم التحكم الصناعية، والتقنيات التشغيلية
وصف الدور الوظيفي	مباشرة حوادث الأمن السيبراني، وتحليلها والاستجابة لها، في بيئة نظم التحكم الصناعية والتقنيات التشغيلية.
مجالات الكفاءة	إدارة الحوادث (CA011)، الأمن السيبراني الصناعي وأمن إنترنت الأشياء (CA018)
المهمات	T0009, T0026, T0027, T0028, T0031, T0044, T0047, T0051, T0058, T0062, T0087, T0101, T0106, T0138, T0142, T0143, T0144, T0145, T0148, T0150, T0154, T5025, T5031, T6014, T6015, T6020
المعارف	K0001, K0002, K0003, K0004, K0005, K0019, K0021, K0024, K0025, K0032, K0043, K0047, K0064, K0074, K0084, K0087, K0088, K0090, K0099, K0100, K0117, K0121, K0123, K0133, K0171, K0186, K0195, K0196, K0205, K3507, K4511, K4512, K4513, K5503, K6012, K6014, K6015, K6016, K6017, K6020, K6022, K6023
المهارات	S0002, S0004, S0006, S0009, S0011, S0012, S0013, S0014, S0015, S0018, S0020, S0022, S0023, S0025, S0026, S0027, S0033, S0035, S0041, S0044, S0046, S0048, S0051, S0052, S0054, S0060, S0068, S0085, S0093, S0094, S0095, S0097, S0098, S0099, S0101, S0103, S0104, S1022, S1023, S1034, S1060, S2002, S2506, S2523, S2526, S2533, S2557, S3500, S3501, S5000, S5001, S5002, S5003, S5009, S5010, S5011, S5012, S5013, S5014, S5025, S5030, S5031, S5032, S5033, S5034, S5501, S6006, S6007, S6009, S6010

٢,٣ الملحق ب: قائمة المهمات والمعارف والمهارات

كما ذُكر سابقًا، فقد جرى تطوير الإطار السعودي لكوادر الأمن السيبراني، باستخدام المنهجية المتبعة في أفضل الممارسات العالمية إلا أن الفئات ومجالات التخصص، والأدوار الوظيفية الواردة في الإطار السعودي لكوادر الأمن السيبراني، تم مواءمتها، لتلبية احتياج كوادر الأمن السيبراني في المملكة العربية السعودية.

وقد جرى تعريف **المهمات** والمعارف والمهارات المطلوبة، لأداء كل دور وظيفي في هذا الإطار، باستخدام القائمة الطويلة من **المهمات** والمعارف، والمهارات الموجودة في أفضل الممارسات العالمية مع تعديل ما يلزم لإظهار احتياجات كوادر الأمن السيبراني في المملكة.

كما جرى ترقيم **المهمات** والمعارف والمهارات، حسب ما هو موضح في (الجدول ٨). ويقدم (الجدول ٩) و(الجدول ١٠) و(الجدول ١١) أوصاف **المهمات** والمعارف والمهارات المستخدمة في هذا الإطار.

الفئة	مجال التخصص	مدى الترقيم للمهمات والمعارف والمهارات
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	2999-2500
	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
نظم التحكم الصناعية، والتقنيات التشغيلية	نظم التحكم الصناعية، والتقنيات التشغيلية	6000-6499

جدول ٨: نظام ترقيم المهمات والمعارف والمهارات، في الإطار السعودي لكوادر الأمن السيبراني

رمز المهمة	وصف المهمة
T0001	تقديم المشورة للإدارة العليا بشأن مستويات مخاطر الأمن السيبراني، ووضع الأمن السيبراني.
T0002	التواصل الفعال مع الإدارة العليا بشأن الجوانب المالية للأنشطة، المتعلقة بالأمن السيبراني.
T0003	تقييم التزام المنظمة بالسياسات التنظيمية للأمن السيبراني.
T0004	تنفيذ سياسات الأمن السيبراني على التطبيقات.
T0005	تطبيق ضوابط الأمن السيبراني للنظام.
T0006	تطوير وصف مخاطر الأمن السيبراني.
T0009	ربط بيانات الحوادث.
T0010	فك تشفير البيانات المضبوطة باستخدام وسائل تقنية.
T0011	تطوير سياسات الأمن السيبراني، والإجراءات ذات العلاقة.
T0012	وضع إستراتيجيات الحد من المخاطر.
T0013	تطوير إجراءات مضادة خاصة بالأمن السيبراني؛ لمعالجة النظام والتطبيقات.
T0014	توثيق المخاطر الأمنية الأولية، أو المتبقية؛ التي تؤثر على تشغيل النظام.
T0015	استخدام منتجات الأمن السيبراني، وتقنيات التحكم الأمني؛ للحد من المخاطر المكتشفة إلى مستويات مقبولة.
T0016	التأكد من توافق قدرات الحماية والاكتشاف، مع بنية الأمن السيبراني على مستوى المنظمة.
T0017	تأسيس قنوات اتصال ملائمة مع أصحاب المصلحة.
T0018	إنشاء علاقات بين الفرق الداخلية والخارجية.
T0019	ضمان التزام العقود بمتطلبات الأمن السيبراني، وحماية البيانات القانونية، والتنظيمية.
T0021	تحديد البيانات، أو المعلومات الاستباقية، ذات القيمة بكونها أدلّة جنائية.
T0022	تقييم استيفاء المنتجات المُنفَّذة لمتطلبات الأمن السيبراني.
T0023	تحسين الوثائق ذات الصلة بالأمن السيبراني؛ لتلبية متطلبات الالتزام.
T0024	الحفاظ على مجموعة أدوات تدقيق الدفاع السيبراني، القابلة للتفعيل.

T0025	تصعيد الحوادث السيبرانية التي يمكنها أن تؤدي إلى أثر فوري أو مستمر على البيئة.
T0026	تحديد التهديدات المحتملة لموارد الشبكة.
T0027	إجراء فرز لحوادث الأمن السيبراني.
T0028	تحليل توجهات الدفاع السيبراني، وتقديم تقارير بشأنها.
T0029	تحديد فاعلية الهجمة المرصودة.
T0030	تحليل توقيعات الملفات؛ لتحديد سماتها المميزة.
T0031	التوصية بإستراتيجيات الإصلاح السريع والحد من المخاطر لنُظم المنظمة.
T0032	إجراء تحليل جنائي رقمي حي.
T0033	تحليل الخط الزمني للأحداث.
T0035	الحد من الثغرات الأمنية المحتملة في البرمجة.
T0036	تحديد الفجوات في المعمارية الأمنية.
T0037	إجراء مراجعات الأمن السيبراني للمعمارية الأمنية؛ لإثراء إستراتيجيات الحد من المخاطر.
T0038	تنفيذ إدارة النُظم على تطبيقات الدفاع السيبراني ونظمه المتخصصة.
T0039	تحليل المخاطر المحتملة، على التطبيقات والنُظم، التي تخضع لتغييرات جوهرية.
T0040	التوصية بالتعديلات على النُظم؛ لسد الثغرات المحددة.
T0041	إعداد تقارير التدقيق.
T0042	تقديم إرشادات توعوية للمنظمة؛ لدعم خطط إدارة استمرارية الأعمال وحماية البيانات.
T0043	تقديم المشورة، بشأن أنشطة إجراءات، إطار إدارة المخاطر والوثائق، ذات الصلة.
T0044	تحديد أسباب تنبيهات الشبكة.
T0046	توفير الخبرة الاستشارية عن الأمن السيبراني في مجالس السياسات، الخاصة بالمؤسسات والقطاعات.
T0047	تتبع حوادث الدفاع السيبراني؛ منذ اكتشافها الأوَّلي إلى الحل النهائي.
T0048	التأكد من اتخاذ الإجراءات المناسبة؛ للحد من التهديدات.

T0049	رصد حركة البيانات الشبكية، المرتبطة بالعمليات الضارة.
T0050	تحديث وثائق الأمن السيبراني، العاكسة لخصائص التصميم الحالية، لأمن التطبيقات والنُظم.
T0051	إعداد تقارير نتائج الحوادث السيبرانية.
T0052	البحث في التقنيات المعاصرة؛ لفهم قدرات الدفاع السيبراني، المطلوبة من قبل النُظم أو الشبكات.
T0053	تقديم التوجيه في مجال الأمن السيبراني، لعمليات حوكمة المخاطر للمنظمة.
T0054	الكشف عن الهجمات السيبرانية، وعمليات التسلل.
T0055	المراقبة المستمرة لأنشطة النُظم.
T0056	تحديد أثر الأنشطة الضارة على النُظم والمعلومات.
T0057	تحديد حماية البنية التحتية الحاسمة، للدفاع السيبراني ومواردها، وترتيب أولوياتها وتنسيقها.
T0058	تطبيق مبادئ وممارسات الدفاع الأمني ذي المستويات المتعددة بما يتسق مع سياسات المنظمة.
T0059	إدارة معالجة الثغرات بفاعلية.
T0060	إنشاء أدلة قابلة للتدقيق على التدابير الأمنية.
T0061	التأكد من تلبية عمليات الاستحواذ، والمشتريات، وجهود الاستعانة بمصادر خارجية لمتطلبات الأمن السيبراني.
T0062	الحد من حوادث الدفاع السيبراني المحتملة.
T0063	التأكد من الالتزام المؤسسي.
T0064	وضع الإجراءات للتصدي لمجموعات التسلل.
T0067	تحديد حالات الاشتباه بحركة مرور البيانات عبر الشبكة.
T0068	تحديد المؤشرات، والتحذيرات؛ من خلال البحث والتحليل، والربط عبر مجموعات بيانات متعددة.
T0069	التحقق من تنبيهات نظام كشف التسلل.
T0070	إزالة البرمجيات الضارة.
T0071	تحليل حركة مرور البيانات، عبر الشبكة؛ لتحديد مكونات بيئة أحد أجهزة الشبكة.
T0072	استخدام حركة مرور البيانات، عبر الشبكة؛ لإعادة تمثيل النشاط الضار.

T0073	تحديد أنشطة التعرف على التخطيط الشبكي، وعلى نظم التشغيل.
T0074	تقييم فاعلية ضوابط الأمن السيبراني.
T0075	إنشاء توقيعات أدوات شبكة الدفاع السيبراني.
T0076	الإبلاغ عن الحوادث السيبرانية المشتبه بها؛ وفقًا لخطة المنظمة للاستجابة للحوادث السيبرانية.
T0078	الحصول على التمويل الكافي، للتدريب على الأمن السيبراني.
T0079	التأكد من فاعلية عمليات إدارة الإعدادات.
T0080	جمع المقاييس وبيانات التوجهات.
T0082	ضمان التزام سياسات وإدارة كوادر الأمن السيبراني وعملياته، بالمتطلبات القانونية، ومتطلبات المنظمة.
T0083	تقديم المعلومات التقنية، لفئات التقنيين، وغير التقنيين.
T0084	عرض البيانات بصيغ إبداعية.
T0085	رفع الوعي بسياسة الأمن السيبراني، بين مديري المنظمة.
T0086	تحديد متطلبات التدريب.
T0087	إعداد المراجعات لاستخلاص الدروس المستفادة، بعد أحداث الأمن السيبراني.
T0088	دمج القوانين والتنظيمات في سياسة الأمن السيبراني.
T0089	استخدام أدوات الهندسة العكسية.
T0090	تصميم نظم إدارة البيانات.
T0091	دمج أفضل ممارسات التشفير في التطبيقات.
T0095	مواءمة إستراتيجية الأمن السيبراني للمنظمة، مع إستراتيجية الأعمال الخاصة بها.
T0096	تصميم إجراءات أمن النُظم.
T0097	تحليل التوجهات في الحالة الأمنية للمنظمة.
T0098	إعداد تقارير توجهات الحالة الأمنية للنُظم.
T0100	تقييم مدى كفاية ضوابط التحكم بالوصول.

T0101	الحفاظ على فهم محدث، لحالة تهديدات الأمن السيبراني.
T0102	التأكد من فاعلية تنفيذ النُظم، وعمليات اختبارها.
T0103	التأكد من فاعلية سياسات الأمن السيبراني المؤسسية، وإجراءاتها.
T0105	إجراء تقييمات لمخاطر الأمن السيبراني.
T0106	تنسيق وظائف الاستجابة للحوادث.
T0107	التوصية بإستراتيجيات الحد من مخاطر التهديدات، والثغرات.
T0108	تقديم المشورة، والإرشادات للإدارة، والعاملين، والمستخدمين، عن سياسة الأمن السيبراني.
T0109	إجراء عمليات تدقيق برامج ومشاريع التقنيات.
T0111	العمل مع أصحاب المصلحة؛ لحل حوادث الأمن السيبراني، وقضايا الالتزام المتعلقة بالثغرات.
T0112	توفير المشورة والمدخلات، في مجال الأمن السيبراني، لخطط التعافي من الكوارث، والطوارئ، واستمرارية العمليات التشغيلية.
T0113	أداء تقييمات تقنية، وغير تقنية، للمخاطر والثغرات للبيئات التقنية في المنظمة.
T0122	توفير إشعارات للموظفين المختصين بالنوايا، أو الأنشطة العدائية الوشيكة.
T0127	ضمان وضع الضوابط الملائمة؛ للحد من المخاطر، المتعلقة بمخاوف حماية البيانات، ومعالجتها، خلال عمليات تقييم المخاطر.
T0128	وضع برنامج لإدارة مخاطر الأمن السيبراني.
T0130	وضع إستراتيجيات إدارة المخاطر بالمنظمة.
T0132	تسهيل رفع مستوى الوعي لدى أصحاب المصلحة، بمستويات المخاطر القائمة؛ من خلال المراقبة المنتظمة للمخاطر.
T0133	إجراء المراقبة المستمرة للمخاطر.
T0134	تطوير عناصر المعمارية الأمنية؛ للحد من التهديدات عند نشوئها.
T0136	وضع خطط معالجة الثغرات.
T0137	ضمان إدراج مبادئ سليمة للأمن السيبراني، في رؤية المنظمة وأهدافها.
T0138	تحديد الآثار التشغيلية، لخروقات الأمن السيبراني.
T0139	تقييم مدى مواءمة سياسة الأمن السيبراني للمنظمة، مع توجيهاتها.

T0140	الحفاظ على قنوات الاتصال مع أصحاب المصلحة.
T0141	توثيق حوادث الأمن السيبراني.
T0142	تحديد النشاط غير الاعتيادي للشبكة.
T0143	التوصية بإستراتيجيات معالجة الحوادث.
T0144	تحديد نطاق حوادث الأمن السيبراني، ودرجة إلحاحها وأثرها.
T0145	جمع الصور الرقمية بطريقة سليمة، من الناحية الجنائية.
T0146	وضع خطة لإدارة مخاطر الأمن السيبراني.
T0147	إدارة أجهزة الشبكة الافتراضية الخاصة.
T0148	توثيق حوادث الدفاع السيبراني؛ من الكشف الأوَّلي، إلى الحل النهائي.
T0149	تحليل حركة البيانات الشبكية، المرتبطة بالعمليات الضارة.
T0150	مشاركة نتائج الحوادث، مع الأطراف المعنية المختصة.
T0151	الإبلاغ عن هجمات الأمن السيبراني، والتنبيهات المتعلقة بالتسلل.
T0152	التمييز بين الهجمات السيبرانية الضارة، وتلك التي يحتمل أن تكون ضارة، وعمليات التسلل.
T0153	التأكد من وضع خطط معالجة الثغرات.
T0154	جمع الأدلة الرقمية لعمليات التسلل.
T0155	تحليل حالات الاشتباه، بحركة مرور البيانات عبر الشبكة.
T0156	تحليل حزم البيانات في الشبكة.
T0157	عزل البرامج الضارة.
T0158	تحديث إجراءات أمن النُظم.
T0159	تحليل توجهات الحالة الأمنية للمنظمة.
T0160	الإشراف على عمليات التدقيق المستقلة للأمن السيبراني.
T0161	تنفيذ عمليات تدقيق مستقلة للأمن السيبراني؛ لبرمجيات التطبيقات، والشبكات، والنُظم.

T0162	تطوير عمليات تدقيق مستقلة للأمن السيبراني؛ لبرمجيات التطبيقات، والشبكات، والنُظم.
T0163	التأكد من توافق عمليات البحث والتصميم وإجراءاتها، مع متطلبات الأمن السيبراني.
T0164	التأكد من اتّباع عمليات البحث والتصميم وإجراءاتها بدقة، من قبل موظفي الأمن السيبراني، عند تنفيذ أنشطتهم اليومية.
T0165	تعزيز الوعي بإستراتيجية الأمن السيبراني، بين مديري المنظمة.
T0500	تقديم حلول سحابية، آمنة لفرق التطوير.
T0502	تقييم التصاميم الأمنية، ومعماريتها، وتحديد مدى فاعليتها.
T0503	تطوير إستراتيجية سحابية آمنة.
T0504	تطوير تصاميم آمنة للخدمات السحابية.
T0505	بناء حلول لتحديد بيانات المنظمة الموجودة بداخل البيئات السحابية.
T0507	تنفيذ عمليات آمنة لإدارة الإعدادات.
T0508	تحديد قدرات النُظم ووظائف الأعمال الحيوية وتصنيف أولوياتها.
T0511	تحليل المعمارية المرشحة، وتخصيص الخدمات الأمنية، واختيار الآليات الأمنية.
T0512	تعريف السياقات الأمنية للنُظم.
T0514	تحرير المواصفات الوظيفية لمعمارية الأمن السيبراني.
T0515	وضع خطة لمعمارية آمنة تلبي احتياجات العمل.
T0516	تطوير المعمارية المؤسسية الآمنة، التي تلبي احتياجات العمل.
T0517	توثيق كل أنشطة التعريف والمعمارية وتحديثها، حسب الضرورة.
T0518	تحديد ضوابط الأمن السيبراني، المناسبة للنُظم، والشبكات المتصلة بالفضاء السيبراني.
T0519	تصميم وظائف إدارة الأمن السيبراني.
T0520	تحديد متطلبات عمليات التعافي من الكوارث، واستمرارية الأعمال.
T0523	تحديد أولويات قدرات النُظم أو وظائف الأعمال اللازمة لاستعادة النظام وترتيبها، جزئيًا أو كليًا، بعد وقوع عطل كارثي.
T0524	تطوير تصاميم الأمن السيبراني ودمجها، للنُظم والشبكات، التي لها متطلبات أمن متعددة المستويات.

T0525	تعريف متطلبات معمارية الأمن السيبراني، في جميع مراحل الشراء، والاستحواذ.
T0526	ضمان اتساق النُظم والمعمارية، مع إرشادات المنظمة، لمعمارية الأمن السيبراني.
T0527	ترجمة قدرات الأمن السيبراني إلى متطلبات تقنية.
T0529	تصميم ("حلول إثبات المفهوم" (POC)) والمشاريع التجريبية، في مجالات التقنيات الناشئة.
T0530	قراءة المخططات والمواصفات، والرسومات، والتصاميم الأولية والرسومات البيانية التخطيطية، ذات العلاقة بالنُظم والشبكات، ومن ثم تغييرها.
T0532	تنفيذ إستراتيجية سحابية آمنة.
T0533	تطبيق تصاميم آمنة للخدمات السحابية.
T0534	تحديد قدرات النُظم، ووظائف الأعمال الأساسية.
T0535	تطوير وثائق مفهوم العمليات، لأمن النُظم.
T0536	تحديد المتطلبات الأساسية، لأمن النُظم.
T0537	تحديد متطلبات الأعمال؛ لتطوير معمارية فعالة وآمنة.
T0538	إجراء تقييمات إدارة الأمن السيبراني.
T0539	تعريف مستويات التوافر، المناسبة، لوظائف النُظم.
T0540	تعريف متطلبات هندسة أمن النُظم، في جميع مراحل الشراء، والاستحواذ.
T0541	تقييم مدى مواءمة وثائق مفهوم العمليات، مع أفضل الممارسات.
T0542	تنفيذ عمليات البنية التحتية البرمجية (IaC) بطريقة آمنة؛ لتوفير الموارد من خدمات سحابية متعددة، وإدارتها.
T0543	إدارة منصات تنسيق الحاويات؛ للحفاظ على أساس آمن، وقابل لتوسيع التطبيقات السحابية.
T1000	تحديد مواصفات البيانات.
T1001	التخطيط للتغييرات المتوقعة، في متطلبات سعة البيانات.
T1002	التوصية بتطوير تطبيقات جديدة، أو تعديل التطبيقات القائمة.
T1003	تحليل مدى واقعية تصميم البرمجيات؛ ضمن قيود الوقت والتكلفة.
T1004	تحديد متطلبات دعم، دورة حياة النظام.

T1005	إجراء مراجعات الشفرات البرمجية.
T1006	توثيق الشفرات البرمجية الآمنة.
T1007	تقييم فاعلية تدابير الأمن السيبراني للنُظم.
T1008	بناء نماذج أولية للمنتجات، واختبارها، وتعديلها؛ للبرهنة على التزامها بمتطلبات الأمن السيبراني، وذلك من خلال النماذج الفعلية، أو النظرية.
T1009	دمج أهداف، وغايات المنظمة، في المعمارية الأمنية.
T1010	إعداد وثائق تطوير البرامج؛ خلال مراحل التطوير الأولية، والتحديثات اللاحقة.
T1011	تحديد متطلبات أداء النُظم.
T1012	تطوير نماذج التهديدات.
T1013	تقييم مَواطن الارتباط، بين الأجهزة والبرمجيات.
T1014	التحقق من الوصول للنتائج المرغوبة من البرنامج.
T1015	تطوير منتجات الأمن السيبراني، أو المنتجات المدعومة بالأمن السيبراني.
T1016	ضمان تلبية الأجهزة، ونُظم التشغيل، وتطبيقات البرمجيات؛ لمتطلبات الأمن السيبراني بشكلٍ كافٍ.
T1017	تطوير العمليات الفنية والإجرائية؛ لتأمين النسخ الاحتياطية للنُظم.
T1018	تطوير إجراءات اختبار النُظم، وأعمال التوثيق، وعمليات التحقق.
T1019	التحقق من برامج استخراج البيانات وعملياتها ومتطلباتها، وكذلك تخزين البيانات.
T1020	وضع معايير البيانات، وسياساتها، وإجراءاتها.
T1021	إعداد وثائق تصميم أمن النُظم.
T1022	وضع خطط التعافي من الكوارث، واستمرارية العمليات، للنظم الخاضعة للتطوير.
T1023	تطوير عمليات البرمجة الآمنة، ومعالجة الأخطاء.
T1024	تحديد إعدادات الأجهزة.
T1025	تحديد مدى أهمية البيانات المستعادة.
T1026	تخصيص الوظائف الأمنية، لمكونات النُظم، وعناصرها.

T1027	معالجة المشكلات التقنية، التي تجري مواجهتها، أثناء اختبار النُظم، وتنفيذها.
T1029	تحديد الأخطاء البرمجية.
T1031	وضع متطلبات الأمن السيبراني، لجميع مراحل تطوير البرمجيات.
T1033	تضمين حلول الثغرات الأمنية، في عمليات تصميم النُظم (على سبيل المثال: تنبيهات الثغرات الأمنية).
T1034	إدارة تجميع البيانات، وفهرستها، وتخزينها، وتوزيعها، واسترجاعها.
T1035	إجراء اختبارات مدمجة؛ لضمان الجودة.
T1036	إعداد مخططات تدفق العمليات، والرسومات البيانية، ذات الصلة.
T1038	تقديم إرشادات؛ لتنفيذ النُظم المطورة، للعملاء، أو فرق تثبيت النُظم.
T1039	تقديم توصيات، بشأن التقنيات، والمعمارية الجديدة، لقواعد البيانات.
T1040	معالجة التبعات الأمنية، في مرحلة قبول البرمجيات.
T1041	تحليل قدرات النظام ومتطلباته.
T1042	تنفيذ أنشطة الاختبار والتقييم.
T1043	تضمين المتطلبات الأمنية، في عناصر تصميم التطبيقات.
T1044	استخدام النماذج، والمحاكاة؛ لتحليل أداء النظام، في ظل ظروف تشغيل مختلفة، أو التنبؤ به.
T1045	وضع إستراتيجيات القدرات السيبرانية؛ لتطوير الأجهزة، والبرمجيات المخصصة.
T1046	إجراء اختبارات الاختراق.
T1048	التخطيط لتطوير أمن النظام.
T1049	تطوير تصاميم الأمن السيبراني؛ لتلبية احتياجات تشغيلية وعوامل بيئية محددة.
T1050	تحديد أدوات حلول الأمن السيبراني وتقنياته.
T1051	تطوير أدوات الأمن السيبراني، وتقنياته.
T1052	تحديد النظام المؤسسي؛ للتحكم بالإصدارات، عند تصميم التطبيقات الآمنة وتطويرها، والاستفادة منه.
T1053	تنفيذ منهجيات دورة حياة تطوير النُظم، ودمجها في بيئة التطوير، لنظم الأمن السيبراني.

T1054	استشارة العملاء بشأن تصميم نظم الأمن السيبراني وتحديثها.
T1055	إعداد وثائق البرمجيات.
T1057	تقديم التوصيات بتحسينات بنية الشبكات.
T1058	اتباع معايير دورة حياة هندسة البرمجيات والنُظم وعملياتها، وذلك عند تطوير نظم وحلول الأمن السيبراني.
T1059	تحليل مصادر البيانات؛ لتقديم توصيات قابلة للتنفيذ.
T1060	تقييم صحة النتائج.
T1061	إجراء اختبار الفرضيات.
T1062	التشاور مع محللي النُظم، والمهندسين، والمبرمجين، وغيرهم؛ لتصميم تطبيقات الأمن السيبراني.
T1063	تنفيذ الواجهات الآمنة، بين نظم المعلومات، والنُظم المادية، والتقنيات المدمجة.
T1064	تطوير عمليات جمع البيانات.
T1066	برمجة خوارزميات مخصصة.
T1069	التخصيص الفعّال، لسعة التخزين، في تصميم نظم إدارة البيانات.
T1070	قراءة النصوص البرمجية البسيطة، وتفسيرها، وكتابتها، وتعديلها، وتنفيذها لأداء المهمات.
T1071	استخدام لغات برمجة مختلفة؛ لكتابة الشفرات البرمجية، ولفتح الملفات، وأخرى لقراءتها، وكتابة المخرجات في ملفات مختلفة.
T1072	استخدام لغات مفتوحة المصدر.
T1073	استكشاف أخطاء التصاميم، في النماذج الأولية، ومعالجة المشكلات.
T1074	تقديم التوصيات، بالخصائص الوظيفية والأمنية؛ لمعالجة الثغرات.
T1075	تصميم التطبيقات الآمنة وتطويرها.
T1076	إجراء أعمال التحليل؛ لتقديم معلومات إلى أصحاب المصلحة؛ بما يدعم تطوير تطبيقات أمنية، أو تعديلها.
T1078	التشغيل التجريبي للبرامج، وتطبيقات البرمجيات.
T1079	ضمان تلبية النُظم؛ للحد الأدنى من المتطلبات الأمنية.
T1081	تطوير إجراءات اختبار نظام البرمجيات، والمصادقة عليها.

T1083	تطوير برامج استخراج البيانات وتنفيذها، وكذلك الأمر مع برامج مستودعات البيانات.
T1085	ترقية واجهات البرمجيات.
T1087	تحديد الفجوات الأمنية، في البنية المعمارية المؤسسية.
T1088	تقديم المشورة المتخصصة في الأمن السيبراني؛ بشأن الخطط التنفيذية، وإجراءات التشغيل النمطية، وتوثيق أعمال التحديث، ومواد التدريب على التحديث.
T1089	ضمان تلبية مكونات التصميم، لمتطلبات النظام.
T1090	تحديد قابلية التوسع، في معمارية النظام.
T1091	ضمان توافق الأجهزة والبرمجيات، مع المواصفات، والمتطلبات المحددة.
T1092	إعداد تقارير تحليل الثغرات.
T1093	تقديم المتطلبات التشغيلية، للبحث والتطوير، وشراء القدرات السيبرانية.
T1094	تطوير العمليات المؤتمتة، وحلول الذكاء الاصطناعي؛ ذات التصنيف العالمي.
T1096	إجراء التحليلات التنبؤية.
T1098	إجراء تحليل كمي للبيانات، باستخدام مجموعة متنوعة، من مجموعات البيانات.
T1099	مواكبة أبحاث التحليلات المرئية الحاسوبية، والتعلُّم الآلي لتأسيس تقنيات جديدة ونسخها.
T1100	إنشاء الأدوات المرئية؛ لتصور البيانات، ولوحات المعلومات، لتعميم النتائج.
T1101	إجراء عملية تشخيص البيانات.
T1102	تحويل مخططات سير العمل، والرسومات البيانية، إلى تعليمات برمجية، بلغة الحاسب.
T1104	تضمين الإجراءات الأمنية اللازمة؛ عندما يصل منتج معين، إلى نهاية دورة حياته.
T1105	دمج أدوات الاختبار الأمني، في عمليات ضمان الجودة.
T1106	تحديد متطلبات البيانات.
T1108	وضع خطط تطوير التطبيقات الجديدة، أو تعديل التطبيقات القائمة.
T1109	تصميم واجهات التطبيقات.
T1110	تصحيح أخطاء البرنامج.

T1111	تصميم منتجات الأمن السيبراني، أو المنتجات، المدعومة بالأمن السيبراني.
T1112	تطوير العمليات الفنية، والإجرائية؛ لتخزين النسخ الاحتياطية للبيانات.
T1113	تقييم فاعلية خطط التعافي من الكوارث، واستمرارية العمليات، للنظم الخاضعة للتطوير؛ خلال مرحلة الاختبار.
T1114	توجيه معالجة المشكلات التقنية، التي تواجه؛ أثناء اختبار النُظم وتنفيذها.
T1115	توثيق عناصر الثغرات؛ التي قد تتعرض للهجمات البرمجية.
T1116	تنفيذ عملية نمذجة التهديدات.
T1117	تنفيذ عملية تطوير أمن النُظم.
T1118	تصميم أدوات الأمن السيبراني وتقنياته.
T1119	تقييم الثغرات في بنية الشبكة.
T1120	تصميم واجهات آمنة، بين نظم المعلومات، والنُظم المادية والتقنيات المدمجة.
T1121	تقديم التوصيات بالخصائص، الوظيفية والأمنية؛ لاستكشاف الثغرات.
T1122	ضمان تلبية التطبيقات؛ للحد الأدنى من المتطلبات الأمنية.
T1123	إعداد وثائق نظام البرمجيات.
T1124	تحسين أداء البرمجيات.
T1125	تكييف البرمجيات مع الأجهزة الجديدة.
T1126	إجراء مراجعات الأمن السيبراني، للبنية المعمارية المؤسسية.
T1127	إجراء تحليل الثغرات، في إصلاحات البرمجيات وتحديثاتها.
T1128	تحديد أولويات المتطلبات التشغيلية؛ للبحث والتطوير، وشراء القدرات السيبرانية.
T1129	الموافقة على المتطلبات التشغيلية؛ للبحث والتطوير، وشراء القدرات السيبرانية.
T1130	إجراء التحليل الإحصائي، وتحليل التعلم الآلي.
T1131	تحديد إجراءات الأمن السيبراني، لمرحلة التشغيل المستقر، للبرمجيات وإدارتها.
T1132	ضمان التكامل الآمن، لقواعد بيانات التطبيقات.

T1133	تسجيل بيانات الاختبارات.
T1134	إدارة بيانات الاختبار.
T1135	تحديد الاحتياجات الخاصة للنظم السيبرانية المادية.
T1501	توفير المفتشين العموميين، والإشراف والالتزام؛ للتحليل القانوني والقرارات.
T1502	ضمان جمع وتحديث البيانات المناسبة؛ لتلبية المتطلبات المحددة، لتقارير الأمن السيبراني.
T1503	إطلاع أصحاب المصلحة في المنظمة، على أهمية الأمن السيبراني.
T1504	ضمان تقييم أنشطة التحسينات الأمنية، وتنفيذها، والتحقق منها؛ حسب الحاجة.
T1505	ضمان تنسيق حملات تفتيش الأمن السيبراني، في البيئة الشبكية، وأعمال الاختبارات والمراجعات.
T1506	ضمان إدراج متطلبات الأمن السيبراني، في جميع عمليات التخطيط؛ لاستمرارية الأعمال، والتعافي من الكوارث.
T1507	ضمان توافق تصاميم معمارية الأمن السيبراني، مع إستراتيجية الأمن السيبراني للمنظمة.
T1510	تحديد تبعات التقنيات الجديدة، وأعمال الترقية على برنامج الأمن السيبراني.
T1511	التواصل بفاعلية مع الأطراف الخارجية؛ عند وقوع حادث أمن سيبراني.
T1513	ضمان المحافظة على الوعي بالحالة الراهنة، لمتطلبات جمع معلومات الأمن السيبراني، والمهمات المرتبطة بها.
T1516	الإشراف على برنامج التدريب، والتوعية بالأمن السيبراني.
T1518	المشاركة في تطوير خطط ومتطلبات برنامج الأمن السيبراني؛ أو تعديلها.
T1520	ضمان توفير التدريب التوعوي بالأمن السيبراني، لجميع الموظفين بالمنظمة.
T1521	ضمان إدراج متطلبات الأمن السيبراني الملائمة اللازمة في أعمال الشراء.
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	المحافظة على سياسات الأمن السيبراني بالمنظمة؛ وكذلك الوثائق ذات العلاقة، ومن ثم مراجعتها بشكل دوري.
T1526	اتخاذ الإجراءات الملائمة لمعالجة المخاطر؛ عند وقوع حادثة، تتعلق بالأمن السيبراني.

T1527	استخدام وثائق أفضل الممارسات، المتاحة دوليًا؛ لإثراء وثائق المنظمة وتعزيزها.
T1528	تعزيز الوعي بالأمن السيبراني، لدى إدارة المنظمة.
T1529	التأكد من معالجة إستراتيجية الأمن السيبراني للمنظمة، بفاعلية؛ من خلال سياسات الأمن السيبراني، والوثائق ذات الصلة.
T1530	تقديم التوصيات، بإجراء التحسينات، على أنشطة المشتريات؛ لتلبية متطلبات الأمن السيبراني.
T1531	التأكد من تحديد متطلبات الأمن السيبراني، لجميع نظم تقنية المعلومات.
T1532	المشاركة في عملية الاستحواذ، حسب الضرورة؛ مع ضمان تبني الممارسات المناسبة، لإدارة مخاطر سلسلة الإمداد.
T1534	تنفيذ سياسات حماية البنية التحتية الحساسة وإجراءاتها.
T1535	تحديد المتطلبات المستقبلية، لإستراتيجية الأمن السيبراني.
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 الموردين وتقييمهم.
T1540	إعداد التقارير، عن أحداث الأمن السيبراني الدولية، وتقديمها للإدارة العليا.
T1541	حضور الفعاليات الدولية للأمن السيبراني.
T1542	إجراء مراجعات دورية للفرضيات، ذات العلاقة بالأمن السيبراني.
T1543	تحديد متطلبات شراء التقنيات الحساسة.
T1544	تقديم وجهات نظر موضوعية وصادقة للإدارة العليا.
T1545	ضمان معالجة أنشطة المشتريات لمخاطر سلسلة الإمداد بشكلٍ كافٍ.
T1546	وضع سياسات وإجراءات حماية البنية التحتية الحساسة.
T1547	المشاركة في الفعاليات الدولية للأمن السيبراني.
T1548	الحصول على الموارد؛ لدعم أهداف برنامج الأمن السيبراني وغاياته.
T1549	تنسيق مبادرات التخطيط الاستراتيجي؛ مع أصحاب المصلحة الداخليين، والخارجيين على حد سواء.
T1550	الحفاظ على مصفوفة الأدوار والمسؤوليات لمهمات الأمن السيبراني.

T1551	إعداد تقارير دورية، عن أداء الأمن السيبراني، وحوادث الأمن السيبراني.
T1552	إجراء تحليلات التكلفة والعائد لبرامج الأمن السيبراني، وسياساته، وعملياته، ونظمه، ومكوناته.
T1553	تقييم تحليل التكلفة والعائد، والتحليل الاقتصادي، وتحليل المخاطر في عملية اتخاذ القرار.
T1554	تقديم المشورة للإدارة العليا (مثل، مدير تقنية المعلومات) بشأن تحليل التكلفة، والعائد للبرامج الأمنية، وسياساتها، وعملياتها، ونُظمها ومكوناتها.
T1555	تحويل المتطلبات الإستراتيجية إلى مواصفات وظيفية. ؛
T1556	تقييم دراسة الجدوى، المتعلقة بالأمن السيبراني.
T1557	تقديم الدعم لصنّاع القرار، في دراسة الجدوى، المتعلقة بالأمن السيبراني.
T2000	حيازة الموارد الملائمة؛ لوضع خطة فعالة، لإدارة استمرارية الأعمال.
T2002	إجراء تدريبات تفاعلية.
T2003	تطوير إستراتيجية الأمن السيبراني للمنظمة.
T2004	تطوير مواد التدريب التوعوية، المناسبة للفئات المستهدفة.
T2005	تقييم فاعلية البرامج التدريبية، وشموليتها.
T2006	تحديد أصحاب المصلحة في السياسات التنظيمية.
T2007	التأكد من أن متطلبات الأمن السيبراني، لتقنية المعلومات، تتوافق مع إستراتيجية 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 على الأمن السيبراني.
T2011	تصميم سيناريوهات التمارين وتنفيذها.
T2012	كتابة المواد التعليمية الخاصة بالأمن السيبراني.
T2013	تطوير وحدات التدريب والفصول.
T2014	تطوير الواجبات، المرتبطة بالدورات التدريبية.
T2015	تطوير تقييمات الدورات التدريبية.

T2016	تطوير معايير الدرجات والكفاءات.
T2017	وضع خطط معالجة فجوات التدريب، والتطوّر، لدى المتدربين.
T2018	تطوير غايات التعلُّم، وأهدافه.
T2019	تطوير مواد التدريب للمنظمة.
T2020	تطوير تقييمات الكفاءة.
T2021	تقييم فاعلية التعليم وكفاءته؛ بناء على مؤشرات أداء مختلفة.
T2022	إجراء تقييمات احتياجات التعلّم.
T2023	التأكد من أن معايير التأهيل؛ تعكس المتطلبات الوظيفية للمنظمة وتمتثل لمعايير القطاع.
T2024	تطوير التدريبات، التعليمية التفاعلية.
T2025	تطوير الأوصاف الموحدة للمناصب الوظيفية، استنادًا إلى الأدوار المحددة، في الإطار السعودي لكوادر الأمن السيبراني.
T2026	تطوير عمليات الاستقطاب، والتوظيف، والاحتفاظ بالأدوار الوظيفية، في الأمن السيبراني.
T2027	تطوير هيكل التصنيف لمهن الأمن السيبراني، أو تنفيذه لتضم تحديد متطلبات دخول المجال الوظيفي، وغيرها من المصطلحات، كالرموز والمُعرفات.
T2028	تطوير سياسات التدريب للأمن السيبراني وإجراءاته.
T2029	تطوير الأهداف والغايات، لمناهج المنظمة للأمن السيبراني.
T2031	وضع مقاييس جاهزية كوادر الأمن السيبراني.
T2032	تحديد متطلبات الدخول، في المجال الوظيفي للأمن السيبراني.
T2033	إنشاء مسارات التدرج الوظيفي، في مجال الأمن السيبراني في المنظمة.
T2034	وضع متطلبات، تقديم تقارير كوادر الأمن السيبراني.
T2035	وضع برامج إدارة كوادر الأمن السيبراني.
T2036	وضع الإستراتيجيات التعليمية.
T2038	تحديد سياسات المنظمة، ذات الصلة بكوادر الأمن السيبراني.
T2039	دمج كوادر الأمن السيبراني، في عمليات تطوير دورة حياة نظم المعلومات.

T2040	ربط التدريب والتعليم، بمتطلبات الأعمال أو رسالة المنظمة.
T2042	تقديم الدورات التدريبية.
T2044	تطوير مناهج، وموارد التدريب التقني.
T2046	ضمان تلبية دورات التدريب، والتعليم، والتوعية، في مجال الأمن السيبراني؛ للأهداف المحددة.
T2047	تحديد المشكلات، ذات الصلة بالإدارة، والتخطيط، لكوادر الأمن السيبراني.
T2048	التخطيط لأساليب التعليم وأنماطه، داخل القاعات الدراسية.
T2049	التخطيط لأساليب التعليم وأنماطه، خارج القاعات الدراسية.
T2050	إجراء المراجعات الدورية، للمواد، والدورات التعليمية؛ من حيث دقتها وحداثتها.
T2051	التوصية بشأن تحديثات المواد التعليمية، والمناهج الدراسية.
T2053	مراجعة سياسات اختيار مورّدي التدريب واعتمادها، وإدارتها.
T2054	تطوير مواد التدريب، على حماية البيانات، والالتزامات القانونية.
T2055	تنفيذ سياسات، وإجراءات المنظمة، الخاصة بالتدريب والتعليم.
T2056	تصميم التقييمات والأنشطة؛ لقياس أداء المتدربين، وفاعلية المناهج الدراسية.
T2057	وضع أهداف للتعلم، واضحة، وقابلة للقياس.
T2058	الشراكة مع الخبراء المتخصصين؛ لإنشاء المحتوى، ومراجعته، وتحديثه.
T2059	المراجعة الدورية لأدوار الأمن السيبراني ومسؤولياته داخل المنظمة.
T2060	تنفيذ خطة فعالة؛ لإدارة استمرارية الأعمال، والحفاظ عليها.
T2061	تطوير برامج التدريب للمنظمة.
T2062	إجراء التقييمات لكوادر الأمن السيبراني.
T2063	تقييم برامج إدارة كوادر الأمن السيبراني.
T2064	تقديم التدريب للمتدربين.
T2065	معالجة مشكلات تخطيط، وإدارة كوادر الأمن السيبراني.

T2066	تنسيق التدريب والتعليم.
T2067	تقديم دورات تدريبية، للتوعية بشأن حماية البيانات.
T2068	تضمين أولويات القيادة.
T2069	وضع إجراءات الاستثناء، لمتطلبات الدخول في مجال الأمن السيبراني، والمؤهلات التدريبية المطلوبة.
T2070	تنفيذ حملات محاكاة التصيد الاحتيالي؛ لتقييم مستوى استجابة المستخدمين ووعيهم.
T2071	إنشاء حملات محاكاة التصيد الاحتيالي؛ لتقييم مستوى استجابة ووعي المستخدمين.
T2072	تقييم أثر مبادرات التوعية بالأمن السيبراني، وفاعليتها.
T2073	تنسيق الحملات والأنشطة الدورية، للتوعية بالأمن السيبراني.
T2074	إعداد مواد التوعية القائمة على الحالات، التي تحاكي هجمات الهندسة الاجتماعية الواقعية.
T2075	تطبيق آليات جمع الملحوظات لتعزيز جودة برامج التوعية.
T2076	إعداد ملخصات صغيرة للتوعية بالأمن السيبرانية، تتسق مع أحداث المنظمة (على سبيل المثال، حوادث التصيد الاحتيالي، وإطلاق البرمجيات).
T2077	تصميم أنشطة التوعية التفاعلية، أو المنافسات (على سبيل المثال، الاختبارات القصيرة عن الأمن السيبراني، والتحديات، ولوحات المتصدرين).
T2500	وضع إستراتيجيات مراقبة المخاطر والالتزام والضمان.
T2501	توثيق متطلبات الأمن، والصمود، والاعتمادية.
T2503	إدارة حزم الاعتماد المتفق عليها.
T2504	ضمان توافق النُظم، مع متطلبات الأمن، والصمود، والاعتمادية.
T2505	التخطيط لمراجعات قضايا التصريح الأمني، للتثبيت الأولي للنظم والشبكات.
T2506	إعداد التقييمات الفنية؛ لتطبيقات البرمجيات، والنُظم، والشبكات.
T2507	التأكد من أن وثائق التصاريح والضمان؛ تُحدد المستوى المقبول من المخاطر، لكل تطبيق، وبرنامج، ونظام، وشبكة.
T2508	إجراء أعمال التدقيق للحالة الأمنية للبرامج، والشبكة، والنظام، حسب ما ورد في سياسات الأمن السيبراني، وتقديم توصيات بالأنشطة المطلوبة، لعلاج الفجوات المكتشفة.
T2509	تطوير عمليات الالتزام بالأمن السيبراني، للخدمات المقدمة، من أطراف الخارجية.
T2510	المراجعة الدورية؛ لضمان مواءمة سياسات الأمن السيبراني، والوثائق ذات العلاقة، مع الغايات، والإستراتيجيات المعلنة للمنظمة.

T2511	تحديد أثر تنفيذ نظام جديد أو واجهات جديدة، وأثرها على وضع الأمن السيبراني للمنظمة.
T2512	توثيق أنشطة تصميم الأمن السيبراني وتطويرها.
T2513	تحديد مخاطر سلسلة الإمداد، لعناصر النُظم الحرجة.
T2514	دعم أنشطة الالتزام بالأمن السيبراني.
T2515	التأكد من أن عمليات التدقيق للأمن السيبراني، تختبر جميع الجوانب، ذات العلاقة بالبنية التحتية للمنظمة، والالتزام بالسياسات.
T2516	التأكد من أن إعدادات برامج التطبيقات، والشبكات، والنُظم، تلتزم بسياسات المنظمة للأمن السيبراني.
T2519	التعاون مع المؤسسات التنظيمية المعنية، والكيانات القانونية الأخرى؛ فيما يخص التحقيقات، وعمليات مراجعة الالتزام.
T2521	تحديد نطاق تقارير التحليلات، حسب الفئات المستهدفة المختلفة، والتي تأخذ في الحساب، قيود سرية البيانات ومشاركتها.
T2522	ضمان رفع التقارير المناسبة عن الحوادث، إلى الجهات التنظيمية؛ حسب الحاجة.
T2523	إنشاء نظم مراقبة؛ للكشف عن حالات عدم الالتزام، والإبلاغ عنها.
T2524	مراقبة التغييرات في القوانين، والأنظمة؛ للحفاظ على بقاء برامج الالتزام، محدثة باستمرار.
T2525	إجراء عمليات التدقيق الداخلي؛ لضمان الالتزام بمتطلبات الأمن السيبراني.
T2526	دعم الأعمال في إدارة المخاطر السيبرانية الخاصة بها.
T2527	العمل مع مُدقّقين خارجيين؛ لإدارة عمليات التدقيق الخارجي، والاعتمادات.
T2528	المراجعة الدورية، لخطط إدارة مخاطر الأمن السيبراني وإجراءاتها.
T2529	وضع إستراتيجيات قياس المخاطر، والالتزام، والضمان.
T2530	وضع مواصفات المخاطر، والالتزام، والضمان.
T2531	الموافقة على حزم الاعتماد، المتفق عليها.
T2532	تطوير وثائق إثبات الضمان الأمني، الخاصة بتثبيت النُظم، والشبكات.
T2533	إجراء مراجعات التصاريح الأمنية؛ لتثبيت النُظم والشبكة.
T2534	توثيق التطبيقات البرمجية، والنُظم، وأوضاع أمن الشبكات، والقدرات، والثغرات.
T2535	تطوير عمليات تدقيق الأمن السيبراني، للخدمات المقدمة من أطراف خارجية.

T2536	توثيق مخاطر سلسلة الإمداد، لعناصر النُظم الحرجة.
T2537	تعزيز السلوك واتخاذ القرار، بناء على المخاطر.
T2538	وضع الضوابط المناسبة، والضوابط التعويضية، التي تعزز سياسات الأمن السيبراني القائمة.
T2539	تحديد أثر عدم الالتزام، على مستويات المخاطر في المنظمة.
T2540	تحديد أثر عدم الالتزام، على فاعلية برنامج الأمن السيبراني، الخاص بالمنظمة.
T2541	ضمان التزام الخدمات الجديدة، والقائمة، بالتزامات الأمن السيبراني وحماية البيانات.
T2542	تحديد الفجوات في الالتزام، بالأمن السيبراني للمنظمة.
T2543	معالجة الفجوات، في الالتزام بالأمن السيبراني للمنظمة.
T2544	تقديم المشورة القانونية في مجال الأمن السيبراني، في عقود شركاء الأعمال.
T3001	تفسير القوانين، أو التنظيمات أو السياسات أو المعايير، أو الإجراءات حسب الضرورة، والعمل على تطبيقها.
T3002	حل التعارضات في القوانين، أو التنظيمات، أو السياسات، أو المعايير، أو الإجراءات.
T3004	تحديد أي انتهاكات مزعومة للقوانين، أو التنظيمات، أو السياسات، أو الإرشادات.
T3005	تطوير السياسات والإرشادات، الخاصة بتنفيذ الأمن السيبراني.
T3007	تقييم أثر التغييرات في القوانين، أو التنظيمات، أو السياسيات، أو المعايير، أو الإجراءات.
T3008	توفير إرشادات، من منظور الأمن السيبراني، بشأن القوانين، أو التنظيمات، أو السياسات، أو المعايير، أو الإجراءات، لصالح الإدارة أو العاملين، أو العملاء.
T3010	إعداد الوثائق القانونية.
T3013	تطوير العلاقات مع الجهات التنظيمية، والإدارات الحكومية، المعنية بقضايا حماية البيانات.
T3014	تسجيل قواعد البيانات، مع السلطات المحلية، المعنية بحماية البيانات.
T3019	العمل لتكوين حلقة اتصال لحماية البيانات، لمستخدمي النُظم التقنية.
T3023	إدارة مشاركة المنظمة، في الفعاليات العامة، المنعقدة بشأن قضايا حماية البيانات، والأمن السيبراني.
T3025	إعداد تقارير الوضع الراهن، لبرنامج حماية البيانات.
T3026	تطوير برنامج حماية البيانات الخاص بالمنظمة.

T3029	وضع الجزاءات المترتبة على عدم الامتثال لسياسات حماية البيانات.
T3030	معالجة ادعاءات عدم الامتثال لسياسات حماية البيانات.
T3031	تطوير إطار لإدارة المخاطر، وضمان الالتزام بسياسات حماية البيانات.
T3033	وضع آليات لتقديم الشكاوى المتعلقة بحوادث وانتهاكات حماية البيانات
T3036	المحافظة على برنامج حماية البيانات للمنظمة.
T3037	وضع سياسات حماية البيانات بالمنظمة وتطوير إجراءاتها.
T3038	مراقبة التقدم، في استخدام تقنيات حماية البيانات.
T3039	مراقبة تطوير النُظم وعملياتها؛ لضمان التزامها بسياسات الأمن السيبراني وحماية البيانات.
T3041	مواءمة ممارسات حماية البيانات في خطط أمن معلومات النُظم.
T3042	وضع إجراءات تدقيق الموردين.
T3049	وضع الخطط الإستراتيجية لمشاركة المعلومات.
T3050	تنفيذ سياسات حماية البيانات وإجراءاتها؛ للمنظمة، والحفاظ عليها.
T3051	إدارة اختراقات البيانات
T3052	المحافظة على التوعية بقوانين حماية البيانات، وتنظيماتها، ومعايير الاعتماد المعمول بها.
T3056	إدارة الإجراءات بشأن الشكاوى، المتعلقة بالأمن السيبراني في المنطقة.
T3057	وضع إجراءات تدقيق الموردين.
T3500	تطبيق أدوات الدفاع السيبراني.
T3502	إدارة أعمال تحديث القواعد، والتوقيعات، لتطبيقات الدفاع السيبراني المتخصصة.
T3503	التحقق من مصداقية التنبيهات الشبكية.
T3504	تقديم تقارير أحداث الشبكات اليومية وأنشطتها.
T3506	المساعدة في تقييم، أثر تنفيذ بنية تحتية مخصصة، للدفاع السيبراني، والحفاظ عليها.
T3507	تقييم المنصات، التي يديرها مزودو الخدمات.

T3508	إدارة قوائم التحكم بالوصول إلى الشبكات، داخل نظم الدفاع السيبراني المخصصة.
T3511	توثيق الأوصاف الوظيفية؛ لتنفيذ الضوابط، في أمن النُظم.
T4000	تطبيق مبادئ المعمارية الأمنية، الموجهة نحو الخدمات؛ بما يتوافق مع متطلبات المنظمة، الخاصة بالسرية، والنزاهة، والتوافر.
T4001	ضمان توثيق عمليات أمن النُظم، وأنشطة الصيانة، وتحديثها بشكل صحيح.
T4002	تطبيق حزم التحديثات الأمنية، للمنتجات التجارية.
T4004	دمج القدرات المؤتمتة، المخصصة؛ لتحديث برمجيات النُظم أو إصلاحها.
T4005	إجراء اختبار الأمن السيبراني، للتطبيقات والنُظم، بعد تطويرها.
T4006	توثيق أنشطة أمن النُظم.
T4007	تقديم إرشادات، بشأن الأمن السيبراني إلى القيادة.
T4008	الكشف عن البيانات المشفرة والمخفية.
T4009	تطوير إجراءات نقل عمليات النظام، إلى موقع بديل.
T4010	تنفيذ إجراءات التعافي من الكوارث، واستمرارية الأعمال.
T4011	تنفيذ تدابير أمنية على النظام، أو مكوناته.
T4013	ضمان دمج الحلول العابرة للنطاقات، وتنفيذها في بيئة آمنة.
T4014	رفع التوصيات للإدارة باتخاذ الإجراءات اللازمة؛ للحد من المخاطر، وتصحيحها، أو قبول المخاطر، عند الكشف عن جوانب القصور الأمني، أثناء الفحص.
T4015	تحديد الحد الأدنى، من المتطلبات الأمنية، لجميع التطبيقات.
T4016	تصميم حلول لإدارة الهوية، والوصول، وتطبيقها.
T4017	وضع إستراتيجية إدارة الهوية، والوصول.
T4018	ضمان اتباع معايير وسياسات المنظمة؛ عند تنفيذ حلول إدارة الهوية، والوصول.
T4019	تحديد ومعالجة الفجوات؛ عند تنفيذ حلول إدارة الهوية، والوصول.
T4021	تصميم خوارزميات التشفير وتطويرها.
T4022	تحليل خوارزميات التشفير؛ للكشف عن نقاط ضعفها، وكسر الشفرات.

T4023	تطوير العمليات، والإجراءات الخاصة، بالتحديث، وعمل الإصلاح اليدوي؛ لبرمجيات النُظم.
T4024	إعداد سياسات المجموعات.
T4025	إدارة حسابات مستخدمي النظام، والشبكة.
T4026	تطوير وظائف إدارة النُظم، والإشراف على النُظم، للمستخدمين ذوي الصلاحيات الإضافية.
T4027	إنشاء إجراءات صلاحيات الوصول إلى النُظم.
T4028	إنشاء عمليات وإجراءات التحكم، في الوصول؛ لأدوات وتقنيات المراقبة المستمرة.
T4029	تنفيذ عمليات التحكم في الوصول، لأدوات المراقبة المستمرة وتقنياتها.
T4030	التأكد من توافق تطبيق الإصلاحات الأمنية، للمنتجات التجارية؛ مع متطلبات الجدول الزمني.
T4031	إجراء اختبار التعطّل؛ لنقل عمليات النظام إلى موقع بديل.
T4032	حل الثغرات في النُظم ومكوناتها.
T4033	الحد من المخاطر، في النُظم، ومكوناتها.
T4034	تنفيذ خوارزميات التشفير.
T4035	إعداد قوائم التحكم في الوصول.
T4036	تصميم وظائف إدارة النُظم، والإشراف على النُظم، للمستخدمين ذوي الصلاحيات الإضافية.
T4500	إجراء اختبارات الاختراق، المصرح بها، على أصول شبكة المنظمة.
T4501	إجراء المراجعات المطلوبة؛ بما في ذلك مراجعة التدابير الدفاعية، حسب سياسات المنظمة.
T4502	التوصية بالضوابط الأمنية الفعالة؛ من حيث التكلفة.
T4503	إجراء التحليل التقني للشبكة، واستخدامها.
T4504	محاكاة تقنيات الهندسة الاجتماعية الضارة؛ التي يستخدمها المهاجمون.
T4505	تحديد المنهجيات التي قد يستخدمها المهاجمون؛ لاستغلال الثغرات في النُظم والشبكات.
T4507	مسح الثغرات الأمنية على النُظم.
T4508	إعداد تقارير نتائج اختبارات الاختراق، وتقييم الثغرات، ويشمل ذلك مستوى المخاطر، واقتراحات المعالجة، وجميع التفاصيل التقنية اللازمة؛ لإعادة إصدار نتائج الاختبار.

T4509	مناقشة النتائج الأمنية، مع الإدارة، والقيادة، وفرق تقنية المعلومات.
T4510	تصميم عمليات فريق اختبار الاختراق وتطويرها.
T4511	إجراء اختبار الشبكة عن بعد.
T4512	تخطيط أساليب الاختراق وإنشائها، وكذلك نصوص الاختراق واختباراته.
T4513	تصميم نماذج محاكاة للهجمات؛ لتوضح الأثر على أعمال المنظمة ومستخدميها.
T4514	عرض نتائج الاختبار، والمخاطر، والاستنتاجات، على فئات التقنيين، وغير التقنيين.
T4515	توضيح التبعات المترتبة على الأعمال؛ بسبب الثغرات المكتشفة.
T4516	إجراء التقييمات الأمنية المادية، للخوادم، والنُظم، وأجهزة الشبكات.
T4517	فحص الثغرات في التطبيقات على الشبكة العنكبوتية، وتطبيقات العميل، والتطبيقات النمطية.
T5000	تحديد أفضل المنهجيات؛ لمعرفة هوية مخترق الشبكة.
T5001	عقد مقابلات مع ضحايا الجريمة السيبرانية، وكذلك مع الشهود.
T5002	تحديد حوادث التسلل.
T5003	مكافحة حوادث الدفاع السيبراني.
T5004	إنشاء نسخة مطابقة وسليمة، للأدلة الجنائية.
T5005	التحقيق في الأنشطة المشبوهة، والجرائم السيبرانية المزعومة.
T5006	إعداد ملخص تقني، لتقارير عرض النتائج.
T5007	ضمان تتبع تسلسل العُهَد، لجميع الوسائط الرقمية، المستحوذ عليها؛ وفقًا للقوانين الوطنية، أو سياسات المنظمة المعمول بها.
T5008	إجراء تحليل للهجمات، على شبكات الحاسب الآلي.
T5009	تحديد ما إذا كان الحادث الأمني، يُعد مخالفًا للقانون، ومن ثم فإنه يتطلب اتخاذ إجراء قانوني محدد.
T5010	تحديد الأدلة الرقمية للتحليل.
T5012	جمع الأدلة النصية، أو المادية المرتبطة، بحوادث التسلل السيبرانية، والتحقيقات والعمليات.
T5013	إجراء تحليل ديناميكي، على محركات الأقراص.

T5014	إجراء مقارنة التجزئة، على قواعد البيانات؛ حسب متطلبات سياسات المنظمة.
T5015	إجراء تحليل للوسائط، غير القابلة للتغيير.
T5016	إجراء تحليل للبرمجيات الضارة، على الرُتبة الأولى، والثانية، والثالثة.
T5017	إعداد الوسائط الرقمية للنسخ.
T5018	إدارة مسرح الجريمة.
T5019	معالجة الأدلة الرقمية.
T5020	التعرف على الوحدات الجنائية الأولية، والإبلاغ عنها، بما يتسق مع سياسات الإبلاغ.
T5022	استخلاص البيانات من الأجهزة.
T5023	استعادة المعلومات، من مصادر البيانات الجنائية.
T5024	إجراء تحليل 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") لقرص مع وجود القرص الأصلي، أو بدونه.
T5029	إجراء تحليل ثابت للبرمجيات الضارة.
T5031	ربط بيانات تقييم التهديدات.
T5034	تحديد أثر التهديدات، على الأمن السيبراني.
T5035	تقديم الدعم والمشورة على أنه خبير تقني، خلال مجريات العملية القضائية.
T5036	معالجة الصور المستخدمة، بوصفها دليل جنائي.
T5037	إجراء تحليل، لسجل ويندوز المركزي.
T5038	مراقبة الملفات، والسجل المركزي على نظام التشغيل الحي.
T5039	إدخال معلومات الوسائط الرقمية، في قواعد بيانات التتبع.

T5040	الإبلاغ عن الحوادث السيبرانية؛ لإثراء الدفاع السيبراني.
T5041	إعداد مجموعة أدوات الدفاع الإلكتروني.
T5042	تحليل المواد، المتعلقة بحوادث الأمن السيبراني؛ للحصول على أدلة على وجود طرف أجنبي عدائي، أو نشاط إجرامي.
T5043	الحفاظ على الأدلة الرقمية.
T5045	تحليل ملفات السجلات.
T5046	تحديد الأطراف المسؤولة، عن عمليات التسلل، أو الجرائم السيبرانية الأخرى.
T5047	توثيق الحالة الأصلية للأدلة الرقمية.
T5049	إعداد التقارير التحقيقية.
T5052	مراجعة المعلومات، التي جرى جمعها؛ للتأكد من مصداقيتها، وعلاقتها بالتحقيق، بما يتوافق مع سياسات المنظمة.
T5055	تنقية التقارير؛ لحماية البيانات، أو المنهجيات ذات الملكية الخاصة، أو التجارية، أو الشخصية، أو غيرها من البيانات، أو المنهجيات السرية، أو الحساسة.
T5056	تتبع حالة طلبات المعلومات.
T5057	توثيق الدروس، المستفادة من مخرجات الفعاليات والتمارين.
T5058	تحديد أيّ نشاط ضار محتمَل؛ من خلال تفريغ الذاكرة، أو السجلات، أو الحِزم الملتقطة.
T5060	تقييم إمكانية، تعرض الأهداف للاستغلال؛ باستخدام حالات الاستغلال، والحلول، والتقنيات المخصصة.
T5061	إجراء المقابلات مع المشتبه، بارتكابهم جرائم سيبرانية.
T5062	تحديد التسلل؛ من خلال التحليل الديناميكي.
T5063	إنشاء محطة عمل، للتحليل الجنائي.
T5064	توثيق كل ما جرت معرفته عن عمليات التسلل.
T5065	تحليل عمليات التسلل.
T5066	تنسيق الدعم التقني، لتقنيي الدفاع السيبراني، على مستوى المنظمة.
T5067	التوصية بمسارات العمل المحتملة.
T5500	التوصية بتدابير جديدة، أو منقحة، للأمن، والصمود، والاعتمادية.

T5501	تحليل نتائج اختبارات النُظم المختلفة؛ لتحديد التحسينات ذات الكفاءة العالية؛ من حيث التكلفة، للحد من المخاطر المكتشفة.
T5502	الإجابة عن طلبات المعلومات؛ بما يتوافق مع سياسات المنظمة.
T5504	تعزيز خطط الاستجابة للحوادث؛ استنادًا إلى المعرفة بالجهات المسؤولة، عن التهديدات، وأنشطتها.
T5505	تنسيق مصادر المعلومات الاستباقية للمنظمة، وتوثيقها، وإدارتها.
T5507	إعداد وتقديم ملخصات، عن تهديدات معينة للمنظمة.
T5509	إجراء استطلاع الشبكات.
T5510	إجراء التحليل العُقدي للشبكات.
T5511	الكشف عن حالات الاستغلال، ضد الشبكات، والمضيفات.
T5512	تحديد التقنيات المستخدمة؛ من قبل هدف معين.
T5514	جمع بيانات الجهات المسؤولة عن التهديدات وتحليلها.
T5515	تقييم عمليات اتخاذ القرار، المتعلقة بالتهديدات.
T5517	تحديد التهديدات السيبرانية الرئيسة للمنظمة.
T5519	تحديد أساليب التهديدات السيبرانية ومنهجياتها.
T5520	تحديد الثغرات
T5521	تحديد هيكلية الجهة المسؤولة عن التهديد ومكوناتها.
T5523	وضع مسارات العمل؛ استنادًا إلى عوامل التهديد.
T5524	مراقبة التغييرات في مجموعات المشكلات المحددة، الخاصة بتحذيرات العمليات السيبرانية.
T5525	مراقبة أنشطة التهديد.
T5526	مراقبة المواقع الإلكترونية، المفتوحة المصدر، للمحتوى العدائي، الموجه ضد مصالح المنظمة أو شركائها.
T5527	مراقبة أنشطة الجهات، التي تمثل مصدرًا للتهديدات؛ والإبلاغ عنها.
T5530	تقديم التحليل، والدعم في مجال المعلومات الاستباقية.
T5531	إعداد تقارير تسلل الشبكة.

T5532	تنفيذ التعامل الفوري؛ مع حوادث الدفاع السيبراني.
T5535	المحافظة على تصور مشترك، للمعلومات الاستباقية.
T5537	تطوير متطلبات المعلومات ذات الأولوية.
T5538	إنشاء طلبات الحصول على معلومات الأمن السيبراني.
T5539	إصدار معلومات استباقية مدمجة، وفي الوقت المناسب؛ من جميع مصادر العمليات السيبرانية، ومن دلائل، وتحذيرات منتجات المعلومات الاستباقية.
T5541	التوصية بالتعديلات على إستراتيجيات جمع المعلومات الاستباقية.
T5543	تحديد فاعلية عمليات جمع المعلومات الاستباقية.
T5546	إعداد تقارير التغييرات، في مجموعات المشكلات المحددة، الخاصة بتحذيرات العمليات السيبرانية.
T5547	إعداد تقارير أنشطة التهديد.
T5548	إدارة متطلبات جمع المعلومات.
T5549	تقييم فاعلية تقارير المعلومات الاستباقية.
T5550	تقييم فاعلية إصدار المعلومات الاستباقية.
T6000	تحديد أولويات قدرات النُظم وترتيبها، أو وظائف الأعمال اللازمة لاستعادة النظام جزئيًا أو كليًا؛ بعد وقوع عطل كارثي في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
T6001	تطوير تصاميم الأمن السيبراني؛ لتلبي احتياجات تشغيلية، وعوامل بيئية محددة، في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
T6002	تحديد جميع مراحل عمليات الشراء، والاستحواذ، لمعمارية الأمن السيبراني، في بيئات تقنية المعلومات، ونظم التحكم الصناعية، والتقنيات التشغيلية.
T6003	ضمان اتساق النُظم، والبُنى المعمارية، مع الإرشادات المنظمة لمعمارية الأمن السيبراني، في بيئات تقنية المعلومات، ونظم التحكم الصناعية، والتقنيات التشغيلية.
T6004	ترجمة القدرات المقترحة، إلى متطلبات تقنية، في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
T6005	تحليل التقنيات المادية، والتقنيات الرقمية المنطقية، في بيئات التحكم الصناعية والتقنيات التشغيلية ونظمها؛ لتحديد السبل المحتملة للوصول إليها.
T6006	بحث توجهات تقنيات الاتصالات الناشئة؛ لإثراء سياسات التصاميم والأمن، بالمنظمة في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
T6007	تحديد ضوابط أمن النُظم المطلوبة في بيئات نظم التحكم الصناعية والتقنيات التشغيلية.
T6008	تنفيذ ضوابط أمن النُظم في بيئات نظم التحكم الصناعية والتقنيات التشغيلية.
T6009	تحديد الآثار المترتبة على التقنيات الجديدة والمحسنة لبرنامج الأمن السيبراني في بيئات نظم التحكم الصناعية والتقنيات التشغيلية.

T6010	تصميم نظم وحلول لدعم نجاح "حلول إثبات المفهوم" والمشاريع التجريبية في مجالات التقنيات الناشئة في بيئات ونظم التحكم الصناعية والتقنيات التشغيلية.
T6012	استكشاف مواطن الخلل في نظم وخوادم الاتصالات والأتمتة الصناعية ومن ثم إصلاحها.
T6014	حل حوادث الدفاع السيبراني، الخاصة بنظم التحكم الصناعية، والتقنيات التشغيلية.
T6015	تنفيذ التعامل الفوري، مع حوادث الدفاع السيبراني، في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
T6016	إجراء تحليل المخاطر، لبيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
T6017	دمج أهداف المنظمة وغاياتها في المعمارية الأمنية في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
T6018	تحديد جميع مراحل الشراء والاستحواذ لمتطلبات هندسة أمن النُظم في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
T6019	توثيق عمليات تنفيذ مراقبة أمن النُظم المخطط لها في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
T6020	تنسيق الدعم التقني لأخصائي الدفاع السيبراني في نظم التحكم الصناعية، والتقنيات التشغيلية.

جدول ٩: أوصاف المهمات

رمز المعرفة	الوصف
K0001	معرفة بمكونات الشبكة وبتشغيلها.
K0002	معرفة بمبادئ وممارسات تقييم المخاطر وممارستها.
K0003	معرفة بقوانين الأمن السيبراني وتنظيماته.
K0004	معرفة بمبادئ الأمن السيبراني وممارساته.
K0005	معرفة بتهديدات الأمن السيبراني.
K0007	معرفة بأدوات المصادقة، والتحقق من الهوية وتقنياتها.
K0008	معرفة بنموذج الأعمال داخل المنظمة وممارساتها؛ لتحديد إستراتيجيات الأمن السيبراني المناسبة.
K0009	معرفة الثغرات الشائعة في التطبيقات.
K0010	معرفة بمبادئ البنية التحتية للشبكات، وممارساتها.
K0011	معرفة بقدرات معدات الشبكات، وتطبيقاتها.
K0012	معرفة بمبادئ تحليل المتطلبات، وممارساتها.
K0013	معرفة بأدوات الدفاع السيبراني، وتقنياته.
K0014	معرفة بقدرات الخوارزميات الحاسوبية، وتطبيقاتها.
K0015	معرفة بمبادئ وممارسات البرمجة.
K0016	معرفة بقدرات خوارزميات التشفير، وتطبيقاتها.
K0017	معرفة بمبادئ التشفير، وممارساته.
K0018	معرفة بسياسات إدارة البيانات، وإجراءاتها.
K0019	معرفة بسياسات النسخ الاحتياطي للبيانات وإجراءاته، وكيفية واسترجاع البيانات.
K0020	معرفة بنظم قواعد البيانات، وبرمجياتها.
K0021	معرفة بسياسات الأعمال والتعافي من الكوارث، وإجراءات الاستمرارية.
K0022	معرفة بمبادئ معمارية الأمن السيبراني بالمنظمة، وممارساته.

رمز المعرفة	الوصف
K0024	معرفة بنظم التحكم في الوصول إلى المضيف، وبرمجياته.
K0025	المعرفة بمبادئ الاتصالات إلى الشبكة، وممارساته.
K0027	معرفة بمبادئ التفاعل بين الإنسان والحاسوب، وممارساته.
K0028	معرفة بعمليات التصريح والتقييم للأمن السيبراني.
K0029	معرفة بمبادئ إدارة المخاطر، وممارساتها.
K0030	معرفة بمبادئ تطوير البرمجيات من منظور الأمن السيبراني، وكذلك المعرفة بممارساته.
K0031	معرفة بمصادر المعلومات؛ لتحديد الثغرات ومعالجتها بفاعلية.
K0032	معرفة بمبادئ الاستجابة للحوادث، وممارساتها.
K0034	معرفة بطرق إجراء تحليل، لأفضل الممارسات.
K0035	معرفة بمبادئ السرية والسلامة والتوافر، وممارساتها.
K0037	معرفة بسياسات إدارة المخاطر، وإجراءاتها.
K0039	معرفة بلغات البرمجة الحاسوبية الأولية.
K0042	معرفة بمبادئ إدارة الهوية والوصول، وممارساتها.
K0043	المعرفة بأدوات تحليل حركة المرور عبر الشبكات، وتقنياتها.
K0044	معرفة بالتقنيات الجديدة والناشئة؛ من منظور الأمن السيبراني.
K0045	معرفة بمبادئ نظام التشغيل.
K0046	المعرفة ببروتوكولات حركة مرور البيانات، عبر الشبكات.
K0047	معرفة بأدوات التحليل وتقنياته؛ على مستوى الحزم.
K0048	معرفة مبادئ الحوسبة المتوازية والموزعة، وممارساتها.
K0049	معرفة بضوابط التحكم بالوصول المبنية على السياسات.
K0051	معرفة ببُنى لغات البرامج ومنطقها.

رمز المعرفة	الوصف
K0053	معرفة بمبادئ إدارة الأمن السيبراني، وممارساتها.
K0054	معرفة بأدوات تصميم النُظم، وتقنياته.
K0056	معرفة بجميع جوانب إدارة دورة حياة النظام.
K0057	معرفة بأدوات اختبار النُظم وتقنياتها، وتقييمها.
K0058	معرفة بمبادئ الاتصال عن بعد، وممارساته.
K0059	معرفة بأدوات إدارة البيانات، وتقنياته.
K0061	معرفة بإستراتيجية وأهداف تقنية المعلومات في المنظمة، وتقنياتها.
K0062	معرفة بعمليات هندسة النُظم.
K0063	معرفة بنظم الشبكات الخاصة الافتراضية، وبرمجياتها.
K0064	معرفة بخصائص الهجمة الشبكية.
K0065	معرفة بقوانين التهديدات الداخلية وتنظيماتها.
K0066	معرفة بالمكونات المادية للحاسب الآلي.
K0068	المعرفة بأدوات الشبكات، وتقنياتها.
K0069	معرفة بمبادئ الدفاع الأمني المتعمقة، وممارساته.
K0070	معرفة بأنواع الاتصالات الشبكية.
K0072	معرفة بامتدادات الملفات.
K0073	المعرفة بمبادئ إدارة مخاطر سلسلة الإمداد، وممارساتها.
K0074	معرفة بتنظيمات الأمن السيبراني الوطنية ذات الصلة بالمنظمة، ومتطلباتها.
K0075	معرفة بخصائص بيانات التحليل الجنائي الرقمي
K0076	معرفة بلغات الحوسبة المفسرة والمجمعة.
K0077	معرفة بمصادر المعلومات الاستباقية، للتهديدات، وقدراتها وحدودها.

رمز المعرفة	الوصف
K0078	معرفة بكيفية جمع المعلومات الاستباقية من قبل مصادر المعلومات الاستباقية للتهديدات.
K0080	معرفة بمخاطر الأمن السيبراني الجديدة والناشئة.
K0081	معرفة بالقوانين والأنظمة لضوابط التصدير والتوريد من منظور الأمن السيبراني.
K0083	معرفة بمعايير إدارة مخاطر سلسلة الإمداد، وأفضل الممارسات المتبعة من منظور الأمن السيبراني.
K0084	معرفة بسياسات الأمن السيبراني، وإجراءاته.
K0085	معرفة بسياسات أمن مستخدمي تقنية المعلومات في المنظمة.
K0086	معرفة متجهات الهجمة الشبكية.
K0087	معرفة بخصائص الهجمة السيبرانية.
K0088	معرفة بأنواع المهاجمين السيبرانيين، وقدراتهم، وغاياتهم.
K0090	معرفة بمنهجيات إدارة النُظم، وإدارة الشبكات، وتحصين نظم التشغيل.
K0092	معرفة بسياسات مخاطر سلسلة الإمداد المتعلقة بالأمن السيبراني، وإجراءاته وإدارته.
K0093	معرفة بنُظم المعلومات الحساسة، التي يجري تصميمها بقدر محدود من ضوابط الأمن السيبراني التقنيّة.
K0094	معرفة بأدوات الهندسة العكسية للأجهزة، وتقنياتها.
K0095	معرفة بقدرات البرمجيات الوسيطة، وتطبيقاتها.
K0096	معرفة ببروتوكولات الشبكات.
K0097	معرفة بأدوات الهندسة العكسية للبرمجيات، وتقنياتها.
K0098	معرفة بمخططات لغة التوصيف الموسعة (XML).
K0099	معرفة بمراحل الهجوم السيبراني.
K0100	معرفة مبادئ معمارية أمن الشبكات، وممارساته.
K0101	معرفة بمبادئ إدارة نظم الشبكات، وممارساته.
K0102	معرفة بأدوات التشفير، وتقنياته.

رمز المعرفة	الوصف
K0103	معرفة بمبادئ توقيعات البرامج الضارة، وممارساتها.
K0104	معرفة بمنافذ نظام التشغيل ("ويندوز")، وخدماته.
K0105	معرفة بأدوات معالجة البيانات، وتقنياته.
K0106	معرفة مبادئ الحوسبة السحابية، وممارساتها.
K0107	معرفة بمعايير تصنيف البيانات، وأفضل الممارسات المتبعة.
K0108	معرفة بواجهات برمجة تطبيقات الوصول إلى قواعد البيانات.
K0109	معرفة بمبادئ تحسين العمليات، وممارساتها.
K0111	معرفة بمبادئ إدارة الخدمات، وممارساتها.
K0112	معرفة بمبادئ جدران الحماية للتطبيقات، وممارساتها.
K0113	معرفة بمعايير الأمن السيبراني للقطاع، وأطره.
K0114	معرفة بأدوات الاتصال الخفية، وتقنياته.
K0117	معرفة بنموذج ("ترابط النُظم المفتوحة" /(OSI)).
K0119	معرفة بمبادئ إدارة نظم التشغيل، وممارساتها.
K0120	معرفة بمبادئ معمارية الحاسب الآلي، وممارساتها.
K0121	معرفة بنماذج الخدمات السحابية، وأطرها.
K0123	معرفة بمبادئ تحليل البرمجيات الضارة، وممارساتها.
K0124	معرفة بمعايير أمن البيانات، وأفضل الممارسات، ذات العلاقة بمعلومات المعرفات الشخصية.
K0125	معرفة بمعايير أمن البيانات، وأفضل الممارسات، لقطاع بطاقات الدفع.
K0126	معرفة بمعايير أمن البيانات، المتعلقة بالقطاع، الذي تعمل فيه المنظمة.
K0128	معرفة بالقوانين والتنظيمات الخاصة بالبنية التحتية الحساسة؛ من حيث صلتها بالأمن السيبراني.
K0129	معرفة بأدوات إدارة الإعدادات، وتقنياته.

رمز المعرفة	الوصف
K0132	معرفة بأدوات مزامنة المحتوى، وتقنياته.
K0133	معرفة بأدوات تصنيف بيانات الأمن السيبراني، وتقنياته.
K0134	معرفة بأدوات اختبار نظام الأمن السيبراني، وتقنياته.
K0135	معرفة بالتهديدات والثغرات في أجهزة الشبكة.
K0136	معرفة بمبادئ تصميم التدابير المضادة، وممارساتها.
K0137	معرفة بمبادئ بناء مخططات الشبكات، وممارساتها.
K0139	معرفة باستخدام أدوات الشبكة الجزئية، وتقنياتها.
K0144	معرفة بمبادئ مشاركة معلومات الأمن السيبراني، وممارساتها.
K0145	معرفة بأدوات واجهة أوامر نظام التشغيل، وتقنياتها.
K0146	معرفة بالنُظم المدمجة، وكيفية تطبيق ضوابط الأمن السيبراني عليها.
K0147	معرفة بأدوات نظم كشف التسلل، وتقنياته.
K0149	معرفة بمبادئ تصميم الشبكات، وممارساته.
K0153	معرفة بمبادئ اختبار الاختراق، وممارساته.
K0156	معرفة بمبادئ إدارة قواعد البيانات، وممارساتها.
K0159	معرفة بمبادئ أمن العمليات، وممارساتها.
K0160	معرفة بغايات المنظمة وأولويات القيادة.
K0166	معرفة بمبادئ تصنيف المخاطر، وممارساتها.
K0167	معرفة بأدوات تقييم المخاطر، وتقنياته.
K0169	معرفة بإجراءات الإبلاغ عن انتهاك البيانات.
K0170	معرفة بالبيانات الست عشرية.
K0171	معرفة بأدوات تحليل التعليمات البرمجية، وتقنياتها.

رمز المعرفة	الوصف
K0172	معرفة بمبادئ البنية التحتية للمفاتيح العامة (PKI).
K0173	معرفة بمبادئ وممارسات إدارة الشهادات الرقمية.
K0174	معرفة بعمليات البحث والتصميم، وإجراءاته.
K0175	معرفة بمبادئ جدار الحماية الشبكي، وممارساته.
K0176	معرفة بخوارزميات التشفير.
K0177	معرفة بإعدادات الشبكة.
K0178	المعرفة بأدوات تحليل السلوك، وتقنياته.
K0179	معرفة بأدوات التحقق من الهوية، وتقنياتها؛ عن طريق الخصائص الحيوية.
K0180	معرفة بأدوات منع فقدان البيانات، وتقنياته.
K0181	معرفة بمبادئ أمن إنترنت الأشياء، وممارساته.
K0182	معرفة بأدوات المصادقة ذات العناصر المتعددة وتقنياتها.
K0183	معرفة بمبادئ تقسيم الشبكات، وممارساتها.
K0184	معرفة بأدوات التنسيق والأتمتة والاستجابة الأمنية (SOAR)، وتقنياتها.
K0185	معرفة بمبادئ نموذج "الثقة الصفرية"، وممارساتها.
K0186	معرفة بضوابط الأمن السيبراني.
K0187	معرفة بمبادئ الحد من المخاطر، وممارساتها.
K0188	معرفة بمبادئ حماية البيانات، وممارساتها.
K0189	معرفة بالثغرات في الأمن السيبراني.
K0190	معرفة أساليب التحكم في الوصول.
K0191	معرفة بأدوات تقييم الثغرات، وتقنياتها.
K0192	معرفة بمبادئ إدارة التشفير الرئيسية، وممارساتها.

رمز المعرفة	الوصف
K0193	معرفة بممارسات تصميم قواعد البيانات الآمنة.
K0194	معرفة بنظم التحكم في الوصول إلى الشبكة، وبرامجها.
K0195	معرفة بسياسات الاستجابة للحوادث، وإجراءاتها.
K0196	معرفة بأدوات الاستجابة للحوادث، وتقنياتها.
K0197	معرفة بضوابط التحكم بالوصول التكيفية (القابلة للتكيف) للمخاطر (RADAC).
K0198	معرفة بأدوات التهديدات الداخلية، وتقنياتها.
K0199	معرفة بالمؤشرات التشغيلية للتهديدات الداخلية.
K0200	معرفة بسياسات التهديدات الداخلية، وإجراءاتها.
K0201	معرفة بأساليب التعامل مع التهديدات الداخلية.
K0202	معرفة بأهداف التهديدات الداخلية.
K0203	معرفة بالأجهزة الطرفية للحاسب الآلي.
K0204	معرفة بأفضل أساليب الأمن السيبراني في البرامج المتوسطة.
K0205	معرفة بمبادئ الأمن السيبراني للشبكات، وممارساتها.
K0206	معرفة بمنافذ يونكس، وخدماته.
K0207	معرفة بمبادئ إدارة المعرفة، وممارساتها.
K0208	معرفة بأدوات إدارة المعرفة، وتقنياتها.
K0209	معرفة بنماذج تطوّر العمليات، وأطرها.
K0210	معرفة بمعايير إدارة الخدمات، وأفضل الممارسات المتبعة.
K0211	معرفة بأدوات مشاركة معلومات الأمن السيبراني، وتقنياتها.
K0212	معرفة بأدوات نظام منع التسلل (IPS)، وتقنياته.
K0213	معرفة بأدوات اختبار الاختراق، وتقنياته.

رمز المعرفة	الوصف
K0214	معرفة بوظائف فريق اختبار الاختراق، وقدراته.
K0215	معرفة بقوانين الاستغلال، وتنظيماته.
K0216	معرفة قوانين الدفاع السيبراني، وتنظيماته.
K0500	معرفة بمبادئ البرمجة النصية، وممارساتها.
K0503	معرفة بأجهزة الشبكات ووظائفها.
K0504	معرفة بتقنيات الشبكات.
K0507	معرفة بالنُظم الأمنية ذات المستويات المتعددة (MLS) والحلول المستخدمة في نطاقات مختلفة.
K0509	معرفة بمعمارية الشبكات ذات الطبقات المتعددة، في نظم تقنية المعلومات.
K0510	معرفة بنماذج معمارية تقنية المعلومات، وأطرها.
K0512	معرفة بمبادئ تقييم نظم تقنية المعلومات، وممارستها؛ والتحقق منها.
K0513	معرفة بأدوات تحمل العيوب وتقنياته في نظم تقنية المعلومات.
K0514	معرفة بالمناطق الشبكية المعزولة، في بيئات تقنية المعلومات.
K0516	معرفة بنمذجة التصاميم.
K0517	معرفة بأساليب التصميم.
K0518	معرفة بمتطلبات التبديل التلقائي، أو المواقع البديلة.
K0519	معرفة بمتطلبات النسخ الاحتياطي للنُظم.
K0520	معرفة بأدوات ضبط الأداء، وتقنياته.
K0521	معرفة بأفضل الممارسات الأمنية لتنسيق الحاويات.
K1000	معرفة بهياكل البيانات المعقدة.
K1001	معرفة ممارسات تخزين البيانات، ومبادئه.
K1002	معرفة بنُظم إدارة قواعد البيانات (DBMS).

رمز المعرفة	الوصف
K1003	معرفة بأدوات إدارة الحقوق الرقمية (DRM)، وتقنياتها.
K1005	معرفة بنُظم الاتصالات المؤسسية، وبرمجياتها.
K1006	معرفة ممارسات الصمود والنُظم الرديفة، ومبادئها.
K1007	معرفة معايير هندسة نظم الأمن السيبراني التي تستخدمها المنظمة، ومبادئها.
K1008	معرفة ممارسات الشبكات المحلية (LAN)، ومبادئها.
K1009	معرفة ممارسات هندسة العمليات، ومبادئها.
K1010	معرفة بلغات الاستعلام.
K1011	معرفة بأدوات إدارة الإعدادات الآمنة (CM)، وتقنياتها.
K1012	معرفة بمبادئ تصحيح الأخطاء البرمجية، وممارساتها.
K1013	معرفة بأدوات تصميم البرمجيات، وتقنياتها.
K1014	معرفة بأطر تطوير البرمجيات، ونماذجها.
K1015	معرفة ممارسات هندسة البرمجيات، ومبادئها.
K1016	معرفة بمصادر مجموعات البيانات بالمنظمة وخصائصها واستخداماتها.
K1017	معرفة وممارسات التحليل المنظم، ومبادئه.
K1021	معرفة بأدوات البرمجة الآمنة، وتقنياتها.
K1023	معرفة ممارسات ضمان جودة البرمجيات (SQA)، ومبادئه.
K1024	معرفة بأدوات نشر البرمجيات الآمنة، وتقنياتها.
K1025	معرفة بأدوات التسجيل، وتقنياته.
K1027	معرفة بأدوات تحليل البيانات، وتقنياتها.
K1028	معرفة ممارسات التعلم الآلي، ومبادئه.
K1030	معرفة بمعمارية الاتصالات المتنقلة.

رمز المعرفة	الوصف
K1031	معرفة بهياكل نظم التشغيل، ومكوناتها الداخلية.
K1032	معرفة بأدوات تحليل الشبكات، وتقنياته.
K1034	معرفة بأدوات القرصنة الأخلاقية، وتقنياتها.
K1035	معرفة بمبادئ هندسة الحاسب الآلي، وممارساتها.
K1036	معرفة بمبادئ نظرية المعلومات، وممارساتها.
K1037	معرفة بأدوات تحليل الأسباب الجذرية، وتقنياتها.
K1038	معرفة بإستراتيجيات البحث.
K1039	معرفة بتطوير البرمجيات، بلغات عالية المستوى.
K1040	معرفة بنصوص نظم التشغيل.
K1041	معرفة بتقنيات اختبار التقنيات، وأدواتها.
K1043	المعرفة بأدوات معالجة اللغة الطبيعية، وتقنياتها.
K1045	معرفة بخوارزميات التعلم الآلي.
K1047	المعرفة بالتقنيات ذات المصدر المفتوح.
K1048	معرفة أساليب اختبار البرمجيات.
K1049	معرفة أدوات تخطيط البيانات، وتقنياتها.
K1050	المعرفة بمعايير البرمجة والاختبار.
K1051	المعرفة بمبادئ تصميم الأجهزة، وممارساتها.
K1052	المعرفة بمبادئ تخزين البيانات، وممارساتها.
K1053	المعرفة بمعايير دورة حياة هندسة البرمجيات والنُظم.
K1054	المعرفة بأدوات جمع البيانات، وتقنياته.
K1055	المعرفة بمبادئ الذكاء الاصطناعي، وممارساته.

رمز المعرفة	الوصف
K1056	المعرفة بأدوات الذكاء الاصطناعي، وتقنياته.
K1057	المعرفة بمبادئ أمن واجهة برمجة التطبيقات، وممارساته.
K1058	المعرفة بأدوات الكشف عن التزييف العميق، وتقنياته.
K1059	المعرفة بمبادئ الأمان عبر جميع مراحل تطوير البرامج (DevSecOps)، وممارساته.
K1060	المعرفة أدوات التشفير التماثلي، وتقنياته.
K1061	المعرفة بأدوات منع التصيد الاحتيالي، وتقنياته.
K1062	المعرفة بتحديات التشفير الكمي، وفرصه.
K1063	المعرفة بمبادئ توزيع المفاتيح الكمية (QKD)، وممارساتها.
K1064	المعرفة بأدوات إدارة المعلومات الأمنية والأحداث (SIEM)، وتقنياته.
K1065	المعرفة بمبادئ استخراج البيانات، وممارساته.
K1066	المعرفة بقدرات لغة الاستعلام في قواعد البيانات، وتطبيقاته.
K1067	المعرفة بقدرات مخطط قاعدة البيانات، وتطبيقاته.
K1068	المعرفة بمبادئ الشبكات الواسعة (WAN)، وممارساتها.
K1069	المعرفة أدوات العرض المرئي للبيانات، وتقنياته.
K1500	المعرفة بمؤشرات أداء النُظم.
K1501	المعرفة بمبادئ إدارة الموارد، وممارساتها.
K1502	المعرفة بمبادئ إدارة الخوادم، وممارساتها.
K1503	المعرفة ببنُية العميل والخادم.
K1504	المعرفة بمعايير تصميم النُظم، وأفضل الممارسات المتبعة.
K1505	المعرفة بعمليات دمج التقنيات.
K1506	معرفة بمبادئ إدارة البرامج، وممارساتها.

رمز المعرفة	الوصف
K1509	معرفة بمبادئ شراء تقنيات المعلومات، وممارساتها.
K1510	معرفة بأدوات المراقبة المستمرة، وتقنياتها.
K1511	معرفة بضوابط أمن البيانات.
K1512	معرفة بتدابير توافر النُظم.
K1513	معرفة بنظم تشغيل الأجهزة المحمولة.
K1514	معرفة بسياسات تصميم النُظم، وممارساتها.
K1515	معرفة بمبادئ إدارة المشاريع، وممارساتها.
K2000	معرفة بأطر النطاقات المعرفية، ونماذجها.
K2001	معرفة بأدوات المحاكاة الافتراضية، وتقنياتها.
K2002	معرفة بأدوات تقدير التعلّم، وتقنياته.
K2004	معرفة بمبادئ التصميم التعليمي، وممارساته.
K2005	معرفة بأفضل الممارسات التدريبية.
K2007	معرفة بنُظم نظام إدارة التعلّم (LMS)، وبرمجياته.
K2009	معرفة بطرق التعلّم.
K2010	معرفة بنُظم التدريب، وبرمجياته.
K2011	معرفة بالأدوار الوظيفية في الإطار السعودي، لكوادر الأمن السيبراني، المهمات، والمعارف، والمهارات المرتبطة بها.
K2012	معرفة بأدوات إنتاج الوسائط، وتقنياتها.
K2013	معرفة بسياسات الموارد البشرية في المنظمة، وكذلك عملياتها وإجراءاتها.
K2014	معرفة بسياسات التدريب وإجراءاته والتعليم في المنظمة.
K2015	معرفة بمبادئ تقييم احتياجات التدريب، وممارساته.
K2020	معرفة ببدائل التدريب التقنية للأمن السيبراني، وتمارينها، وحدود قدراتها.

رمز المعرفة	الوصف
K2021	معرفة بتمارين الأمن السيبراني، ومنافساته.
K2022	معرفة باحتياجات كوادر الأمن السيبراني بالمنظمة.
K2023	معرفة بكوادر الأمن السيبراني بالمنظمة.
K2024	معرفة بسياسات كوادر الأمن السيبراني وإجراءاته.
K2025	معرفة بأهداف الأمن السيبراني للمنظمة، وغاياته.
K2026	معرفة بالمسارات الوظيفية للأمن السيبراني.
K2027	معرفة باتجاهات كوادر الأمن السيبراني.
K2028	معرفة بنماذج التصميم التعليم، وأطره.
K2029	معرفة بالتدرج الوظيفي في المنظمة.
K2030	معرفة بأدوار موظفي الأمن السيبراني، ومسؤولياتهم.
K2031	معرفة بممارسات ضمان تحقيق الرسالة، ومبادئه.
K2032	معرفة بنظم إدارة الموظفين، وبرمجياتها.
K2033	معرفة بمبادئ برامج التوعية بالأمن السيبراني، وممارساتها.
K2034	معرفة بأدوات محاكاة التصيد الاحتيالي، وتقنياته.
K2035	معرفة بتقنيات الأنشطة التفاعلية، وتطبيقاتها في برامج التدريب، والتوعية بالأمن السيبراني.
K2036	معرفة بأساليب تقييم مستوى الوعي بالأمن السيبراني،
K2037	معرفة بأفضل الممارسات المتبعة، في مجال التوعية بالأمن السيبراني.
K2501	معرفة بطرق تقييم ملاءمة التقنيات.
K2502	معرفة ممارسات معمارية تقنية المعلومات المؤسسية للمنظمة، ومبادئها.
K2504	معرفة بسياسات إعداد تقارير المعلومات الاستباقية من جميع المصادر، وإجراءات ذلك.
K2505	معرفة بسياسات التدقيق، وإجراءاته.

رمز المعرفة	الوصف
K2506	معرفة بقوالب التقارير؛ لإعداد تقارير الالتزام للأمن السيبراني، لصالح الشركاء الخارجيين.
K2507	معرفة بقوالب التقارير، المعتمدة بالمنظمة؛ للإبلاغ عن مخاطر الأمن السيبراني والالتزام.
K2509	معرفة بقوانين التدقيق، وتنظيماته.
K2510	معرفة بمعايير الاعتماد المحلية والدولية.
K2511	معرفة بمشهد المخاطر الحالي للمنظمة.
K2512	معرفة بتنظيمات نقل البيانات عبر الحدود، بما في ذلك متطلبات إقامة البيانات، وسيادتها، وتوطينها.
K2513	معرفة بمبادئ التأمين السيبراني، وممارساته.
K2514	معرفة بأدوات اكتشاف التهديدات وتقنياته على الأجهزة الطرفية، والاستجابة لها (EDR).
K2515	معرفة بأدوات الكشف والاستجابة وتقنياتها الموسعة (XDR).
K2516	معرفة بسياسات التسجيل، وإجراءاته.
K3000	معرفة بمبادئ معالجة البيانات الجنائية الرقمية، وممارساتها.
K3001	معرفة بمبادئ جمع المعلومات الاستباقية.
K3002	معرفة بسياسات المنظمة، وإجراءات التشغيل الموحدة، المتعلقة بالأمن السيبراني.
K3005	معرفة بأدوات تعزيز حماية البيانات، وتقنياتها.
K3008	معرفة بالجهات المعنية، بتنظيم حماية البيانات.
K3009	معرفة بسياسات حماية البيانات وإجراءاتها بالمنظمة.
K3010	معرفة بضوابط حماية البيانات.
K3011	معرفة بسياسات جمع البيانات الاستباقية، وإجراءاتها.
K3012	معرفة بقوانين جمع البيانات الاستباقية، وتنظيماتها.
K3502	معرفة بأدوات تشويش الإشارة، وتقنياتها.
K3506	معرفة بأدوات تحليل البروتوكولات، وتقنياتها.

رمز المعرفة	الوصف
K3507	معرفة بخطط المنظمة، للاستجابة لحوادث الأمن السيبراني.
K3508	معرفة بأدوات الدفاع وتقنياتها، ضد تهديدات برامج الفدية.
K3509	معرفة بقوانين تشويش الإشارة، وتنظيماتها.
K4000	معرفة بمبادئ الوصول عن بعد، وممارساتها.
K4001	معرفة القدرات، والوظائف، المرتبطة بتقنيات إنشاء المحتوى.
K4002	معرفة بوظائف تقنيات العمل التعاوني وقدراتها؛ وآثارها على الأمن السيبراني.
K4004	معرفة بعلم التصنيف، وعلم الدلالية.
K4006	معرفة بطرق، تقييم الموردين، والمنتجات.
K4007	معرفة بفهارس خدمات تقنية المعلومات.
K4008	معرفة بنظم إدارة اعتماد المستخدم، وبرمجياتها.
K4009	معرفة بمعايير تشفير البيانات، أثناء التخزين (DARE) وأفضل الممارسات المتبعة.
K4011	معرفة بأدوات إخفاء البيانات، وتقنياتها.
K4012	معرفة بأدوات استخراج البيانات، وتقنياتها.
K4015	معرفة بأدوات الشبكات المحلية اللاسلكية (WLAN)، وتقنياتها.
K4016	معرفة بسياسات إعداد التقارير، وإجراءاتها.
K4017	معرفة بأدوات التعتيم، وتقنياته.
K4019	معرفة بمتطلبات توافر النظام.
K4020	معرفة بمبادئ التشفير المتماثلة، وممارساته.
K4021	معرفة بمبادئ التحكم وممارساته، في الوصول، القائم على السمات (ABAC).
K4022	معرفة بمبادئ وسيط أمان الوصول إلى السحابة (CASB)، وممارساته.
K4023	معرفة بمبادئ التحكم في الوصول التقديري (DAC)، وممارساته.

رمز المعرفة	الوصف
K4024	معرفة بمبادئ مصادقة كيربيروس (Kerberos) ، وممارساته.
K4025	معرفة بمبادئ التحكم الإلزامي في الوصول (MAC)، وممارساته.
K4026	معرفة بمبادئ التحكم وممارساته في الوصول، وفقاً للأدوار الوظيفية (RBAC).
K4027	معرفة بأدوات حافة خدمة الوصول الآمن (SASE)، وتقنياته.
K4028	معرفة بمبادئ تسجيل الدخول الأحادي (SSO)، وممارساته.
K4029	معرفة بأدوات وتقنيات تسجيل الدخول الأحادي (SSO).
K4030	معرفة بأدوات الوصول عن بعد، وتقنياته.
K4504	معرفة بلغات البرمجة.
K4505	معرفة بأدوات نظم التشغيل، وتقنياتها.
K4506	معرفة بأدوات الهندسة الاجتماعية، وتقنياتها.
K4508	معرفة بأدوات إدارة نظم الشبكات، وتقنياتها.
K4511	معرفة بمبادئ تكتيكات الخصوم وممارساتها في الأمن السيبراني.
K4512	معرفة بأدوات تكتيكات الخصوم وممارساتها في الأمن السيبراني.
K4513	معرفة بسياسات تكتيكات الخصوم وإجراءاتها في الأمن السيبراني.
K4514	معرفة مبادئ تشكيل الفرق الحمراء، والزرقاء، والبنفسجية، وأساليب ممارساتها.
K5000	معرفة بأدوات تشخيص الخوادم، وتقنياتها.
K5001	معرفة بالأنواع الرئيسية للأجهزة الإلكترونية، وقدراتها.
K5002	معرفة بمبادئ تنفيذ نظم الملفات، وممارساتها.
K5003	معرفة بسياسات احتجاز الأدلة الرقمية، وإجراءاتها.
K5006	معرفة بسياسات حفظ الأدلة الرقمية، وإجراءاتها.
K5007	معرفة بسياسات تسلسل حجز الأدلة، وإجراءاته.

رمز المعرفة	الوصف
K5008	معرفة بمبادئ البيانات المستديمة، وممارساتها.
K5009	معرفة بأدوات البريد الإلكتروني، وتقنياته.
K5010	معرفة بخصائص ملفات النظام.
K5011	معرفة بمبادئ إدارة التحليل الجنائي القابلة للتطبيق، وممارساتها.
K5012	معرفة بنظم الترشيح للشبكة العنكبوتية، وبرمجياتها.
K5014	معرفة بأدوات ربط الأحداث الأمنية، وتقنياتها.
K5015	معرفة بقوانين الأدلة الإلكترونية، وتنظيماتها.
K5016	معرفة بالإجراءات الوطنية، أو المعمول بها في القضاء، والمحاكم، في قضايا الجرائم السيبرانية، وجرائم الاحتيال.
K5017	معرفة بأدوات استخراج البيانات، وأساليبها.
K5019	معرفة بالأدوات المضادة للأدلة الجنائية، وأساليبها.
K5020	معرفة بمبادئ تصميم المختبرات الجنائية، وأساليبها.
K5021	معرفة بأدوات تصحيح الأخطاء، وتقنياتها.
K5022	معرفة بحالات العبث بامتداد اسم الملف.
K5023	معرفة بأدوات تحليل البرمجيات الضارة، وتقنياتها.
K5024	معرفة بأدوات الكشف عن الآلات الافتراضية، وتقنياتها.
K5025	معرفة ببروتوكولات إدارة الأزمات.
K5026	معرفة بالسلوكيات الجسدية والفسيولوجية، التي قد تشير إلى نشاط مشبوه أو غير طبيعي.
K5028	معرفة بأدوات التحليل الثنائي، وتقنياته.
K5031	معرفة بمبادئ التصميم التشغيلي، وممارساته.
K5032	معرفة بقوانين جمع المعلومات الاستباقية، وتنظيماتها.
K5033	معرفة بأدوات إدارة التحليل الجنائي الرقمي، وتقنياتها.

رمز المعرفة	الوصف
K5034	معرفة بمبادئ سلامة البيانات، وممارساتها.
K5035	معرفة بطرق تنقيح المعلومات.
K5036	معرفة بمبادئ الإخفاء المعلوماتي، وممارساتها.
K5037	معرفة بعمليات تسلسل حجز الأدلة.
K5038	معرفة بأدوات الكشف عن الأعطال، وتقنياتها، وتشخيصها (FDD).
K5039	معرفة بأدوات إدارة التحليل الجنائي القابلة للتطبيق، وتقنياتها.
K5040	معرفة بنظم تصميم المختبرات الجنائية، وبرمجياتها.
K5041	معرفة بإجراءات إدارة الأزمات.
K5042	معرفة بأدوات إدارة الأزمات، وتقنياتها.
K5501	معرفة بقدرات نظم إدارة المحتوى (CMS)، وتطبيقاتها.
K5502	معرفة بأدوات الهجوم السيبراني، وتقنياته.
K5503	معرفة بسياسات تصنيف البيانات، وإجراءاته.
K5505	معرفة بمبادئ شبكات الحاسبات، وممارساتها.
K5510	معرفة بمبادئ العمليات السيبرانية، وممارساتها.
K5511	معرفة بالمنتجات الأمنية، المخصصة للاستضافة وقدراتها.
K5513	معرفة بالتهديدات، والمخاطر، المتعلقة بنظم الاتصالات، عبر الإنترنت.
K5514	معرفة بالتهديدات، والمخاطر، المتعلقة بالشبكات اللاسلكية.
K5516	معرفة بمختلف أنواع المؤسسات، والفرق، والأفراد المشاركين في جمع المعلومات الاستباقية، عن التهديدات السيبرانية.
K5519	معرفة بالخطط، التي يمكن للمنظمة تسخيرها؛ للتنبؤ بقدرات المهاجمين وأعمالهم، ومن ثم مكافحتها.
K5520	معرفة مبادئ عنونة الشبكات، وممارساتها.
K5521	معرفة بالجهات، التي تمثل مصدرًا للتهديدات السيبرانية.

رمز المعرفة	الوصف
K5522	معرفة بإجراء تحليل لبيئة التهديدات.
K5523	معرفة بالبرمجيات الضارة.
K5524	معرفة بسياسات اتخاذ القرار السيبراني، وإجراءاته.
K5525	معرفة بوظائف الجهات وقدراتها، مصدرًا للتهديدات السيبرانية.
K5526	معرفة بأدوات الجهات وقدراتها، التي تمثل مصدرًا للتهديدات السيبرانية.
K5529	معرفة بعوامل التهديد، التي يمكن أن تؤثر على عمليات الجمع.
K5531	معرفة بنظم التهديد السيبراني، وبرمجياته.
K5532	معرفة بأدوات المحاكاة الافتراضية الآلية، وتقنياتها.
K5535	معرفة بأدوات الحجب والخداع، وتقنياتها.
K5536	معرفة بالأدوات والتقنيات التحليلية.
K5537	معرفة بمبادئ رصد التهديدات، وممارساته.
K6002	معرفة بقدرات منتجات الأمن السيبراني ووظائفها في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
K6003	معرفة بمعايير إدارة مخاطر الأمن السيبراني وممارساتها، في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
K6004	معرفة بالنُظم الأمنية ذات المستويات المتعددة، والحلول المستخدمة، في نطاقات مختلفة، في بيئات تقنية المعلومات، ونظم التحكم الصناعية، والتقنيات التشغيلية.
K6005	معرفة بتدابير التخطيط؛ لحماية النظام في بيئات تقنية المعلومات، ونظم التحكم الصناعية، والتقنيات التشغيلية.
K6006	معرفة بمعمارية الشبكات ذات الطبقات المتعددة، في بيئات تقنية المعلومات ونظم التحكم الصناعية، والتقنيات التشغيلية.
K6007	معرفة بالمفاهيم، والأنماط المعمارية، في بيئات تقنية المعلومات، ونظم التحكم الصناعية، والتقنيات التشغيلية.
K6009	معرفة بمعايير التقييم والمصادقة، ذات العلاقة بنطاقات بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
K6010	معرفة بمنهجيات تحمل العيوب بالنُظم، في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
K6011	معرفة بالمناطق الشبكية، المعزولة في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
K6012	معرفة بنُظم التحكم الإشرافي وحيازة البيانات (SCADA)، وبرمجياتها.

رمز المعرفة	الوصف
K6013	معرفة بهيكل الشبكات الرقمية، والهاتفية الحديثة، ومعماريتها وتصميمها، في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
K6014	معرفة ببيئات تشغيل نظم التحكم الصناعية، والتقنيات التشغيلية، ووظائف هذه البيئات.
K6015	معرفة ببروتوكولات حركة مرور البيانات، خلال شبكات نظم التحكم الصناعية، والتقنيات التشغيلية.
K6016	معرفة بأجهزة نظم التحكم الصناعية، والتقنيات التشغيلية.
K6017	معرفة بنطاق التهديدات، المرتبطة بنظم التحكم الصناعية، والتقنيات التشغيلية.
K6019	معرفة بأدوات كشف التسلل (IDS) وأساليبه، لكشف حالات التسلل إلى بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
K6020	معرفة بأدوات أمن نظم التحكم الصناعية، وتقنياته.
K6021	معرفة بطرق التصميم، لبيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
K6022	معرفة بلغات برمجة بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.
K6023	معرفة بأدوات كشف التسلل (IDS) وتقنياته؛ لكشف حالات التسلل إلى بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.

جدول ١٠: أوصاف المعارف

رمز المهارة	وصف المهارات	مهارة فنية
S0001	مهارة أداء مسوحات الثغرات الأمنية.	نعم
S0002	مهارة تحديد البرمجيات الضارة.	نعم
S0003	مهارة تطبيق تقنيات المعلومات ودمجها في الحلول المقترحة.	نعم
S0004	مهارة تطبيق مبادئ الأمن السيبراني الأساسية.	نعم
S0005	مهارة تطبيق ضوابط الاستضافة، والتحكم في الوصول إلى الشبكة.	نعم
S0006	مهارة تطوير التوقيعات الرقميّة.	نعم
S0008	مهارة تصميم دمج حلول الأجهزة والبرمجيات.	نعم
S0009	مهارة كشف التسلل، لكشف عمليات التسلل، ذات العلاقة بالاستضافة والشبكات.	نعم
S0011	مهارة تطوير خطط الطوارئ، والتعافي، للبنية التحتية للشبكات.	نعم
S0012	مهارة تقييم تصاميم نظام الأمن السيبراني.	نعم
S0013	مهارة الحفاظ على سلامة الأدلة الرقمية.	نعم
S0014	مهارة ضبط إعدادات أجهزة استشعار الشبكة.	نعم
S0015	مهارة استخدام أدوات تحليل البروتوكولات.	نعم
S0016	مهارة ضبط إعدادات اتصالات الشبكة المشفرة.	نعم
S0017	مهارة كتابة البرامج، بلغة برمجة مدعومة حاليًا	نعم
S0018	مهارة حل المشكلات.	لا
S0019	مهارة صيانة الآلات الافتراضية.	نعم
S0020	مهارة إجراء التحليلات الجنائية الرقمية.	نعم
S0021	مهارة ضبط إعدادات أدوات الحماية الحاسوبية واستخدامها.	نعم

S0022	مهارة تأمين اتصالات الشبكات.	نعم
S0023	مهارة تصنيف أنواع الثغرات الأمنية.	نعم
S0025	مهارة تقييم الأضرار.	نعم
S0026	مهارة استخدام أدوات تحليل بيانات الشبكات.	نعم
S0027	مهارة ضبط إعدادات مكونات حماية الشبكات.	نعم
S0028	مهارة إجراء عمليات تدقيق الأمن السيبراني، أو المراجعات الأمنية للنُظم التقنية.	نعم
S0029	مهارة استخدام أدوات تحليل النصوص الثنائية.	نعم
S0030	مهارة تنفيذ وظائف التجزئة، أحادية الاتجاه.	نعم
S0031	مهارة قراءة البيانات الست عشرية.	نعم
S0032	مهارة تحديد تقنيات التشفير الشائعة.	نعم
S0033	مهارة قراءة التوقيعات الرقميّة.	نعم
S0034	مهارة تطوير أنشطة التعلّم.	لا
S0035	مهارة تطبيق تقنيات التحصين.	نعم
S0036	مهارة تصميم خطط اختبار الأمن السيبراني.	نعم
S0037	مهارة إجراء تقييمات، لثغرات التطبيقات.	نعم
S0038	مهارة تنفيذ تشفير البنية التحتية، للمفاتيح العامة (PKI).	نعم
S0039	مهارة تطبيق نماذج الأمن السيبراني.	نعم
S0040	مهارة تقييم الضوابط الأمنية، المستندة إلى مبادئ الأمن السيبراني.	نعم
S0041	مهارة إجراء تحليلات على مستوى الحزم.	نعم
S0044	مهارة إجراء تقييمات المخاطر.	نعم

S0045	مهارة تطبيق تقنيات البرمجة الآمنة بفاعلية.	نعم
S0046	مهارة استخدام، أدوات ربط الأحداث الأمنية بفاعلية.	نعم
S0047	مهارة استخدام، أدوات تحليل الشفرات البرمجية بفاعلية.	نعم
S0048	مهارة إجراء تحليل الأسباب الجذرية لقضايا الأمن السيبراني.	نعم
S0049	مهارة إجراء البحث باستخدام الشبكة العنكبوتية، العميقة، بأمان وفاعلية.	نعم
S0050	مهارة تحليل النظام المستهدف بفاعلية.	نعم
S0051	مهارة إعداد الملخصات وتقديمها بفاعلية ووضوح، واختصار.	لا
S0052	مهارة التعرف على نشاط الشبكة الضار، في حركة البيانات وتفسيرها.	نعم
S0053	مهارة الهندسة العكسية للبرمجيات الضارة.	نعم
S0054	مهارة تحليل الأدوات، والتقنيات، والإجراءات المستخدمة من قبل الخصوم عن بعد؛ لاستغلال الهدف، والثبات فيه.	نعم
S0055	مهارة تطبيق الملحوظات الواردة، لتحسين عمليات الأمن السيبراني، ومنتجاته، وخدماته.	لا
S0056	مهارة تحليل مصادر التهديد.	نعم
S0057	مهارة سد الفجوة، بين المعلومات الاستباقية، حول التهديدات، وفعالية الإستراتيجية.	لا
S0058	مهارة التواصل بفاعلية.	لا
S0059	مهارة تحديد تهديدات الأمن السيبراني.	نعم
S0060	مهارة الاستجابة بفاعلية، لحوادث الأمن السيبراني، في بيئة الحوسبة السحابية.	نعم
S0061	مهارة تطبيق مبادئ السرية، والسلامة، والتوافر (CIA).	نعم
S0062	مهارة استخدام تقنيات إدارة المخاطر.	نعم
S0063	مهارة الاستفادة من مقدمي خدمات الدفاع السيبراني.	نعم
S0064	مهارة تحديد قضايا الأمن السيبراني، في سلسلة الإمداد الخاصة بالمنظمة.	نعم

S0065	مهارة تصميم العمليات، والحلول السيبرانية.	نعم
S0066	مهارة البرمجة عالية المستوى.	نعم
S0067	مهارة البرمجة منخفضة المستوى.	نعم
S0068	مهارة تحليل إعدادات البرمجيات.	نعم
S0069	مهارة تحليل تدفق البيانات، عبر الشبكة.	نعم
S0070	مهارة تحديد عيوب البرمجة، المتعلقة بالأمن السيبراني.	نعم
S0071	مهارة تصميم معمارية شبكية آمنة.	نعم
S0072	مهارة تطبيق أدوات وأساليبها وتقنياتها تصميم النُظم.	نعم
S0073	مهارة دمج متطلبات الأمن السيبراني، في عملية الاستحواذ.	لا
S0074	مهارة تصميم معمارية آمنة.	نعم
S0075	مهارة تصميم الأطر.	لا
S0076	مهارة الحد من أساليب الخداع، في إعداد التقارير، والتحليلات.	لا
S0077	مهارة تطبيق التفكير النقدي.	لا
S0078	مهارة تحديد الأولويات.	لا
S0079	مهارة إنشاء برنامج إدارة المخاطر.	لا
S0080	مهارة وضع إستراتيجية إدارة المخاطر.	لا
S0081	مهارة إنشاء برنامج داخلي، لمشاركة المعلومات.	لا
S0082	مهارة تحديد نظم المعلومات الحساسة.	نعم
S0083	مهارة تثبيت ترقيات النُظم، والمكونات.	نعم
S0084	مهارة تحسين أداء النُظم.	نعم

S0085	مهارة اختبار خطط النسخ الاحتياطي والتعافي من الكوارث.	نعم
S0086	مهارة نشر مفاهيم الأمن السيبراني وممارساته بفاعلية.	لا
S0087	مهارة تطوير إستراتيجية الأمن السيبراني.	لا
S0088	مهارة وضع سياسات الأمن السيبراني.	لا
S0089	مهارة تطبيق إستراتيجية وممارسات إدارة المخاطر.	نعم
S0090	مهارة مشاركة أفضل الممارسات، بين المنظمات.	لا
S0091	مهارة التعامل مع السجلات الأمنية.	نعم
S0092	مهارة تحديد الثغرات في النُظم الأمنية.	نعم
S0093	مهارة اكتشاف البرمجيات الضارة.	نعم
S0094	مهارة احتواء البرمجيات الضارة.	نعم
S0095	مهارة الإبلاغ عن البرمجيات الضارة.	نعم
S0096	مهارة تطبيق ضوابط الوصول إلى الشبكات.	نعم
S0097	مهارة نشر التوقيعات الرقمية.	نعم
S0098	مهارة اختبار خطط الطوارئ، والتعافي، للبنية التحتية للشبكات.	نعم
S0099	مهارة تنفيذ خطط الطوارئ، والتعافي، للبنية التحتية للشبكات.	نعم
S0100	مهارة استخدام وظائف التجزئة؛ أحادية الاتجاه.	نعم
S0101	مهارة تفسير التوقيعات الرقمية.	نعم
S0102	مهارة قراءة تقارير تقييم الثغرات، في التطبيقات.	نعم
S0103	مهارة العرض على الفئات المستهدفة.	لا
S0104	مهارة تفسير نشاط الشبكة الضار، في حركة مرور البيانات.	نعم

S0106	مهارة دمج العمليات، والحلول السيبرانية.	نعم
S0501	مهارة تصميم النماذج.	نعم
S0503	مهارة تصميم حلول أمنية؛ متعددة المستويات.	نعم
S0504	مهارة استخدام منهجيات التصميم.	نعم
S0505	مهارة ترجمة المتطلبات التشغيلية، إلى ضوابط أمنية.	نعم
S0506	مهارة تنفيذ عملية الفصل بين الشبكات.	نعم
S0507	مهارة تحليل معمارية الأمن السيبراني.	نعم
S0508	مهارة تحليل احتياجات المستخدم.	لا
S0509	مهارة تحليل معمارية تقنية المعلومات المؤسسية، في المنظمة.	نعم
S0510	مهارة بناء حالات الاستخدام.	نعم
S0511	مهارة تصميم الحلول العابرة للنطاقات.	نعم
S1000	مهارة تطوير الخوارزميات.	نعم
S1001	مهارة تصحيح أخطاء البرمجيات.	نعم
S1002	مهارة إنشاء النماذج الرياضية.	نعم
S1003	مهارة التحقق من المدخلات، ومصادقتها.	نعم
S1004	مهارة تصميم ضوابط الأمن السيبراني.	نعم
S1005	مهارة تطوير قواميس البيانات.	نعم
S1006	مهارة تطوير نماذج البيانات.	نعم
S1007	مهارة تطوير ضوابط التحكم بالوصول، لنظام الأمن السيبراني.	نعم
S1008	مهارة تحديد احتياجات الحماية، لنُظم المعلومات، وشبكاتها.	نعم

S1009	مهارة إعداد التقارير.	لا
S1010	مهارة تطبيق أساليب اختبار البرمجيات.	نعم
S1012	مهارة المعالجة المسبقة للبيانات.	نعم
S1013	مهارة تحديد الأنماط، أو العلاقات المخفية.	نعم
S1014	مهارة إجراء تحويلات على التنسيق.	نعم
S1015	مهارة إجراء تحليل للحساسية.	نعم
S1016	مهارة تطوير علم أدلة تفهمه الآلات.	نعم
S1017	مهارة إجراء تحليل الانحدار.	نعم
S1018	مهارة إجراء تحليل التحول.	نعم
S1019	مهارة استخدام الإحصاءات الوصفية.	نعم
S1020	مهارة إجراء تحليل البيانات.	نعم
S1021	مهارة إجراء تخطيط البيانات.	نعم
S1022	مهارة معرفة القيم الشاذة، وتقنيات التخلص منها.	نعم
S1023	مهارة كتابة البرامج النصية الحاسوبية لأتمتة المهمات.	نعم
S1024	مهارة إجراء عملية هندسة النُظم.	نعم
S1026	مهارة معالجة الأخطاء في التطبيقات.	نعم
S1028	مهارة البحث، لاستخلاص المعلومات الاستباقية، ذات المصدر المفتوح (OSINT).	نعم
S1029	مهارة التنقيب عن البيانات.	نعم
S1030	مهارة تقييم أصول بيانات المنظمة.	نعم
S1031	مهارة تصميم النُظم، المبنية على الكائنات.	نعم

S1032	مهارة استخدام نظم التحكم بالإصدارات.	نعم
S1034	مهارة تصميم أنظمة التحليل المؤتمتة.	نعم
S1035	مهارة إجراء البحوث.	لا
S1036	مهارة تطوير نماذج التعلم الآلي.	نعم
S1038	مهارة تحديد البصمات الرقمية الجنائية.	نعم
S1039	مهارة تحليل الشفرات البرمجية الثابتة.	نعم
S1040	مهارة إجراء المقابلات مع العملاء.	لا
S1041	مهارة التخزين المؤقت للبيانات.	نعم
S1042	مهارة تصنيف البيانات.	نعم
S1043	مهارة تجميع البيانات.	نعم
S1044	مهارة توزيع البيانات.	نعم
S1045	مهارة استرجاع البيانات.	نعم
S1046	مهارة تصميم حلول تخزين البيانات.	نعم
S1047	مهارة تنفيذ حلول تخزين البيانات.	نعم
S1048	مهارة إجراء التحليل الكمي.	نعم
S1049	مهارة إجراء تحليل الفجوات.	لا
S1050	مهارة إنشاء هياكل البيانات المعقدة.	نعم
S1051	مهارة استخدام أدوات عرض البيانات.	نعم
S1052	مهارة نشر البرمجيات بشكل آمن.	نعم
S1053	مهارة ضبط إعدادات التسجيل الآمن.	نعم

S1054	مهارة تحليل هياكل البيانات.	نعم
S1055	مهارة إنشاء النماذج الإحصائية.	نعم
S1056	مهارة استخدام النماذج الرياضية.	نعم
S1057	مهارة استخدام النماذج الإحصائية.	نعم
S1058	مهارة إجراء تحليل التنقيب عن البيانات.	نعم
S1059	مهارة تطوير النُظم المبنية على الكائنات.	نعم
S1060	مهارة تطوير نظم التحليل المؤتمتة.	نعم
S1500	مهارة تطوير سياسات أمن النُظم.	نعم
S1501	مهارة تقييم موثوقية الموردين الخارجيين.	لا
S1502	مهارة تحديد التقنيات الجديدة، باستمرار، وتأثيرها المحتمل على متطلبات الأمن السيبراني.	نعم
S1504	مهارة التعاون مع أصحاب المصلحة الداخليين، والخارجيين.	لا
S1505	مهارة دمج متطلبات الأمن السيبراني في عمليات المشتريات.	لا
S1506	مهارة تحديد التحديات التقنية، المتعلقة بالأمن السيبراني في المنظمة.	لا
S1507	مهارة تحديد تحديات الأعمال المتعلقة بالأمن السيبراني في المنظمة.	لا
S1508	مهارة تصميم مركز الدمج الأمني وإدارته.	لا
S1509	مهارة تصميم مركز العمليات الأمنية (SOC) وإدارته.	لا
S1510	مهارة تقييم موثوقية منتجات الموردين الخارجيين.	نعم
S1511	مهارة إجراء تحليل التكلفة مقابل العائد.	نعم
S2001	مهارة استخدام تقنيات إدارة المعرفة.	نعم
S2002	مهارة إجراء تحليل حركة مرور البيانات؛ عبر الشبكات.	نعم

S2003	مهارة تطوير مناهج التدريب التقني.	لا
S2004	مهارة تحديد الفجوات في القدرات التقنية.	لا
S2006	مهارة استخدام التقنيات لأغراض تقديرية.	نعم
S2008	مهارة تطوير متطلبات التأهيل الوظيفي.	لا
S2010	مهارة الكتابة الفنية المتقنة.	لا
S2011	مهارة نشر الآلات الافتراضية.	نعم
S2012	مهارة تقييم مستوى فهم المتدرب.	لا
S2013	مهارة تقديم الملحوظات الفعالة للمتدربين.	لا
S2014	مهارة تطوير المواد التدريبية.	لا
S2015	مهارة تقييم متطلبات الكوادر الوظيفية والتنبؤ بها.	لا
S2016	مهارة تطوير المسارات الوظيفية.	لا
S2017	مهارة تقييم توجهات الكوادر.	لا
S2018	مهارة تنفيذ أدوات واجهة أوامر نظام التشغيل.	نعم
S2019	مهارة استخدام نظم الاتصالات الإلكترونية.	نعم
S2020	مهارة إجراء تقييم الاحتياجات التدريبية.	لا
S2021	مهارة تكييف الأساليب التعليمية، لاستيعاب مختلف أساليب التعلم، والقدرات، والخلفيات الثقافية.	لا
S2022	مهارة تهيئة بيئة تتسم بالاحترام، والشمول، في الفصول الدراسية؛ تشجع المتدربين على المشاركة والنجاح.	لا
S2023	مهارة تقديم البرامج التدريبية.	لا
S2024	مهارة تطوير البرامج التدريبية.	لا
S2025	مهارة تطوير محتوى التوعية بالأمن السيبراني؛ المصمم خصيصًا، لأوصاف المخاطر، وأدوار المستخدمين المحددة.	نعم

S2026	مهارة تنظيم الحملات الخاصة، بمحاكات التصيد الاحتيالي، وتنفيذها.	نعم
S2027	مهارة تصميم أنشطة التوعية التفاعلية.	نعم
S2028	مهارة تفسير الملحوظات، وبيانات التقييمات، لتعزيز الدورات التدريبية للتوعية.	لا
S2029	مهارة نشر مفاهيم التوعية بالأمن السيبراني، للفئات من غير التقنيين.	لا
S2500	مهارة مراقبة أداء النُظم.	نعم
S2501	مهارة تطبيق ضوابط الأمن السيبراني.	نعم
S2502	مهارة تحديد متطلبات البنية التحتية، الخاصة بإستراتيجيات الاختبار والتقييم (TES).	نعم
S2504	مهارة إدارة أصول الاختبارات.	نعم
S2506	مهارة مراجعة السجلات.	نعم
S2507	مهارة تشخيص الحالات غير الطبيعية في البنية التحتية للدفاع السيبراني ومن ثم معالجتها.	نعم
S2509	مهارة إجراء المراجعات للنُظم؛ من منظور الأمن السيبراني.	نعم
S2512	مهارة تطبيق السياسات؛ التي تحقق أهداف الأمن السيبراني، لأنظمة المنظمة.	نعم
S2513	مهارة تنفيذ أنشطة التخطيط الإداري.	لا
S2516	مهارة تدقيق أجهزة الشبكات.	نعم
S2517	مهارة تحديد الفجوات، والقيود في توفير المعلومات الاستباقية.	نعم
S2520	مهارة تحديد اللغات واللهجات الإقليمية، لمصادر التهديدات.	لا
S2521	مهارة تحديد الأجهزة، التي تعمل ضمن كل مستوى، من مستويات نماذج الإجراءات.	نعم
S2522	مهارة إجراء تحليل البيانات الجغرافية المكانية.	نعم
S2523	مهارة تحديد أولويات المعلومات.	لا
S2524	مهارة تفسير لغات البرمجة المجمعة.	نعم

S2525	مهارة تفسير وتقييم البيانات الوصفية.	نعم
S2526	مهارة تفسير نتائج تتبع مسارات البيانات.	نعم
S2527	مهارة تفسير نتائج مسح الثغرات الأمنية.	نعم
S2529	مهارة إدارة العلاقات مع العملاء.	لا
S2530	مهارة إعداد الخطط.	لا
S2533	مهارة تحليل التقارير، والتوصية بالإجراءات، الواجب اتخاذها.	لا
S2537	مهارة تحليل مجموعة المعلومات الاستباقية.	نعم
S2540	مهارة الوصول إلى المعلومات المتعلقة، بموارد الأمن السيبراني الداخلية والخارجية؛ الحالية واستخداماتها الحالية وأولوياتها.	لا
S2541	مهارة استخدام قواعد البيانات.	نعم
S2542	مهارة مراجعة إستراتيجيات الشركات، أو الوثائق القانونية، أو التنظيمية، أو السياسة المعمول بها؛ لتحديد القضايا التي تتطلب توضيحًا، أو إجراء.	لا
S2543	مهارة تطوير المتطلبات المناسبة، والفعالة، لإثراء عملية انتقاء مصادر المعلومات الاستباقية، للتهديدات السيبرانية، أو نشاط المراقبة.	لا
S2544	مهارة تفسير تقارير مستوى الجاهزية.	لا
S2546	مهارة تحليل التقارير، الداخلية، والخارجية.	لا
S2547	مهارة تصميم إستراتيجيات الاختبار والتقييم (TES).	نعم
S2548	مهارة تيسير جلسات المناقشات الجماعية.	لا
S2549	مهارة تطوير تقييمات الأمن السيبراني.	لا
S2550	مهارة العمل بفاعلية، في بيئة حركية، وسريعة التطوّر.	لا
S2551	مهارة تحديد الشركاء الخارجيين.	لا
S2552	مهارة الحد من التحيز المعرفي.	لا
S2553	مهارة تطبيق معايير إدارة مخاطر سلسلة الإمداد.	نعم

S2554	مهارة إجراء تحليل البيانات الضخمة.	نعم
S2555	مهارة تحديد القدرة على تحمل المخاطر السيبرانية وإدارتها، وإدارة المخاطر بشكل فعال.	نعم
S2556	مهارة ضبط إعدادات النُظم؛ لتحسين الأداء.	نعم
S2557	مهارة تحديد الأدلة على عمليات التسلل السابقة.	نعم
S2558	مهارة تفسير لغات البرمجة التفسيرية.	نعم
S3000	مهارة إنشاء سياسات حماية البيانات.	نعم
S3001	مهارة التفاوض على اتفاقيات المورّدين.	لا
S3002	مهارة تقييم ممارسات حماية البيانات لدى الموردين.	لا
S3003	مهارة تقييم قوانين الأمن السيبراني.	لا
S3004	مهارة تقييم اللوائح التنظيمية للأمن السيبراني.	لا
S3005	مهارة تحديد مدى الحاجة إلى اتخاذ إجراءات قانونية، بعد حوادث الأمن السيبراني.	نعم
S3500	مهارة استخدام منهجيات معالجة الحوادث.	نعم
S3501	مهارة جمع البيانات من مجموعة متنوعة من مصادر الأمن السيبراني.	نعم
S3502	مهارة إجراء تحليل التوجهات.	نعم
S4000	مهارة البحث عن المعلومات.	لا
S4001	مهارة تقييم تطبيق معايير التشفير.	نعم
S4002	مهارة تحليل قوة التشفير، وكسر الشفرات.	نعم
S4003	مهارة استخدام خوارزميات التشفير.	نعم
S4004	مهارة تحديد مدى توافر الأصول، والقدرات، والقيود،	نعم
S4005	مهارة إدارة حقوق الوصول إلى الحسابات.	نعم

S4006	مهارة جمع بيانات الشبكات.	نعم
S4007	مهارة نشر أنظمة إدارة بيانات اعتماد المستخدم.	نعم
S4008	مهارة تنفيذ أنظمة إدارة بيانات اعتماد المستخدم.	نعم
S4009	مهارة تنفيذ التشفير المتماثل.	نعم
S4501	مهارة تطوير سيناريوهات الاختبار، المبنية على العمليات.	نعم
S4502	مهارة تنفيذ نماذج محاكاة التهديدات.	نعم
S4503	مهارة اختبار أمن النُظم المتكاملة.	نعم
S4504	مهارة استخدام أدوات اختبار الاختراق، وتقنياته.	نعم
S4505	مهارة استخدام أساليب الهندسة الاجتماعية.	لا
S4506	مهارة تنفيذ خطط استمرارية الأعمال، للبنية التحتية للشبكة، وخطط التعافي من الكوارث.	نعم
S4507	مهارة تقييم بيئة التهديدات على المنظمة.	نعم
S4509	مهارة كتابة شفرات برمجية، مخصصة، لتجاوز الضوابط الأمنية.	نعم
S4510	مهارة تنفيذ الأساليب، والتقنيات، والإجراءات المضادة.	نعم
S4512	مهارة اختبار خطط استمرارية الأعمال، للبنية التحتية لشبكة الاختبار، وخطط التعافي من الكوارث.	نعم
S5000	مهارة تحليل عملية تفريغ الذاكرة.	نعم
S5001	مهارة تحديد البيانات المهمة واستخلاصها، للتحليل الجنائي من وسائط متنوعة.	نعم
S5002	مهارة إدارة مكونات نظم التشغيل وتعديلها.	نعم
S5003	مهارة جمع الأدلة الرقمية.	نعم
S5004	مهارة إنشاء محطة عمل، للتحليل الجنائي.	نعم
S5005	مهارة استخدام أدوات التحليل الجنائي الرقمية.	نعم

S5006	مهارة تفكيك أجهزة الحاسب الشخصي.	نعم
S5008	مهارة تحليل كود المصدر.	نعم
S5009	مهارة تحليل البيانات المتطايرة.	نعم
S5010	مهارة تحديد تقنيات التعتيم.	لا
S5011	مهارة تفسير نتائج برامج كشف الأخطاء البرمجية.	نعم
S5012	مهارة تحليل البرمجيات الضارة.	نعم
S5013	مهارة إجراء التحليل على مستوى ("البت") في (الأرقام الثنائية).	نعم
S5014	مهارة معالجة الأدلة الرقمية.	نعم
S5015	مهارة كتابة النصوص البرمجية، الخاصة بنواة لينكس.	نعم
S5018	مهارة تحديد النشاط غير الطبيعي.	نعم
S5019	مهارة إجراء التحليل الجنائي، لأنظمة إدارة الملفات.	نعم
S5020	مهارة استخراج المعلومات، من عمليات التقاط الحزم.	نعم
S5021	مهارة إجراء التحليل الديناميكي.	نعم
S5022	مهارة فك تشفير المعلومات.	نعم
S5023	مهارة التصفح في شبكة الإنترنت المظلم (dark web).	نعم
S5024	مهارة فحص الوسائط الرقمية.	نعم
S5025	مهارة تصفح ملفات النظام.	نعم
S5026	مهارة تحديد حالات العبث، بامتداد اسم الملف.	نعم
S5027	مهارة التعرف على بيانات التحليل الجنائي الرقمي.	نعم
S5028	مهارة تتبع البرمجة ذات المستوى المنخفضة.	نعم

S5029	مهارة استخدام أدوات التحليل الجنائي، القابلة للنشر.	نعم
S5030	مهارة استخراج بيانات التحليل الجنائي، في الوسائط المتنوعة.	نعم
S5031	مهارة إجراء تحليل الأدلة الرقمية.	نعم
S5032	مهارة نقل الأدلة الرقمية.	نعم
S5033	مهارة تخزين الأدلة الرقمية.	نعم
S5034	مهارة إنشاء نسخ الأدلة الرقمية.	نعم
S5500	مهارة إجراء بحوث، غير محددة المرجعية.	لا
S5501	مهارة تحديد جوانب البيئة التشغيلية.	نعم
S5502	مهارة التطوير، أو التوصية بمناهج تحليلية، في المواقف التي تكون فيها المعلومات غير كاملة، أو التي لا توجد لها سابقة.	لا
S5503	مهارة تقييم مصادر المعلومات، المحتملة لقيمتها، في التحقيق السيبراني.	نعم
S5504	مهارة تقييم جودة المعلومات.	لا
S5511	مهارة التعرف على تقنيات حجب الخدمة، عن نظم التشغيل والتطبيقات (DOS).	نعم
S5515	مهارة تحليل منتجات المعلومات الاستباقية عن التهديدات.	نعم
S5516	مهارة إجراء استعلامات البيانات.	نعم
S5517	مهارة استخدام أدوات تحليل البيانات.	نعم
S5518	مهارة إجراء عمليات البحث ذات المصدر المفتوح.	نعم
S5519	مهارة استخدام أدوات تحليل الشبكات وإعادة بنائها.	نعم
S5520	مهارة استخدام أدوات مساحة العمل التعاوني، الافتراضية.	نعم
S5523	مهارة مراقبة التهديدات، أو حالة الثغرات الأمنية، والعوامل البيئية.	نعم
S5524	مهارة تقييم آثار الهجمات السيبرانية، على الأطراف الخارجية.	نعم

S5525	مهارة تحليل بيانات التسلل.	نعم
S5526	مهارة تقييم المنتجات الأمنية.	نعم
S5527	مهارة استخراج البيانات الوصفية.	نعم
S5528	مهارة تنفيذ أساليب محاكاة التهديدات.	نعم
S5529	مهارة إجراء التحليل العقدي.	نعم
S5530	مهارة تحويل متطلبات المعلومات الاستباقية، إلى مهمات إنتاج المعلومات الاستباقية.	نعم
S5531	مهارة محاكاة أفكار الجهات الممثلة للتهديد.	لا
S5532	مهارة تحديد التهديدات، المتقدمة، المستمرة.	نعم
S5533	مهارة صيد التهديدات.	نعم
S5534	مهارة التعرف على الشبكات، وتقنيات خداع نظم التشغيل، والتطبيقات.	نعم
S6000	مهارة تصميم النماذج، في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.	نعم
S6001	مهارة صياغة خطط الاختبار في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.	نعم
S6002	مهارة تصميم حلول أمنية، متعددة المستويات، وقابلة للتطبيق، في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.	نعم
S6003	مهارة تنفيذ منهجيات التصميم، في بيئات تقنية المعلومات، ونظم التحكم الصناعية، والتقنيات التشغيلية.	نعم
S6004	مهارة ترجمة المتطلبات التشغيلية، إلى ضوابط أمنية في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.	نعم
S6005	مهارة تنفيذ عملية الفصل بين الشبكات، في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.	نعم
S6006	مهارة تقييم ضوابط الأمن السيبراني الخاصة؛ ببيئات نظم التحكم الصناعية، والتقنيات التشغيلية.	نعم
S6007	مهارة حماية بيئات نظم التحكم الصناعية، والتقنيات التشغيلية، ضد التهديدات السيبرانية.	نعم
S6008	مهارة ضبط إعدادات النُظم الخاصة، ببيئات نظم التحكم الصناعية، والتقنيات التشغيلية، بهدف تحسين الأداء.	نعم
S6009	مهارة استخدام أدوات الكشف، عن التسلل، في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.	نعم

S6010	مهارة تنفيذ عمليات، الاستجابة للحوادث، في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.	نعم
S6011	مهارة قراءة المخططات التقنية، المتعلقة بالنُظم والشبكات في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية، ومن ثم تفسيرها.	نعم
S6012	مهارة بناء حالات الاستخدام، في بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.	نعم
S6013	مهارة تصميم حلول متعددة للنطاقات القابلة للتطبيق، على بيئات نظم التحكم الصناعية، والتقنيات التشغيلية.	نعم

جدول ١١: أوصاف المهارات

٣,٣ الملحق ج: قائمة مجالات الكفاءات

يبين الجدول الآتي مجالات الكفاءة، التي يجري تقديمها في هذا الإصدار، من الإطار السعودي لكوادر الأمن السيبراني؛ لتناول المجالات المهمة في مجال الأمن السيبراني. كما يقدم كل مجال من مجالات الكفاءة؛ وصفاً للقدرات المحددة، المطلوبة لأداء وظائف الأمن السيبراني المتخصصة.

رمز مجال الكفاءة	اسم مجال الكفاءة	الوصف
CA001	إدارة الهوية والتحكم بالوصول	يصف قدرات المتدربين على إدارة الهويات الرقمية، والأدوار، وضوابط التحكم بالوصول؛ لضمان الوصول الآمن، والمُلتزم إلى الموارد المحمية. ويشمل ذلك جوانب المصادقة، والترخيص، وإدارة دورة حياة الهوية، وتطبيق مبادئ التحكم بالوصول لحماية سلامة البيانات، وإنفاذ ضوابط الوصول المصرح به.
CA002	أمن الحوسبة السحابية	يصف قدرات المتدربين على حماية البيانات، والتطبيقات، والبنية التحتية السحابية؛ من التهديدات الداخلية، والخارجية.
CA003	أمن الاتصالات	يصف قدرات المتدربين على تأمين عمليات التشغيل، والتحكم، والتواصل؛ عبر مختلف البنى التحتية للشبكات، مع معالجة التحديات الأمنية الفريدة، الخاصة بالاتصالات اللاسلكية، والتناظرية والرقمية. ويشمل ذلك المعرفة الأساسية بالشبكات، وبروتوكولات الاتصال الآمنة، وتقنيات حماية الإرسال والبث بشكل فعال.
CA004	التشفير	يصف قدرات المتدربين على تحويل البيانات، باستخدام عمليات التشفير؛ لضمان عدم إمكانية قراءتها، إلا من قبل الشخص، المخول بالوصول إليها.
CA005	أمن أنظمة التشغيل	يصف قدرات المتدربين على تركيب نظم التشغيل، وإدارتها، واستكشاف الأخطاء، وإصلاحها، والنسخ الاحتياطي لها، وإجراء عمليات الاسترداد لها؛ ما يكون في بيئات المحاكاة التشبيهية.
CA006	أمن سلسلة الإمداد	يصف قدرات المتدربين على تحليل المخاطر الرقمية، والمادية، الناتجة عن المنتجات التقنية أو الخدمات التي يجري شراؤها من أطراف خارج المنظمة، وكذلك التحكم فيها.
CA007	أمن البيانات وإدارتها	يصف قدرات المتدربين على تأمين البيانات، طوال دورة حياتها؛ مع العناية بسلامة البيانات، وإدارة قواعد البيانات الآمنة، والتحكم بالوصول، وإدارة دورة حياة أمن البيانات. ويشمل ذلك التدابير التقنية؛ لحماية البيانات من الوصول، غير المصرح به، أو عند تَعرُّضها للتعديل أو الضياع؛ فضلاً عن ضمان استيفاء معايير أمن البيانات، عبر مراحل تخزينها، والوصول إليها، والتخلص منها.
CA008	تحليل المخاطر الأمنية	يصف قدرات المتدربين المتعلقة بدراسة المخاطر المحتملة على نظم المعلومات وأصول المنظمة، وتحديدها وتقييمها. ويشمل ذلك تحليل التهديدات، والثغرات الأمنية، والأثر المحتمل للمخاطر؛ فضلاً عن التوصية بإستراتيجيات الحد من المخاطر.
CA009	التحليل الجنائي الرقمي	يصف قدرات المتدربين، المتعلقة باسترجاع المواد الموجودة في الأجهزة الرقمية؛ والتحقيق فيه. ويشمل ذلك تقنيات تحليل الأدلة الرقمية؛ لدعم التحقيقات، أو الاستجابة للحوادث، أو الإجراءات القانونية.

CA010	اختبار الاختراق	يصف قدرات المتدربين، المتعلقة باختبار أمن نظم المعلومات وتقييمه؛ من خلال المحاكاة الواقعية للهجمات. ويشمل ذلك تقنيات اكتشاف الثغرات الأمنية، والاستغلال، والإبلاغ عن النتائج؛ بهدف تحسين الحالة الأمنية.
CA011	إدارة الحوادث	يصف قدرات المتدربين، على تحديد حوادث الأمن السيبراني، والاستجابة لها وإدارتها. ويشمل ذلك المعرفة بأساليب الكشف عن الحوادث، والاستجابة لها، وأدوات تحليل الحوادث، وإستراتيجيات احتواء التهديدات السيبرانية، والحد والتعافي منها.
CA012	إدارة برامج الأمن السيبراني	يصف قدرات المتدربين، المتعلقة بإدارة برامج الأمن السيبراني وتنفيذها داخل المنظمة؛ بما في ذلك تخصيص الموارد، وإدارة المخاطر، وتقييم أداء تلك البرامج.
CA013	إدارة الثغرات الأمنية	يصف قدرات المتدربين، المتعلقة بتحديد الثغرات الأمنية في النُظم والشبكات، وتقييمها والحد منها. ويشمل ذلك استخدام الأدوات والتقنيات؛ لتقييم الحالة الأمنية، والتوصية بالتدابير المضادة.
CA014	تطوير البرمجيات الآمنة	يصف قدرات المتدربين، على تطوير البرمجيات، وتأمينها؛ من خلال دمج الممارسات الأمنية، طوال دورة حياة تطوير البرمجيات. ويشمل ذلك مبادئ التصميم الآمن، وممارسات التشفير الآمنة، والضوابط الأمنية على مستوى التطبيقات، ومراجعات التعليمات البرمجية، وتقييمات الثغرات الأمنية في التطبيقات، ودمج الضوابط الأمنية في خطوط تطوير البرمجيات الحديثة (مثل، الأمان عبر جميع مراحل تطوير البرامج DevSecOps).
CA015	أمن الذكاء الاصطناعي	يصف مجال الكفاءة هذا، قدرات المتدربين على تأمين نظم الذكاء الاصطناعي؛ بما في ذلك فهم المخاطر الخاصة بنماذج التعلم الآلي، والحد منها، وسلامة البيانات في تطبيقات الذكاء الاصطناعي، والتطوير الآمن لأدوات الأمن السيبراني، القائمة على الذكاء الاصطناعي. ويشمل تلك الإستراتيجية، تأمين خطوط تطوير الذكاء الاصطناعي، وضمان موثوقية نظم الذكاء الاصطناعي، المستخدمة في عمليات الأمن السيبراني.
CA016	أمن الأجهزة والبرمجيات الثابتة	يصف هذا قدرات المتدربين على تأمين مكونات الأجهزة، والبرمجيات الثابتة؛ ضد الوصول غير المصرح به، وحمايتها من حالات التلاعب. ويشمل ذلك تنفيذ تدابير أمنية، على مستوى الأجهزة، وتدابير الهندسة العكسية، والحماية من الهجمات المادية.
CA017	تصميم معمارية الأمن السيبراني	يصف قدرات المتدربين على تصميم نظم المعلومات الآمنة وشبكاتها وهندستها. ويشمل ذلك تطبيق مبادئ التصميم الآمن، وتعزيز صمود المعمارية، وتنفيذ الضوابط الأمنية، التي تتوافق مع أهداف المنظمة وغاياتها، ومع المتطلبات التنظيمية.
CA018	الأمن السيبراني الصناعي وأمن إنترنت الأشياء	يصف قدرات المتدربين على تأمين النُظم المدمجة، وأجهزة إنترنت الأشياء، ونظم التحكم الصناعية (ICS). بما يشمل ذلك تأمين أساليب الاتصال، ومراقبة بيئات نظم التحكم الصناعية، وضمان حماية قوية لإنترنت الأشياء، وشبكات الاستشعار اللاسلكية.
CA019	المعلومات الاستباقية للتهديدات السيبرانية	يصف قدرات المتدربين، على تحديد التهديدات السيبرانية، وتحليلها، والدفاع المضاد لها؛ باستخدام أدوات جمع المعلومات الاستباقية، حول التهديدات السيبرانية، والإستراتيجيات الدفاعية. ويشمل ذلك الدفاع عن الشبكات، وفهم بيئة التهديدات السيبرانية، واستخدام الأدوات التحليلية، لمراقبة المخاطر الأمنية، وتقييمها، والحد منها بشكل فوري.
CA020	التدريب والتوعية بشأن الأمن السيبراني	يصف قدرات المتدربين على تصميم برامج فعالة وتطويرها وتقديمها، للتدريب، والتوعية في مجال الأمن السيبراني. ويشمل ذلك إنشاء محتوى جاذب، يسهل الوصول إليه، واختيار الأساليب التعليمية المناسبة، وصياغة مواد تعليمية مؤثرة لتعزيز الوعي، وتقييم فعالية جهود التدريب؛ لضمان تقدم المتدربين وفهمهم.

CA021	تنظيمات الأمن السيبراني والالتزام	يصف قدرات المتدربين على تفسير ضمان الالتزام بقوانين وتنظيمات الأمن السيبراني والمعايير الأخلاقية داخل المنظمة والعمل على تطبيقها. ويشمل ذلك فهم الأطر القانونية ذات الصلة، وإدارة الالتزام التنظيمي، وتقديم المشورة، بشأن القضايا القانونية في مجال الأمن السيبراني؛ وضمان الالتزام بسياسات الأمن السيبراني ومعاييره.
CA022	حماية البيانات	يصف مجال الكفاءة هذا قدرات المتدربين على إدارة مخاطر حماية البيانات، وضمان الالتزام بقوانين حماية البيانات، وتأمين بيانات المنظمة. ويشمل ذلك البيانات الشخصية المعرفة (PII)، وتنفيذ ضوابط حماية البيانات، وإدارة تصنيف البيانات، والتحكم في الوصول إليها؛ وتعزيز الوعي المؤسسي بمسؤوليات حماية البيانات.
CA023	استمرارية الأعمال والتعافي من الكوارث	يصف قدرات المتدربين على تخطيط إستراتيجيات استمرارية الأعمال، والتعافي من الكوارث (BCM/DR) التي تعني بالأمن السيبراني، ومن ثم تنفيذها وإدارتها. ويشمل ذلك تعزيز صمود النُظم، وإنشاء بروتوكولات تعافٍ خاصة بالأمن السيبراني، وضمان استمرارية وظائف الأمن السيبراني الأساسية؛ أثناء الأعطال، أو الحوادث السيبرانية، وبعدها.
CA024	اختبار الأمن السيبراني	يصف قدرات المتدربين، على التقييم المنهجي للحالة الأمنية للنظم، والشبكات، والتطبيقات؛ من خلال منهجيات الاختبار المنظمة. ويعني كذلك على اختبار تكامل النُظم وأمنها، بما في ذلك إجراء الاختبارات الوظيفية، والاختبارات القائمة على الالتزام، واختبارات حقن معلومات عشوائية، أو غير متوقعة؛ للكشف عن الثغرات الأمنية، والاختيارات الاستكشافية.

جدول ١٢: أوصاف مجالات الكفاءة

٤,٣ الملحق د: التحديثات التي أجريت على هذا الإصدار من الإطار السعودي لكوادر الأمن السيبراني

يقدم هذا الإصدار (١,٥) من الإطار السعودي لكوادر الأمن السيبراني، العديد من التحديثات المهمة، التي تهدف إلى تعزيز المواءمة مع المعايير الدولية، وتسهيل الاستخدام لأصحاب المصلحة. وتشمل التغييرات الرئيسة ما يلي:

١- **إصدار وثيقة التقدم الوظيفي التكميلية:** يقدم هذا التحديث ("الإطار السعودي لكوادر الأمن السيبراني - التقدم الوظيفي")، وهو وثيقة تكميلية توضح المسارات المنظمة للتطور المهني، في مجال الأمن السيبراني، **إذ** تم تقديم مساراتٍ واضحة للتطور المهني، والمؤهلات المطلوبة، ومستويات الخبرات المُوصى بها لكل دور وظيفي، مما يساعد الأفراد والمؤسسات، على التخطيط لوظائف الأمن السيبراني، واستكشافها بشكلٍ أكثر فاعلية.

٢- **حذف القدرات:** جرى حذف عبارة القدرات واستبدالها بعبارة ("مهارات")، ويتسق ذلك التغيير مع أفضل الممارسات العالمية.

٣- **إدخال مجالات الكفاءة:** جرى إدخال مجالات الكفاءة في هذا الإصدار ("الملحق ج") لتغطية الاحتياجات الضرورية للأمن السيبراني، وتوفير إطار مرجعي لأصحاب المصلحة.

٤- **مراجعة نصوص بيانات المهمات والمعارف والمهارات:** جرت مراجعة جميع نصوص بيانات المهمات والمعارف والمهارات وإعادة صياغتها؛ وعند الضرورة، حذفها أو تقسيمها إلى مكونات أكثر تحديدًا وتمييزًا للمواءمة مع أفضل الممارسات العالمية.

٥- **تنقيح المهمات والمعارف والمهارات وربطها بالأدوار الوظيفية:** جرى تحديث كل دور وظيفي من خلال مراجعة المهمات، والمعارف، والمهارات المرتبطة به، بما في ذلك عمليات الإضافة والحذف؛ لتعكس بشكل أفضل متطلبات الدور تتسق مع متطلبات الأمن السيبراني المتطورة.

٦- **تصنيف نصوص بيانات المهارات:** جرى تصنيف نصوص بيانات المهارات، على كونها فنية أو غير فنية، مما يتيح فهم طبيعة كل مهارة بشكلٍ أوضح، ويساعد في تطوير برامج التدريب، والتقييم الخاصة بكل دور.

٧- **تحديث أوصاف الأدوار الوظيفية:** تم إجراء تحديثات بسيطة على أسماء وأوصاف الأدوار الوظيفية: أخصائي حماية البيانات، ومدرب الأمن السيبراني، ومُطوّر المناهج التعليمية للأمن السيبراني.

تُعزز هذه التحديثات بمجملها من صلة الإطار السعودي لكوادر الأمن السيبراني، وسهولة استخدامه؛ مع ضمان بقائه شاملاً وفعالاً لبناء وإدارة الكوادر الوطنية للأمن السيبراني.


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority