الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الإطار السعودي لكوادر الأمن السيبراني (سيوف)

التقدم الوظيفي

THE SAUDI CYBERSECURITY WORKFORCE FRAMEWORK

CAREER PROGRESSION

(SCyWF-CP – 1: 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 التوضيحية

قائمة الجداول

١. المقدّمة

تعمل الهيئة الوطنية للأمن السيبراني على حماية الفضاء السيبراني للمملكة؛ ويتطلب ذلك كوادر وطنية مؤهلة في مجال الأمن السيبراني تكون قادرةً على تنفيذ جميع أعمال الأمن السيبراني. وبموجب الأمر الملكي الكريم ذي الرقم ٦٨٠١، والتاريخ ١٤٣٩/٢/١١هـ تتضمن اختصاصات الهيئة الوطنية للأمن السيبراني الآتي: 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. وتُعدّ هذه الوثيقة «الإطار السعودي لكوادر الأمن السيبراني–التقدم الوظيفي» (SCyWF-CP)، ملحقًا للوثيقة المحدثة من الإطار السعودي لكوادر الأمن السيبراني (SCyWF 1.5) وقد طوّرتها الهيئة الوطنية للأمن السيبراني لتوسيع نطاق الإطار وليكون مرجعًا في هذا الجانب. وتحدد هذه الوثيقة مسارات التقدم الوظيفي ضمن الأدوار الوظيفية للأمن السيبراني بصورة منظمة، تدعم اختصاصات الهيئة الوطنية للأمن السيبراني، وجهودها الرامية إلى تأهيل كوادر وطنية ماهرة، ومتمكنّة في مجال الأمن السيبراني.

١,١ الغرض

تحدد هذه الوثيقة مسارات الترقية والتقدم، ضمن الأدوار الوظيفية للأمن السيبراني، المبينة في الإطار السعودي لكوادر الأمن السيبراني (سيوف). وتعتمد الوثيقة في تفصيل المؤهلات والخبرات، والمسارات المهنية، المطلوبة على الإطار السعودي لكوادر الأمن السيبراني، وتدعم الجهود الوطنية الرامية إلى تطوير كوادر وطنية، ذات كفاءة في مجال الأمن السيبراني، وتوضح الوثيقة في كل مستوى، مستويات الإتقان المطلوبة، من المهارات والمؤهلات التعليمية والخبرات. كما تتيح هذه الوثيقة للكوادر العاملة، من خلال ربط أدوارهم الوظيفية بمسارات وظيفية واضحة، إمكانية تطوير مهاراتهم، وتنميتها بشكل فعال مع معالجة تحديات الأمن السيبراني المتغيّرة في الوقت نفسه، كما أنّها تعد مؤشرًا للأدوار الوظيفية التي يمكن للموظف، السعي نحوها في مسيرته المهنية.

٢,١ الأهداف

إنّ الهدف الرئيسي من هذه الوثيقة، هو وضع الحد الأدنى من المتطلبات، وطرح مسارات واضحة للتقدم الوظيفي، في سلّم الأدوار الوظيفية للأمن السيبراني، وتهدف الوثيقة على وجه التحديد إلى ما يلي:

- وضع إطار عمل تفاعلي لتحديد الكفاءات السيبرانية وتوظيفها ورعايتها، من خلال تفصيل مستويات الأدوار الوظيفية، وشروط الالتحاق، ومسارات التقدم الوظيفي، والتوقعات على مستوى الإتقان؛ من أجل مواءمة تطوير المختصين، مع توقعاتهم الوظيفية، على مختلف المستويات المهنية.
- تطوير وتحسين البرامج التعليمية للأمن السيبراني؛ من خلال وضع مصطلحات موحدة للمؤسسات الأكاديمية.
- وضع معيار موحد، لتحديد الأدوار الوظيفية للأمن السيبراني ومواءمتها، ويضمن توضيح المهمات والمهارات والتدريبات المطلوبة.
- دعم المواءمة مع الأهداف الوطنية على صعيد المختصين؛ من خلال تنظيم مسارات تنمية الكفاءات والمواهب، ومساعدة المهنيين على فهم آلية التقدم في مناصبهم الوظيفية، أو كيفية الانتقال إلى أدوار وظيفية جديدة في مهن الأمن السيبراني.

٣,١ نطاق قابلية التطبيق

تعد هذه الوثيقة، وثيقةً داعمةً للإطار السعودي لكوادر الأمن السيبراني (سيوف) إذ تقدم مسارات عملية للتقدم الوظيفي، ضمن الأدوار الوظيفية للأمن السيبراني، وهي بمثابة دليل إرشادي لتوجيه الأفراد والمؤسسات في كيفية تنمية المواهب والكفاءات، بما يتوافق مع الأهداف الوطنية للأمن السيبراني، كما يمكن أن تقوم كل جهة بعمل بعض التعديلات والإضافات لتكييف هذا الإطار بحسب احتياجاتها الوظيفية وبدون الإخلال بالبنية الأساسية لهذا الإطار. وتنطبق وثيقة التقدم الوظيفي على:

١. **المتخصصون في مجال الأمن السيبراني في المستقبل،** الطامحون إلى اكتشاف المؤهلات والمتطلبات التي تفتح لهم أبواب هذا المجال، وتساعدهم على التقدم فيه.
٢. **المتخصصون الحاليون في مجال الأمن السيبراني،** الطامحون إلى تطوير مهاراتهم، واكتساب الكفاءة والتقدم الوظيفي، من خلال مسارات وظيفية محددة.
٣. **أصحاب العمل والمعلّمين في مجال الأمن السيبراني،** الذين يتحملون مسؤولية بناء أشخاص مختصين مهرة، من خلال مواءمة إستراتيجيات تنمية المواهب والكفاءات، مع أهداف الأمن السيبراني على الصعيدين المؤسسي والوطني.

٤,١ العلاقة بمنشورات الهيئة الوطنية للأمن السيبراني

الإطار السعودي لكوادر الأمن السيبراني (سيوف) ووثائقه ذات الصلة، مثل وثيقة ملحق التقدم الوظيفي، جرى تطويرها بما يتسق مع المعايير والأطر والممارسات الدولية، وجميع القوانين واللوائح والمتطلبات الوطنية ذات الصلة، مثل: ضوابط الأمن السيبراني الأساسية وضوابط الأمن السيبراني للبيانات[١].

تحدد هذه الوثيقة سنوات الخبرة المطلوبة لكل مستوى، بناءً على متطلبات المستخدمين والحد الأدنى من الخبرة اللازمة؛ للحصول على الشهادات الاحترافية الأكثر شيوعًا والمعترف بها دولياً، كما يتسق نهج ملحق التقدم الوظيفي مع دليل تصنيف الوظائف[٢] الصادر عن وزارة الموارد البشرية والتنمية الاجتماعية؛ لضمان الاتساق في طريقة تحديد مستويات الوظائف. وبالمثل، فإن النهج المتبع في تحديد المؤهلات التعليمية المطلوبة يتسق مع الإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم)[٣].

[١] انظر الضوابط الأساسية للأمن السيبراني (https://nca.gov.sa/pages/legislation.html، ٢٠٢٤، (ECC - ٢: ٢٠٢٤)، وضوابط الأمن السيبراني للبيانات (DCC-١:٢٠٢٢)، https://nca.gov.sa/pages/legislation.html.

[٢] انظر دليل تصنيف الوظائف، وزارة الموارد البشرية والتنمية الاجتماعية، https://eservices.masar.sa/UCG/

[٣] انظر الإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم - ١: ٢٠٢٠)، ٢٠٢٠ https://nca.gov.sa/ar/scyberedu_en.pdf

٥,١ الحد الأدنى من المؤهلات العلمية

تقبل بعض الأدوار الوظيفية توظيف المرشحين المبتدئين، الحاصلين على دبلوم متوسط، أو درجة البكالوريوس، في حين تتطلب أدوار وظيفية أخرى مؤهلات متقدمة، حتى درجة الدكتوراه. يوضح الجدول الآتي الحد الأدنى من المؤهلات العلمية، بما يتسق مع الإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم).

التصنيف	الحد الأدنى من المؤهلات العلمية
المستوى الأول من المؤهلات العلمية	دبلوم متوسط فى الأمن السيبرانى، أو فى تخصص ذى صلة يغطى وحدات المعرفة المطلوبة، وفقًا للإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم).
المستوى الثانى من المؤهلات العلمية	درجة البكالوريوس في الأمن السيبراني، أو في مجالات ذات صلة وثيقة، مثل: علوم الحاسب الآلي، أو نظم المعلومات، أو تقنية المعلومات، أو هندسة الحاسب الآلي، أو هندسة البرمجيات، أو درجة البكالوريوس في تخصص ذي صلة يغطي وحدات المعرفة المطلوبة، وفقًا للإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم).
المستوى الثالث من المؤهلات العلمية	مؤهل سابق بالمستوى الثاني، وشهادة الدبلوم العالي في الأمن السيبراني، أو في تخصص ذي صلة يغطي وحدات المعرفة المطلوبة، وفقًا للإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم).
المستوى الرابع من المؤهلات العلمية	مؤهل سابق بالمستوى الثاني، ودرجة الماجستير في الأمن السيبراني، أو في تخصص ذي صلة يغطي وحدات المعرفة المطلوبة، وفقًا للإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم).
المستوى الخامس من المؤهلات العلمية	مؤهل سابق بالمستوى الثالث، أو الرابع، ودرجة الدكتوراه في الأمن السيبراني التي تغطي وحدات المعرفة المطلوبة في العمق أو الخبرة ذات الصلة في هذا المجال.

جدول ١: تحديد المؤهلات العلمية وتصنيفها

٦,١ مستويات الأدوار الوظيفية

سيكون لكل دور وظيفي مستوى واحد أو أكثر. وترد هذه المستويات في الجدول ٢ الآتي بشكل موسّع.

مستوى الدور الوظيفي	الوصف
المستوى الأول	عادةً ما يجري وصف الدور الوظيفي في المستوى المبتدئ بأنه الفرد الحاصل على شهادة بكالوريوس أو دبلوم ذي صلة (انظر الجدول ١)، ويعمل بوصفه متدربًا أو عضوًا في فريق الدعم، أو فريق المبتدئين تحت إشراف مباشر من قبل أحد الممارسين، لتطوير المهارات اللازمة؛ ليصبح ممارسًا.
المستوى الثاني	تنفيذ المهمات الأساسية للدور الوظيفي بفاعلية، مع تقديم الحد الأدنى من الإشراف، والقدرة على توجيه، أو إدارة عضو مبتدئ في الفريق.
المستوى الثالث	تنفيذ المهمات الأساسية على نطاق أوسع، أو في بيئات أكثر تعقيدًا، بالإضافة إلى تنفيذ المهمات التي تتطلب المزيد من الخبرة، الأكثر تخصصًا من تلك التي يقوم بها موظفو المستوى الثاني. والقدرة على الإشراف وإدارة وتوجيه الممارسين، أو فرق الممارسين الذين يقومون بالمهمات الأساسية للدور الوظيفي، ويمكن أن ينوب عن الخبراء والعمل بوصفه خبيرًا متخصصًا في الفريق في بعض مجالات المعرفة والمهارات.
المستوى الرابع	تنفيذ مهمات عالية التخصص، أو واسعة النطاق، أو معقدة؛ تتطلب مستويات أعلى بكثير من المهارات والخبرات ذات الصلة بالدور الوظيفي، مقارنةً بالمستويات الأقل. في هذا المستوى، يستطيع الموظفون ذوو الكفاءات الإدارية القوية قيادة فريق مكوّن من كبار الممارسين و/أو الممارسين، في حين يعمل الآخرون بوصفهم خبراء متخصصين في المنظمة في مجموعة متنوعة من مجالات المهارات، والمعرفة ذات الصلة بالدور الوظيفي. من المرجح أن يتولى الموظفون في هذا المستوى تمثيل المنظمة والحضور بالنيابة عنها في المناسبات الخارجية.
المستوى الخامس	يشغل، على سبيل المثال، منصب رئيس إدارة الأمن السيبراني، أو مدير أول للأمن السيبراني، أو مستشار الأمن السيبراني، أو زميل في أكبر المؤسسات وأكثرها تعقيدًا. في هذا المستوى، يتولى الأفراد قيادة فرق كبيرة جدًا لتقديم خبرة عميقة اكتسبوها على مدى سنوات عديدة من العمل بوصفهم متخصصين في الأمن السيبراني، ويستفاد منها في تطوير إستراتيجيات الأمن السيبراني وبرامجه المؤسسية أو الوطنية. من المرجح أن يتولى الموظفون في هذا المستوى تمثيل المنظمة، والحضور بالنيابة عنها في المناسبات الخارجية.

جدول ٢: وصف مستويات الأدوار الوظيفية

هناك بعض المصطلحات الإضافية المستخدمة في الوثيقة؛ ولكنها غير مذكورة في الجدول (٢) الآنف الذكر، بينما يبين الجدول (٣) الآتي بعض هذه المصطلحات.

المصطلح	الوصف
الخريج الحاصل على المستوى الأول من المؤهلات العلمية	يمكن للخريجين الحاصلين على **المستوى الأول من المؤهلات العلمية** (انظر الجدول ١) أن يلتحقوا عادةً بالأدوار الوظيفية للأمن السيبراني في **المستوى الأول**. لديهم معرفة **أساسية** بالأمن السيبراني؛ ولكن بخبرة عملية محدودة، لذلك يبدؤون من المستوى المبتدئ. ومع مرور الوقت، ومع اكتسابهم للخبرة في مجال الأمن السيبراني (انظر الجدول ٥)، يصبحون مؤهلين للتقدم إلى مستويات أعلى.
الخريج الحاصل على المستوى الثاني من المؤهلات العلمية	يمكن للخريجين الحاصلين على **المستوى الثاني من المؤهلات العلمية** (انظر الجدول ١) التقدم لوظائف **المستوى الثاني**؛ بشرط امتلاكهم خبرة مناسبة في الأمن السيبراني، أو مؤهلات أكاديمية أعلى (مثل المستوى الثالث أو الرابع أو الخامس من المؤهلات العلمية). أما المتقدمون لوظائف **المستوى الثالث**؛ فيجب أن يستوفوا الحد الأدنى لمتطلبات المستوى الثاني، مع تقديم دليل على خبرة مهنية أوسع (انظر الجدول ٥)، إذ تمنحهم هذه المجموعة من المؤهلات، والخبرات، القدرة على تولي مهمات أمن سيبراني من المستوى المتوسط.
دور الموارد البشرية أو الدور الإداري	لا يتناول هذا الإطار المهارات المطلوبة لهذه الأدوار الوظيفية، إذ إنها، ما لم يُذكر خلاف ذلك؛ تتركز في المهارات التنظيمية والإدارية، بالإضافة إلى مستويات مختلفة من الكفاءة، في إدارة رأس المال البشري. وستكون هذه المهارات متسقةً عبر جميع المستويات، وفقًا لما هو محدد في الجدول ٢.
الأدوار الفنية للأمن السيبراني	يشمل هذا أي دور وظيفي في فئة معمارية الأمن السيبراني والبحث والتطوير، وفئة الحماية والدفاع وفئة نظم التحكم الصناعية والتقنيات التشغيلية، مع استثناء أخصائي مخاطر الأمن السيبراني في نظم التحكم الصناعية والتقنيات التشغيلية.
الأدوار الرئيسية للأمن السيبراني	ينطبق هذا الوصف على أي دور وظيفي، باستثناء دور مدير الموارد البشرية للأمن السيبراني، ودور أخصائي قانون الأمن السيبراني؛ لأن هذين الدورين لا يتطلبان أي مهارات متخصصة في مجال الأمن السيبراني.

جدول ٣: وصف المصطلحات الإضافية

٧,١ تصنيف الإطار السعودي لكوادر الأمن السيبراني

يوضح الشكل ١ الآتي الفئات، والتخصصات، والأدوار الوظيفية المحددة المتعلقة بالأمن السيبراني في الإطار السعودي لكوادر الأمن السيبراني (سيوف) الصادر عن الهيئة الوطنية للأمن السيبراني. وهي التي ترد الإشارة إليها فيما تبقى من الوثيقة.

شكل ١: الإطار السعودي لكوادر الأمن السيبراني

يتم تحديد الأدوار الوظيفية والمجالات والفئات المتخصصة في الإطار السعودي لكوادر الأمن السيبراني على النحو التالي:

- 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.
- 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.

٨,١ التعليم، الخبرة، والإتقان في المهارات

ويبين الجدول (٤) الآتي المؤهلات العلمية المطلوبة لكل مستوى وظيفي. كما يوضح أن امتلاك مؤهل أكاديمي يفوق الحد الأدنى المحدد، يمكنه أن يعادل بعض سنوات الخبرة المطلوبة لهذا المستوى .ويتضح من الجدول (٤) أن المتطلبات التعليمية للأدوار الوظيفية من المستوى الثاني إلى المستوى الخامس متماثلة.

مستوى الدور الوظيفي	المتطلبات التعليمية
المستوى الأول	الحد الأدنى من المتطلبات التعليمية هو المستوى الأول من المؤهلات العلمية (كما هو موضح في الجدول ١). ومع ذلك، يمكن استخدام المستوى الثاني من المؤهلات العلمية أو المستوى الأعلى ليكون معادلًا لبعض سنوات الخبرة المطلوبة للمستوى.
المستوى الثاني	الحد الأدنى من المتطلبات التعليمية هو المستوى الثاني من المؤهلات العلمية (كما هو موضح في الجدول ١)، ومع ذلك، يمكن استخدام المستوى الثالث من المؤهلات العلمية أو المستوى الأعلى، ليكون معادلًا لبعض سنوات الخبرة المطلوبة للمستوى.
المستوى الثالث	الحد الأدنى من المتطلبات التعليمية، هو المستوى الثاني من المؤهلات العلمية (كما هو موضح في الجدول ١)، ومع ذلك، يمكن استخدام المستوى الثالث من المؤهلات العلمية، أو المستوى الأعلى، ليكون معادلًا لبعض سنوات الخبرة المطلوبة للمستوى.
المستوى الرابع	الحد الأدنى من المتطلبات التعليمية، هو المستوى الثاني من المؤهلات العلمية (كما هو موضح في الجدول ١)، ومع ذلك، يمكن استخدام المستوى الثالث من المؤهلات العلمية، أو المستوى الأعلى، ليكون معادلًا لبعض سنوات الخبرة المطلوبة للمستوى.
المستوى الخامس	الحد الأدنى من المتطلبات التعليمية، هو المستوى الثاني من المؤهلات العلمية (كما هو موضح في الجدول ١)، ومع ذلك، يمكن استخدام المستوى الثالث من المؤهلات العلمية، أو المستوى الأعلى، ليكون معادلًا لبعض سنوات الخبرة المطلوبة للمستوى.

جدول ٤: المتطلبات التعليمية لمستويات الأدوار الوظيفية

مستوى الدور الوظيفي	الحد الأدنى من سنوات الخبرة في مهنة الأمن السيبراني	العدد النموذجي للسنوات التي يقضيها الفرد في هذا المستوى	الحد الأدنى من مستوى الإتقان المطلوبة لكل مهارة
المستوى الأول	٠	١ - ٣	مبتدئ
المستوى الثاني	١	٣ - ٥	مبتدئ
المستوى الثالث	٤	٦ - ١٠	متوسط
المستوى الرابع	١٠	٥ - حتى نهاية المسار الوظيفي	متقدم
المستوى الخامس	١٥+	حتى نهاية المسار الوظيفي	متقدم

جدول 0: وصف الخبرة المطلوبة

يقدم الجدول ٥ إرشادات عن الحد الأدنى من سنوات الخبرة المطلوبة، لكل مستوى من مستويات الأدوار الوظيفية، التي يتوقع أن يكون الفرد قد اكتسبها في أدوار الأمن السيبراني (كما هو محدد في الإطار السعودي لكوادر الأمن السيبراني) قبل أن يكون مؤهلًا للترقية، أو التعيين في دور وظيفي، ضمن هذا المستوى. ويمكن تعيين الخريجين الجدد، أو الموظفين الذين يغيرون وظائفهم، دون امتلاك خبرة في وظيفة الأمن السيبراني في الأدوار الوظيفية من المستوى الأول. من المتوقع أن يتمتع الموظف بخبرة لا تقل عن ١٠ سنوات في الأدوار الوظيفية للأمن السيبراني المحددة في الإطار السعودي لكوادر الأمن السيبراني؛ قبل أن يكون مؤهلًا للحصول على دور وظيفي من المستوى الرابع.

كما يوفر الجدول السابق التوجيه بشأن العدد النموذجي للسنوات، التي يقضيها أخصائي الأمن السيبراني، في كل مستوى. يدخل الفرد المستوى الأول دون خبرة، ويقضي فيه عادةً فترة تتراوح بين سنة، وثلاث سنوات، قبل الانتقال إلى مستوى أعلى. ويمكن ترقية بعض الأفراد إلى المستوى الثاني؛ بعد أن يقضي سنة واحدة، بينما قد يستغرق الآخرون ثلاث سنوات قبل ترقيتهم. عند الانتقال إلى المستوى الثاني؛ يمضي الفرد عادةً فترة تتراوح بين ثلاث وخمس سنوات قبل التقدم إلى المستوى الذي يليه. يقضي معظم المتخصصين في الأمن السيبراني الجزء الأكبر، من مسيرتهم المهنية في المستويين الثاني والثالث، إذ تتوفر غالبية الفرص الوظيفية، وعادةً ما يكونون ذوي قيمة عالية لمؤسساتهم في هذا الوقت، ويمكن أن تصل فترة بقائهم في هذين المستويين إلى ١٥ عامًا (٥ سنوات في المستوى الثاني و١٠ سنوات في المستوى الثالث)، كما يوضح الجدول. بعد ١٠ سنوات على الأقل – أو عادةً بعد ١٥ إلى ١٧ عامًا – تجري ترقية معظم المتخصصين إلى المستوى الرابع، إذ يقضون بقية مسيرتهم المهنية، نظرًا لمهماتهم الإستراتيجية في مؤسساتهم.

يقدم هذا الإطار أيضًا مستويات الإتقان المطلوبة لكل دور وظيفي، كما هو موضح في الجدول ٦ الآتي. في المستويين الأول والثاني، يُتوقع من الأفراد امتلاك مستوى إتقان أساسي للمهارات، وتشمل الإلمام بالمفاهيم الأساسية للأمن السيبراني، والقدرة على تنفيذ المهمات المتكررة تحت إشراف وثيق. في المستوى الثالث، يكون المستوى المتوسط من الإتقان مطلوبًا؛ مما يتيح للأفراد إدارة المهمات العادية، وذات التعقيد المتوسط باستقلالية نسبية، وتحت إشراف محدود. أما في المستويين الرابع والخامس، فمستوى الإتقان المتقدم للمهارات ضروري؛ إذ تتطلب مستوىً عاليًا من الخبرة، والقدرة على القيادة، والتعامل مع التحديات المعقدة، مع تقديم إرشادات إستراتيجية، دون الحاجة إلى إشراف مباشر. ويمكن للجهات تطوير مصفوفات تفصيلية لقياس مستوى الإتقان استنادا الى الجدول ٦.

مستويات الإتقان في المهارات	الوصف
مبتدئ	تُمارَس المهارات بمستوى أساسي لإنجاز المهمات الروتينية تحت إشراف مباشر.
متوسط	تُمارَس المهارات بمستوى متوسط للتعامل مع مهمات متوسطة التعقيد، مع حد أدنى من الإشراف.
متقدم	تُمارَس المهارات بمستوى خبير؛ لإدارة المواقف المعقّدة، وتقديم التوجيه الإستراتيجي، مع القليل من الإشراف، أو بدونه.

جدول ٦: وصف مستويات الإتقان في المهارات

٩,١ الأساس المنطقي للانتقالات المحتملة بين الأدوار الوظيفية

إنَّ الانتقالات الأفقية، المبيّنة في هذه الوثيقة (القسم ١،٢ فصاعدًا) قد جرى تحديدها؛ استنادًا إلى رؤى خبراء الأمن السيبراني، الذين يتمتعون بدراية كافية بحيثيات سوق الأمن السيبراني، وطبيعة التنقّل بين الأدوار الوظيفية، ويضمن هذا المنظور العملي، أن يعكس الإطار مسارات مهنية حقيقية، بدلاً من مسارات نظرية بحتة، وإضافةً إلى ذلك، تحدث معظم هذه التنقلات الأفقية بين أدوار تتشابه فيما بينها في بعض المهمات والمعارف والمهارات المسندة للدور الوظيفي؛ مما يجعل من الأسهل على المتخصصين التكيف والنجاح؛ عند تغيير وظائفهم. فعلى سبيل المثال؛ يمكن لمحلل دفاع الأمن السيبراني الانتقال أفقيًا إلى دور أخصائي تقييم الثغرات؛ لأن كلا الدورين يشتركان بدرجة كبيرة في اكتشاف التهديدات، وتحليل المخاطر، وتقييم الأمن من حيث المهمات والمعرفة والمهارات (TKS).

١٠,١ رموز الأدوار الوظيفية

تستعرض الأقسام التالية خرائط المسار المهني لكل دور وظيفي. ولتسهيل الفهم؛ جرى استخدام ترميز لوني، إذ تشير الألوان الفاتحة إلى الأدوار ذات المستويات الأدنى، في حين تصبح الألوان أغمق تدريجيًا مع التقدم إلى الأدوار الوظيفية العليا وترد رموز الألوان في الشكل ٢ أدناه، وينبغي الإشارة إليها عند الضرورة.

شكل ٢: ترميز ألوان المستويات

يبين الجدول ٧ جميع الأدوار والمستويات ذات الصلة، التي تنطبق على كل دور وظيفي. تشير علامة الاختيار (✓) إلى المستويات الموجودة لكل دور وظيفي. توضح النقاط الآتية مبررات تحديد مستوى بداية كل دور وظيفي:

- **الأدوار التي تبدأ من المستوى الأول** هي **أدوار وظيفية أقل تقدمًا**، لا تتطلب خبرة سابقة في مجال الأمن السيبراني، أو معرفة متعمقة في المجال. وهي تناسب الأفراد الذين يبدؤون حياتهم المهنية في هذا المجال.
- **الأدوار التي تبدأ من المستوى ٢** (دون نظير من المستوى ١) بمثابة **نقطة دخول** إلى الأمن السيبراني؛ مما يتطلب معرفة **تأسيسية** في مجال ذي صلة (على سبيل المثال، علم البيانات لأخصائي علم البيانات للأمن السيبراني). على الرغم من أن الخبرة السابقة في مجال الأمن السيبراني ليست إلزامية؛ إلا أن الفهم الأساسي لهذا القطاع أمر ضروري.
- **تتطلب الأدوار التي تبدأ من المستوى ٣** (بدون مستويات ١ أو ٢) **مستوىً متوسطًا** من الخبرة في مجال الأمن السيبراني. يجب أن يكون لدى المهنيين في هذه المناصب الوظيفية، فهماً قوياً، وخبرة عملية في ممارسات الأمن السيبراني.

الفئة	التخصّص	الأدوار	المستويات				
			١	٢	٣	٤	٥
معمارية الأمن السيبراني والبحث والتطوير	معمارية الأمن السيبراني	مصمم معمارية الأمن السيبراني			✓	✓	
		أخصائي الحوسبة السحابية الآمنة		✓	✓	✓	
	الأبحاث والتطوير في الأمن السيبراني	أخصائي تطوير أمن النُظم	✓	✓	✓	✓	
		مطور الأمن السيبراني	✓	✓	✓	✓	
		مُقيّم البرمجيات الآمنة	✓	✓	✓	✓	
		باحث الأمن السيبراني	✓	✓	✓	✓	
		أخصائي علم البيانات للأمن السيبراني		✓	✓	✓	
		أخصائي الذكاء الاصطناعي للأمن السيبراني		✓	✓	✓	
القيادة وتطوير الكوادر	القيادة	رئيس إدارة الأمن السيبراني				✓	✓
		مدير الأمن السيبراني			✓	✓	✓
		مستشار الأمن السيبراني				✓	✓
	تطوير الكوادر	مدير الموارد البشرية للأمن السيبراني		✓	✓	✓	
		مُطوّر المناهج التعليمية للأمن السيبراني	✓	✓	✓	✓	
		مدرب الأمن السيبراني	✓	✓	✓	✓	
الحوكمة والمخاطر والالتزام والقوانين	الحوكمة والمخاطروالالتزام	أخصائي مخاطر الأمن السيبراني	✓	✓	✓	✓	
		أخصائي الالتزام في الأمن السيبراني	✓	✓	✓	✓	
		أخصائي سياسات الأمن السيبراني	✓	✓	✓	✓	

		مُقيّم ضوابط الأمن السيبراني	✓	✓	✓	✓			
		مُدقّق الأمن السيبراني		✓	✓	✓			
	القوانين وحماية البيانات	أخصائي قانون الأمن السيبراني	✓	✓	✓	✓			
		أخصائي حماية البيانات	✓	✓	✓	✓			
الحماية والدفاع	الدفاع	محلل دفاع الأمن السيبراني	✓	✓	✓	✓	✓		
		أخصائي البنية التحتية للأمن السيبراني		✓	✓	✓	✓		
		أخصائي الأمن السيبراني	✓	✓	✓				
	الحماية	أخصائي التشفير		✓	✓	✓	✓		
		أخصائي إدارة الهويّة والوصول		✓	✓	✓	✓		
		محلل أمن النُظم	✓	✓	✓	✓	✓		
	تقييم الثغرات	أخصائي تقييم الثغرات	✓	✓	✓				
		أخصائي اختبار الاختراقات			✓	✓	✓		
	الاستجابة للحوادث	أخصائي استجابة للحوادث السيبرانية			✓	✓	✓		
		أخصائي التحليل الجنائي الرقمي			✓	✓	✓		
		أخصائي تحقيقات الجرائم السيبرانية			✓	✓	✓		
		أخصائي الهندسة العكسية للبرمجيات الضارة				✓	✓		
	إدارة التهديدات	محلّل معلومات التهديدات السيبرانية			✓	✓	✓		
		أخصائي اكتشاف التهديدات السيبرانية				✓	✓		
نظم التحكم الصناعية والتقنيات التشغيلية	نظم التحكم الصناعية والتقنيات التشغيلية	مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية				✓	✓		
		أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية			✓	✓	✓		
		محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية			✓	✓	✓		
		أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية			✓	✓	✓		
		أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية				✓	✓		

جدول ٧: نظرة عامة على الأدوار والمستويات

تتناول الأقسام الآتية شرحًا تفصيليًا لكل دور وظيفي ومستوى، مع رسوم بيانية وجداول توضح المسارات المهنية المحتملة. ولتبسيط العرض، لم يجرِ تضمين بعض التنقلات بشكل واضح؛ لكنها تبقى خيارات متاحة على النحو الآتي:

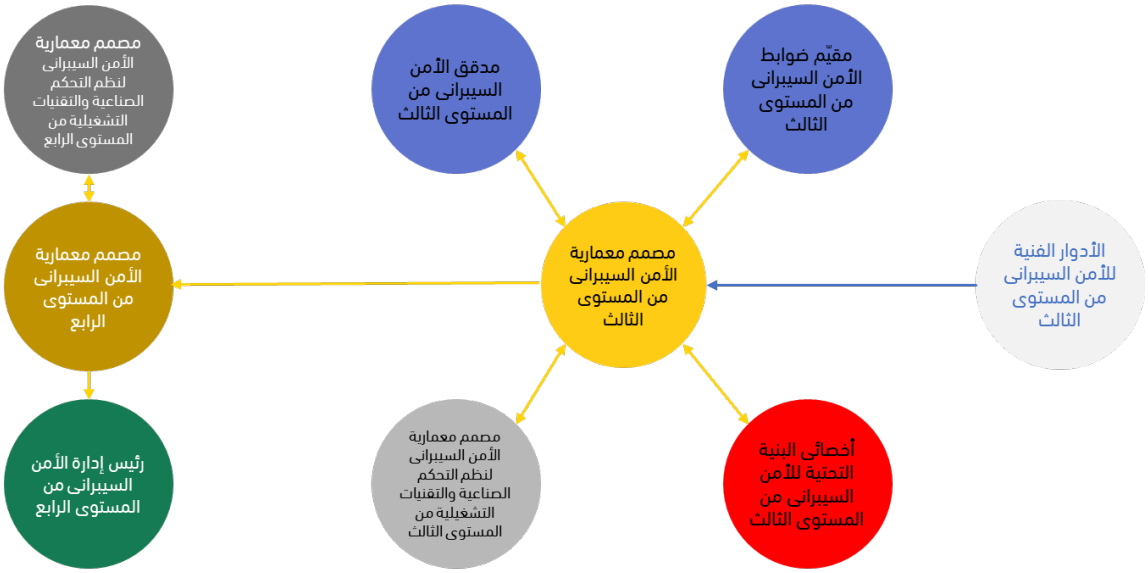
- التنقل الأفقي بين الأدوار الوظيفية، ضمن الفئة الوظيفية نفسها (للمستويين الأول والثاني).
- يستطيع أصحاب المستوى الأول من المؤهلات العلمية من الخريجين المبتدئين؛ بدء أي دور وظيفي في المستوى الأول[١]
- يستطيع أصحاب المستوى الثاني من المؤهلات العلمية من الخريجين المبتدئين؛ بدء أي دور وظيفي في المستوى الثاني[٢]
- الانتقال من أي دور وظيفي من المستوى الثالث إلى دور مدير الأمن السيبراني من المستوى الثالث.
- الانتقال من أي دور وظيفي من المستوى الرابع إلى دور مدير الأمن السيبراني من المستوى الرابع، أو مستشار الأمن السيبراني من المستوى الرابع.

[١] يرجى الرجوع إلى "الخريج الحاصل على المستوى الأول من المؤهلات العلمية" في الجدول ٣ للحصول على مزيد من التفاصيل
[٢] يرجى الرجوع إلى "الخريج الحاصل على المستوى الثاني من المؤهلات العلمية" في الجدول ٣ للحصول على مزيد من التفاصيل

٢. معمارية الأمن السيبراني والبحث والتطوير (CARD)

٢,١ مصمم معمارية الأمن السيبراني

يقوم مصمم معمارية الأمن السيبراني بتصميم نظم وشبكات الأمن السيبراني، والإشراف على إعداداتها، وتطويرها وتنفيذها. يتطلب هذا الدور الحصول على شهادات، أو تدريب في تصميم المعمارية الآمنة، وإدارة المخاطر، والإعداد الآمن، وتقييم مخاطر الأمن السيبراني، والتعافي من الكوارث، ودمج الأمن في تصميم النُظم.



شكل ٣: الخريطة الوظيفية لمصمم معمارية الأمن السيبراني

١,١,٢ مصمم معمارية الأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: مصمم معمارية الأمن السيبراني (CARD-CA-001)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يتولى إدارة الفريق، أو توجيه الآخرين في مجال التصميم والإشراف على نظم وشبكات الأمن السيبراني وإعداداتها، وتطويرها، وتنفيذها. يتحمل الفرد في هذا الدور مسؤولية تنفيذ مهمات مصمم معمارية الأمن السيبراني، ولكن بمستوى أقل، إذ ينجز مهمات معقدة، تتعلق بالدور الوظيفي؛ ليجري مراجعتها من قبل مصمم معمارية الأمن السيبراني من المستوى الرابع، مع العمل تحت توجيهه. وستتضمن مهماته إجراء مراجعات للأمن السيبراني، وتحديد الفجوات في المعمارية الأمنية، وتطبيق ودمج تقنيات المعلومات في الحلول المقترحة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الأدوار الفنية للأمن السيبراني من المستوى الثالث. • أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث. • مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث. • مُقيّم ضوابط الأمن السيبراني من المستوى الثالث. • مُدقّق الأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مصمم معمارية الأمن السيبراني من المستوى الرابع. • أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث. • مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث. • مُدقّق الأمن السيبراني من المستوى الثالث. • مُقيّم ضوابط الأمن السيبراني من المستوى الثالث.

جدول ٨: مصمم معمارية الأمن السيبراني من المستوى الثالث

٢,١,٢ مصمم معمارية الأمن السيبراني من المستوى الرابع

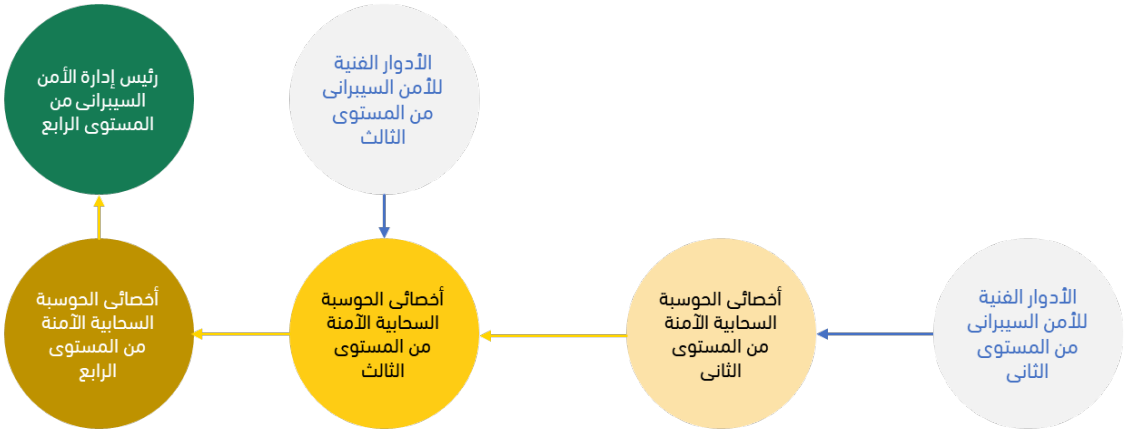
مسمى الدور الوظيفي: مصمم معمارية الأمن السيبراني (CARD-CA-001)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً لتصميم شبكات الأمن السيبراني ونظمه، والإشراف على إعداداتها وتطويرها وتنفيذها. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم مهمات مصمم معمارية الأمن السيبراني من المستوى الثالث، وضمان اكتمالها؛ وفقًا للمعايير المناسبة، وضمن الأطر الزمنية المحددة. تشمل المهمات تحديد أولويات وظائف الأعمال المهمة، بالتعاون مع الجهات المعنية في المنظمة، وتقديم المشورة بشأن تكاليف المشروع، أو مفاهيم التصميم، أو التغييرات التي تطرأ عليه.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مصمم معمارية الأمن السيبراني من المستوى الثالث. • مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • رئيس إدارة الأمن السيبراني من المستوى الرابع. • مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع.

جدول ٩: مصمم معمارية الأمن السيبراني من المستوى الرابع

٢,٢ أخصائي الحوسبة السحابية الآمنة

يقوم أخصائي الحوسبة السحابية الآمنة، بتصميم نظم الحوسبة السحابية الآمنة، وتنفيذها، وتشغيلها مع تطوير سياسات السحابة الآمنة. يتطلب هذا الدور الحصول على شهادات، أو تدريب في مجال الحوسبة السحابية، وتصميم أمن النُظم، وتقييم المخاطر، ومنهجيات الاختبار الآمنة.

١,٢,٢ أخصائي الحوسبة السحابية الآمنة من المستوى الثاني



شكل ٤: الخريطة الوظيفية لأخصائي الحوسبة السحابية الآمنة

مسمى الدور الوظيفي: أخصائي الحوسبة السحابية الآمنة (CARD-CA-002)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يسهم في تصميم نظم الحوسبة السحابية الآمنة، وتنفيذها، وتشغيلها؛ إلى جانب المساعدة في تطوير سياسات الحوسبة السحابية الآمنة. يعمل الفرد في هذا الدور على تنفيذ بعض المهمات الأساسية تحت الإشراف؛ مع تعزيز مهاراته من خلال التطبيق العملي، تشمل مسؤولياته دعم تكامل عناصر الأمن السحابي، ضمن نظم المنظمة، ومراقبة البيئات السحابية، للكشف عن الثغرات.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الأدوار الفنية للأمن السيبراني من المستوى الثاني. • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي الحوسبة السحابية الآمنة من المستوى الثالث.

جدول ١٠: أخصائي الحوسبة السحابية الآمنة من المستوى الثاني

٢,٢,٢ أخصائي الحوسبة السحابية الآمنة من المستوى الثالث

مسمى الدور الوظيفي: أخصائي الحوسبة السحابية الآمنة (CARD-CA-002)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول، يتولى إدارة الفريق، أو توجيه الآخرين في مجال تصميم نظم الحوسبة السحابية الآمنة، وتنفيذها، وتشغيلها، وتطوير سياسات الحوسبة السحابية الآمنة. يتحمل الفرد في هذا الدور مسؤولية تنفيذ الكثير من أعمال أخصائي الحوسبة السحابية الآمنة، على مستوى أدنى، وتنفيذ المهمات المعقدة المتعلقة بالدور الوظيفي؛ لمراجعتها من قبل أخصائي الحوسبة السحابية الآمنة من المستوى الرابع، والعمل تحت إشرافه. وتشمل المهمات تطوير عناصر المعمارية الأمنية؛ للحد من التهديدات عند ظهورها، وبناء الضوابط الأمنية لمراقبة المعلومات الموجودة وحمايتها في البيئات السحابية بشكل صحيح.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي الحوسبة السحابية الآمنة من المستوى الثاني. • الأدوار الفنية للأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي الحوسبة السحابية الآمنة من المستوى الرابع.

جدول ١١: أخصائي الحوسبة السحابية الآمنة من المستوى الثالث

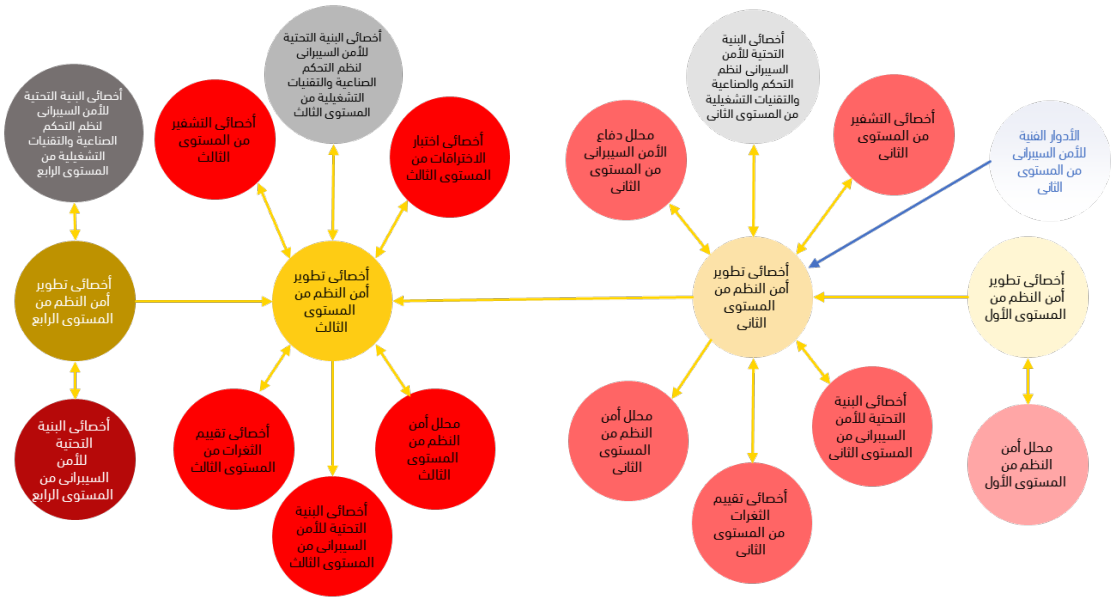
٣,٢,٢ أخصائي الحوسبة السحابية الآمنة من المستوى الرابع

مسمى الدور الوظيفي: أخصائي الحوسبة السحابية الآمنة (CARD-CA-002)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير في إدارة وحدة تعنى بتصميم نظم الحوسبة السحابية الآمنة وتنفيذها، ومن ثم تشغيلها، وتطوير سياسات الحوسبة السحابية الآمنة. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال أخصائي السحابة الآمنة من المستوى الثالث، وضمان اكتمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية المحددة. سوف تشمل المهمات توفير الخبرات المتخصصة؛ لتصميم الجيل القادم من الأمن السيبراني وتطويره للمنظمة والعمل ضمن فرق متعددة التخصصات، وعبر هذه الفرق بوصفه خبيرًا في مجال منهجيات المعمارية الأمنية السحابية ومعاييرها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي الحوسبة السحابية الآمنة من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • رئيس إدارة الأمن السيبراني من المستوى الرابع.

جدول ١٢: أخصائي الحوسبة السحابية الآمنة من المستوى الرابع

٣,٢ أخصائي تطوير أمن النُظم

يتولى أخصـــائي تطوير أمن النُظم، تصـــميم أمن نظم المعلومات، وتطويره واختباره وتقييمه في جميع مراحل تطوير تلك النُظم. تعد الشهادات، أو التدريب في مجال تطوير البرمجيات الآمنة، وتصميم أمن النُظم، وممارسات الترميز الآمنة، وتقييم الثغرات الأمنية، ومنهجيات الاختبار الأمني ضرورية لهذا الدور.



شكل٥ : الخريطة الوظيفية لأخصائي تطوير أمن النظم

١,٣,٢ أخصائي تطوير أمن النُظم من المستوى الأول

مسمى الدور الوظيفي: أخصائي تطوير أمن النُظم (CARD-CRD-001)	المستوى الوظيفي: المستوى الأول
وصف الدور الوظيفي	مساعدة فريق التطوير في تصميم أمن نظم المعلومات وتطويرها واختبارها وتقييمها في جميع مراحل تطوير النظام. يؤدي الفرد في هذا الدور مهمات أساسية تحت إشراف مباشر، في حين أنه يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات دعم أنشطة اختبار، وتقييم الشهادات الأمنية، وإجراء تقييمات لمخاطر الأمن السيبراني.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • محلل أمن النُظم من المستوى الأول. • الخريج الحاصل على المستوى الأول من المؤهلات العلمية.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي تطوير أمن النُظم من المستوى الثاني. • محلل أمن النُظم من المستوى الأول.

جدول ١٣: أخصائي تطوير أمن النُظم من المستوى الأول

٢,٣,٢ أخصائي تطوير أمن النُظم من المستوى الثاني

مسمى الدور الوظيفي: أخصائي تطوير أمن النُظم (CARD-CRD-001)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	يتولى الممارس تصميم أمن نظم المعلومات وتطويرها واختبارها وتقييمها في جميع مراحل تطوير النظام. يعمل الفرد في هذا الدور على الإشراف على العمل، الذي يقوم به أخصائي تطوير أمن النُظم من المستوى الأول، ويواصل تطوير مهاراته، من خلال التطبيق العملي. تتضمن المسؤوليات إجراء تحليل شامل للمخاطر عند إدخال تغييرات كبيرة على أي نظام، أو تطبيق؛ إضافةً إلى دراسة قيود التصميم، والمفاضلة بين الخيارات المختلفة؛ لضمان تصميم أمن سيبراني متكامل، يأخذ في الحسبان متطلبات دورة الحياة التشغيلية.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • أخصائي تطوير أمن النُظم من المستوى الأول. • الأدوار الفنية للأمن السيبراني من المستوى الثاني. • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني. • أخصائي التشفير من المستوى الثاني. • محلل دفاع الأمن السيبراني من المستوى الثاني. • أخصائي تقييم الثغرات من المستوى الثاني. • محلل أمن النُظم من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي تطوير أمن النُظم من المستوى الثالث • محلل دفاع الأمن السيبراني من المستوى الثاني • محلل أمن النُظم من المستوى الثاني • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني • أخصائي تقييم الثغرات من المستوى الثاني • أخصائي التشفير من المستوى الثاني • أخصائي البنية التحتية للأمن السيبراني من المستوى الثاني

جدول ١٤: أخصائي تطوير أمن النُظم من المستوى الثاني

٣,٣,٢ أخصائي تطوير أمن النُظم من المستوى الثالث

مسمى الدور الوظيفي: أخصائي تطوير أمن النُظم (CARD-CRD-001)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول في تصميم أمن نظم المعلومات وتطويره واختباره وتقييمه في جميع مراحل تطوير النظام. يتحمل الفرد في هذا الدور مسؤولية تنفيذ الكثير من أعمال أخصائي تطوير أمن النُظم على مستوى أدنى، وتنفيذ المهمات المعقدة المتعلقة بالدور لمراجعتها من قبل أخصائي تطوير أمن النُظم من المستوى الرابع، والعمل تحت إشرافه. تشمل المهمات استخدام النماذج، والمحاكاة لتحليل أداء النظام، أو التنبؤ به في ظل ظروف التشغيل المختلفة وإعداد وثائق التصميم الأمني التفصيلية لمواصفات المكونات والواجهة لدعم تصميم النظام وتطويره.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي تطوير أمن النُظم من المستوى الثاني. • أخصائي التشفير من المستوى الثالث. • محلل أمن النُظم من المستوى الثالث. • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث. • أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث. • أخصائي تقييم الثغرات من المستوى الثالث. • أخصائي اختبار الاختراقات من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي تطوير أمن النُظم من المستوى الرابع. • أخصائي التشفير من المستوى الثالث. • أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث. • محلل أمن النُظم من المستوى الثالث. • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث. • أخصائي تقييم الثغرات من المستوى الثالث. • أخصائي اختبار الاختراقات من المستوى الثالث.

جدول ١٥: أخصائي تطوير أمن النُظم من المستوى الثالث

٤,٣,٢ أخصائي تطوير أمن النُظم من المستوى الرابع

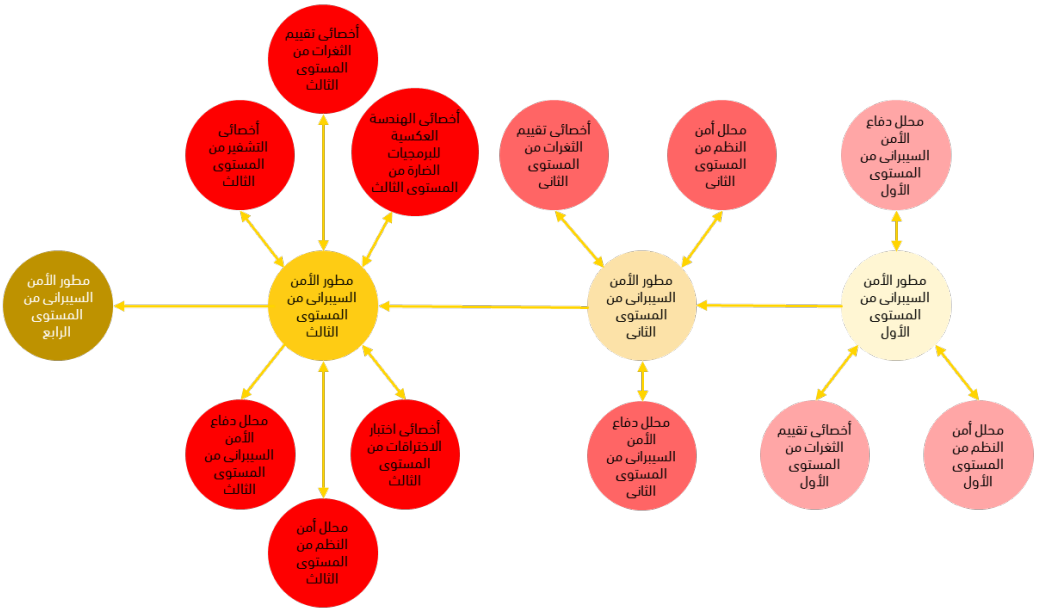
مسمى الدور الوظيفي: أخصائي تطوير أمن النُظم (CARD-CRD-001)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً تعنى بتصميم أمن نظم المعلومات، وتطويرها، واختبارها، وتقييمها في جميع مراحل تطوير تلك النُظم. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على الكثير من أعمال أخصائي تطوير أمن النُظم من المستوى الثالث، وضمان اكتمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية ذات الصلة. تشمل المهمات تصميم إستراتيجيات متكاملة؛ للحد من المخاطر، بما يتسق مع توجهات المنظمة لإدارة المخاطر، مع ضمان تحقيق التوازن بين التكلفة، والجدول الزمني، والأداء، والأمن.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية:	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية:
• أخصائي تطوير أمن النُظم من المستوى الثالث. • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع. • أخصائي البنية التحتية للأمن السيبراني من المستوى الرابع.	• أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع. • أخصائي البنية التحتية للأمن السيبراني من المستوى الرابع.

جدول ١٦: أخصائي تطوير أمن النُظم من المستوى الرابع

٤,٢ مطور الأمن السيبراني

يقوم مطور الأمن السيبراني بتطوير برمجيات، وتطبيقات، ونظم، ومنتجات الأمن السيبراني. يتطلب هذا الدور الحصول على شهادات، أو تدريب في مجال تطوير البرمجيات الآمنة، وأمن التطبيقات، وممارسات الترميز الآمنة، وتقنيات الحد من الثغرات.



شكل ٦: الخريطة الوظيفية لمطور الأمن السيبراني

١,٤,٢ مطور الأمن السيبراني من المستوى الأول

مسمى الدور الوظيفي:	المستوى الوظيفي:
مطور الأمن السيبراني (CARD-CRD-002)	المستوى الأول

وصف الدور الوظيفي	دعم تطوير برمجيات الأمن السيبراني، وتطبيقاته، ونظمه، ومنتجاته. يؤدي الفرد في هذا الدور مهمات أساسية تحت إشراف مباشر، في حين يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات تطبيق معايير الترميز، واختبار الأمان، وتوثيق التعليمات البرمجية الآمنة.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية • محلل دفاع الأمن السيبراني من المستوى الأول. • محلل أمن النُظم من المستوى الأول. • أخصائي تقييم الثغرات من المستوى الأول. • الأدوار الرئيسية للأمن السيبراني من المستوى الأول.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مطور الأمن السيبراني من المستوى الثاني. • محلل دفاع الأمن السيبراني من المستوى الأول. • محلل أمن النُظم من المستوى الأول. • أخصائي تقييم الثغرات من المستوى الأول.

جدول ١٧: مطور الأمن السيبراني من المستوى الأول

٢,٤,٢ مطور الأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي:	المستوى الوظيفي:
مطور الأمن السيبراني (CARD-CRD-002)	المستوى الثاني

وصف الدور الوظيفي	ممارس يقوم بتطوير برمجيات الأمن السيبراني، وتطبيقاته، ونظمه، ومنتجاته. سيتولى الفرد في هذا الدور الإشراف على العمل الذي يقوم به مطور الأمن السيبراني من المستوى الأول، ويواصل تطوير مهاراته؛ من خلال التطبيق العملي. تشمل المهمات دمج عناصر الأمن السيبراني في مرحلة تحديد المتطلبات؛ من خلال تعريف ضوابط الأمان، وتوثيقها بوضوح؛ مع ضمان أن عمليات تطوير البرامج وتحديثها موثقة بشكل يسهل على الآخرين فهمها، وذلك باستخدام تعليقات مدمجة داخل التعليمات المشفرة.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • مطور الأمن السيبراني من المستوى الأول. • الأدوار الفنية للأمن السيبراني من المستوى الثاني. • محلل دفاع الأمن السيبراني من المستوى الثاني. • محلل أمن النُظم من المستوى الثاني. • أخصائي تقييم الثغرات من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مطور الأمن السيبراني من المستوى الثالث. • محلل دفاع الأمن السيبراني من المستوى الثاني. • محلل أمن النُظم من المستوى الثاني. • أخصائي تقييم الثغرات من المستوى الثاني.

جدول ١٨: مطور الأمن السيبراني من المستوى الثاني

٣,٤,٢ مطور الأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: مطور الأمن السيبراني (CARD-CRD-002)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يقوم بتطوير برمجيات الأمن السيبراني، وتطبيقاته، ونظمه، ومنتجاته. يتحمل الفرد في هذا الدور مسؤولية تنفيذ الكثير من أعمال مطور الأمن السيبراني على مستوى أدنى، وتنفيذ المهمات المعقدة المتعلقة بالعمل، لمراجعتها ويعمل تحت إشراف مطور الأمن السيبراني من المستوى الرابع. تتضمن المهمات إنشاء مخططات سير عمل تفصيلية، ورسوم بيانية توضح المدخلات والمخرجات، والعمليات المنطقية لنظم الأمان، بالإضافة إلى تحويل متطلبات الأمان إلى مكونات تصميم التطبيقات، مثل توثيق أسطح الهجوم البرمجي، وتصميم نماذج التهديدات، وتحديد المعايير الأمنية المطلوبة.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مطور الأمن السيبراني من المستوى الثاني. • أخصائي التشفير من المستوى الثالث. • محلل دفاع الأمن السيبراني من المستوى الثالث. • أخصائي الهندسة العكسية للبرمجيات الضارة من المستوى الثالث. • محلل أمن النُظم من المستوى الثالث. • أخصائي تقييم الثغرات من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مطور الأمن السيبراني من المستوى الرابع. • أخصائي التشفير من المستوى الثالث. • محلل دفاع الأمن السيبراني من المستوى الثالث. • أخصائي الهندسة العكسية للبرمجيات الضارة من المستوى الثالث. • محلل أمن النُظم من المستوى الثالث. • أخصائي تقييم الثغرات من المستوى الثالث. • أخصائي اختبار الاختراقات من المستوى الثالث.

جدول ١٩: مطور الأمن السيبراني من المستوى الثالث

٤,٤,٢ مطور الأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: مطور الأمن السيبراني (CARD-CRD-002)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً لتطوير برمجيات الأمن السيبراني، وتطبيقاته، ونظمه، ومنتجاته. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم مهمات مطور الأمن السيبراني من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة، وضمن الأطر الزمنية المحددة. تشمل المهمات دراسة كيفية تلبية متطلبات المستخدم والبرمجيات بما يتوافق مع سياسات الأمن السيبراني، مع تقييم مدى إمكانية تطبيق التصميم بكفاءة، ضمن الإطار الزمني والتكلفة المتاحة.

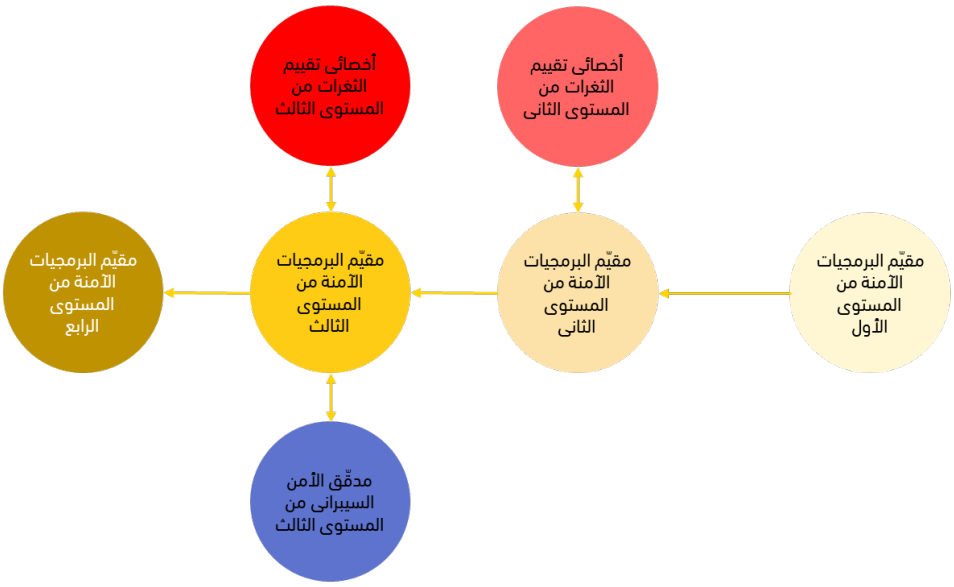
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مطور الأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ٢٠: مطور الأمن السيبراني من المستوى الرابع

٥,٢ مُقيّم البرمجيات الآمنة

يقوم مقيّم البرمجيات الآمنة بتقييم أمن تطبيقات الحاسب، وبرمجياته، وشفراته، أو برامجه مع تقديم نتائج قابلة للتطبيق. يتطلب هذا الدور الوظيفي الحصول على شهادات، أو تدريب في تقييم البرمجيات الآمنة، وممارسات التشفير الآمنة، وتحديد الثغرات، ومعايير أمن البرمجيات.

١,٥,٢ مُقيّم البرمجيات الآمنة من المستوى الأول



شكل ٧: الخريطة الوظيفية لمُقيّم البرمجيات الآمنة

مسمى الدور الوظيفي: مقيم البرمجيات الآمنة (CARD-CRD-003)	المستوى الوظيفي: المستوى الأول
وصف الدور الوظيفي	دعم الفريق في تقييم أمن تطبيقات الحاسب، وبرمجياته، وشفراته، أو برامجه، مع تقديم نتائج قابلة للتطبيق. يؤدي الفرد في هذا الدور مهمات أساسية تحت إشراف مباشر، بينما يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات مراجعة الجوانب الأمنية عند قبول البرمجيات، وإجراء اختبارات تشغيل؛ للتأكد من تحقيق النتائج المطلوبة في البرامج والتطبيقات، مع ضمان صحة التعليمات وتوافق مستويات الأمان.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية. • الأدوار الرئيسية للأمن السيبراني من المستوى الأول.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مُقيّم البرمجيات الآمنة من المستوى الثاني.

جدول ٢١: مُقيّم البرمجيات الآمنة من المستوى الأول

٢,٥,٢ مُقيّم البرمجيات الآمنة من المستوى الثاني

مسمى الدور الوظيفي: مقيم البرمجيات الآمنة (CARD-CRD-003)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يقوم بتقييم أمن تطبيقات الحاسب، وبرمجياته، وشفراته، أو برامجه، مع تقديم نتائج قابلة للتطبيق. سيتولى الفرد في هذا الدور الإشراف على العمل الذي يقوم به مقيّم البرمجيات الآمنة من المستوى الأول، وسوف يواصل تطوير مهاراته من خلال التطبيق العملي لعمله. تشمل المهمات تنفيذ اختبارات أمنية شاملة للبرمجيات، وتحليل الشفرات البرمجية لاكتشاف الثغرات ومعالجتها، إلى جانب تحديد التحديثات البرمجية والإصدارات التي قد تحتوي على ثغرات في البرمجيات، ومن ثم توثيقها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • مُقيّم البرمجيات الآمنة من المستوى الأول. • أخصائي تقييم الثغرات من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مُقيّم البرمجيات الآمنة من المستوى الثالث. • أخصائي تقييم الثغرات من المستوى الثاني.

جدول ٢٢: مُقيّم البرمجيات الآمنة من المستوى الثاني

٣,٥,٢ مُقيّم البرمجيات الآمنة من المستوى الثالث

مسمى الدور الوظيفي: مقيم البرمجيات الآمنة (CARD-CRD-003)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يقوم بتقييم أمن تطبيقات الحاسب، وبرمجياته وشفراته، أو برامجه، مع تقديم نتائج قابلة للتطبيق.
	يتحمل الفرد في هذا الدور مسؤولية تنفيذ الكثير من أعمال مقيّم البرمجيات الآمنة على مستوى أدنى، وتنفيذ المهمات المعقدة المتعلقة بالدور الوظيفي، لمراجعتها من قبل مقيّم البرمجيات الآمنة من المستوى الرابع والعمل تحت إشرافه. تتضمن المهمات إجراء تحليل للمخاطر عند تنفيذ تغييرات جوهرية على التطبيقات، أو النُظم، مع الإشراف على فرق العمل المسؤولة عن مهمات الأمن السيبراني، وضمان توزيعها على الفرق بكفاءة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مُقيّم البرمجيات الآمنة من المستوى الثاني. • أخصائي تقييم الثغرات من المستوى الثالث. • مُدقّق الأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مُقيّم البرمجيات الآمنة من المستوى الرابع. • أخصائي تقييم الثغرات من المستوى الثالث. • مُدقّق الأمن السيبراني من المستوى الثالث.

جدول ٢٣: مُقيّم البرمجيات الآمنة من المستوى الثالث

٤,٥,٢ مُقيّم البرمجيات الآمنة من المستوى الرابع

مسمى الدور الوظيفي:	المستوى الوظيفي:
مقيم البرمجيات الآمنة (CARD-CRD-003)	المستوى الرابع

وصف الدور الوظيفي	خبير يدير وحدةً تعنى بتقييم مستوى الأمن في تطبيقات الحاسب، وبرمجياته، وشفراته، أو برامجه مع تقديم نتائج قابلة للتطبيق. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال مُقيّم البرمجيات الآمنة من المستوى الثالث، وضمان استكمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية المحددة. تشمل المهمات تصميم نماذج التهديد، بناءً على احتياجات العملاء، ومدخلاتهم، وتحويل متطلبات الأمان إلى عناصر تصميم متكاملة داخل التطبيقات.

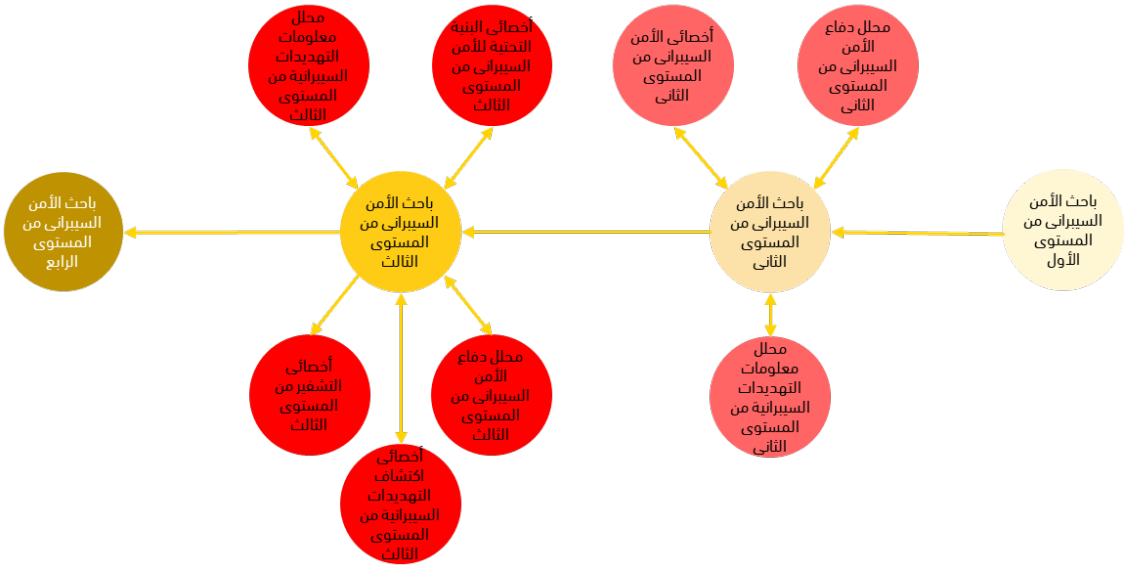
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مُقيّم البرمجيات الآمنة من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ٢٤: مُقيّم البرمجيات الآمنة من المستوى الرابع

٦,٢ باحث الأمن السيبراني

يقوم باحث الأمن السيبراني بإجراء الأبحاث العلمية في هذا المجال، ويستلزم هذا العمل الحصول على شهادات، أو تدريبات في منهجيات البحث السيبراني، وتحليل الثغرات الأمنية، وتطوير الأدوات والتقنيات ذات الصلة؛ إلى جانب الحصول على تدريبات متخصصة في المجالات البحثية المستهدفة.

١,٦,٢باحث الأمن السيبراني من المستوى الأول



شكل ٨: الخريطة الوظيفية لباحث الأمن السيبراني

مسمى الدور الوظيفي: باحث الأمن السيبراني (CARD-CRD-004)	المستوى الوظيفي: المستوى الأول
وصف الدور الوظيفي	دعم الفريق؛ لإجراء الأبحاث العلمية في مجال الأمن السيبراني. يؤدي الفرد في هذا الدور مهمات أساسية تحت إشراف مباشر، بينما يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات تقييم الثغرات في البنية التحتية للشبكات، والالتزام بمعايير دورة حياة هندسة النُظم والبرمجيات، وعملياتها أثناء تطوير نظم الأمن السيبراني وحلوله.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • باحث الأمن السيبراني من المستوى الثاني.

جدول ٢٥: باحث الأمن السيبراني من المستوى الأول

٢,٦,٢باحث الأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي: باحث الأمن السيبراني (CARD-CRD-004)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يجري الأبحاث العلمية في مجال الأمن السيبراني. سوف يتولى الفرد في هذا الدور الإشراف على الأعمال التي يقوم بها باحث الأمن السيبراني من المستوى الأول، وسوف يواصل تطوير مهاراته من خلال التطبيق العملي. تشمل المهمات البحث في التقنيات المعاصرة؛ لفهم قدرات الدفاع السيبراني المطلوبة من قبل النُظم، أو الشبكات، وتحديد أدوات الهندسة العكسية وتطويرها؛ لتعزيز القدرات وكشف الثغرات.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • باحث الأمن السيبراني من المستوى الأول. • محلل دفاع الأمن السيبراني من المستوى الثاني. • أخصائي الأمن السيبراني من المستوى الثاني. • محلل معلومات التهديدات السيبرانية من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • باحث الأمن السيبراني من المستوى الثالث. • محلل دفاع الأمن السيبراني من المستوى الثاني. • محلل معلومات التهديدات السيبرانية من المستوى الثاني. • أخصائي الأمن السيبراني من المستوى الثاني.

جدول ٢٦: باحث الأمن السيبراني من المستوى الثاني

٣,٦,٢ باحث الأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: باحث الأمن السيبراني (CARD-CRD-004)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يجري الأبحاث العلمية في مجال الأمن السيبراني. يتحمل الفرد في هذا الدور مسؤولية تنفيذ الكثير من أعمال باحث الأمن السيبراني، ضمن مستوى أدنى، وتنفيذ المهمات المعقدة المتعلقة بالعمل؛ لمراجعتها من قبل باحث الأمن السيبراني من المستوى الرابع والعمل تحت إشرافه. تشمل المهمات تطوير قدرات آمنة لإدارة البيانات؛ لدعم المختصين ومراجعة برامج استخراج البيانات، وعملياتها ومتطلباتها، وتخزينها والتحقق منها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • باحث الأمن السيبراني من المستوى الثاني. • محلل دفاع الأمن السيبراني من المستوى الثالث. • أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث. • محلل معلومات التهديدات السيبرانية من المستوى الثالث. • أخصائي اكتشاف التهديدات السيبرانية من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • باحث الأمن السيبراني من المستوى الرابع. • أخصائي التشفير من المستوى الثالث. • محلل دفاع الأمن السيبراني من المستوى الثالث. • أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث. • محلل معلومات التهديدات السيبرانية من المستوى الثالث. • أخصائي اكتشاف التهديدات السيبرانية من المستوى الثالث.

جدول ٢٧: باحث الأمن السيبراني من المستوى الثالث

٤,٦,٢ باحث الأمن السيبراني من المستوى الرابع

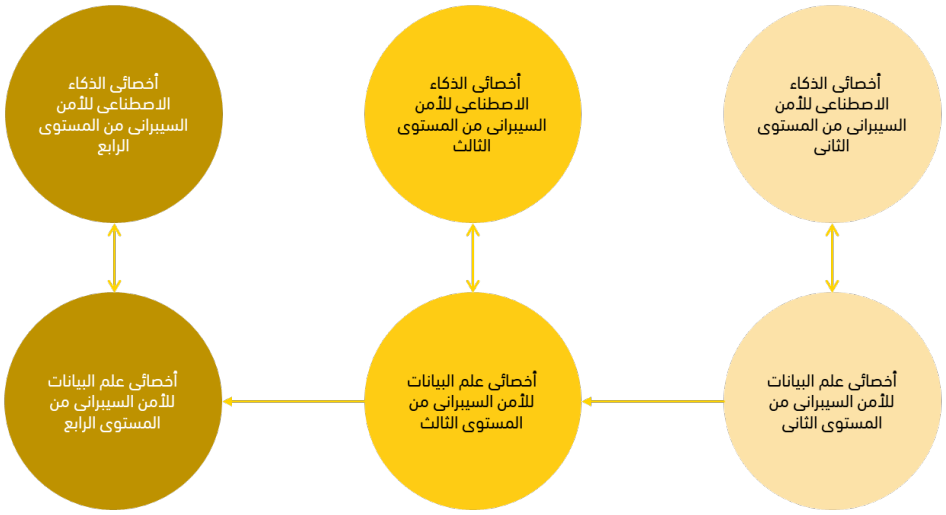
مسمى الدور الوظيفي: باحث الأمن السيبراني (CARD-CRD-004)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً، تعنى بإجراء الأبحاث العلمية في مجال الأمن السيبراني. يتحمل الفرد في هذا الدور مسؤولية الإشراف على معظم أعمال باحث الأمن السيبراني من المستوى الثالث، وضمان اكتمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية ذات الصلة. تشمل المهمات تحديد إستراتيجيات قدرات الأمن السيبراني؛ لتطوير الأجهزة والبرمجيات المخصصة، بناءً على متطلبات المنظمة، والتعاون مع أصحاب المصلحة؛ لتحديد تقنية حلول الأمن السيبراني المناسبة.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • باحث الأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هى أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ٢٨: باحث الأمن السيبراني من المستوى الرابع

٧,٢ أخصائي علم البيانات للأمن السيبراني

يستخدم أخصائي علوم بيانات الأمن السيبراني نماذج رياضية، وأساليب وعمليات علمية، لتصميم خوارزميات ونظم لاستخلاص المرئيات وتنفيذها من الأمن السيبراني من مجموعات بيانات واسعة النطاق. يتطلب هذا العمل الحصول على شهادات، أو تدريب في علوم البيانات، والتحليل الإحصائي، والتعلم الآلي، وتقنيات استخراج البيانات المصممة خصيصًا؛ لتطبيقات الأمن السيبراني.



شكل ٩: الخريطة الوظيفية لأخصائي علم البيانات للأمن السيبراني

١,٧,٢ أخصائي علم البيانات للأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي: أخصائي علم البيانات للأمن السيبراني (CARD-CRD-005)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يستخدم نماذج رياضية، وأساليب، وعمليات علمية؛ لتصميم خوارزميات ونظم وتنفيذها؛ لاستخلاص مرئيات ومعارف الأمن السيبراني من مجموعات بيانات واسعة النطاق. يعمل الفرد في هذا الدور على تنفيذ بعض المهمات الأساسية تحت الإشراف، مع تعزيز مهاراته من خلال التطبيق العملي، وتشمل المهمات جمع المقاييس، وبيانات التوجهات، وتحليل مصادر البيانات؛ لتقديم توصيات قابلة للتطبيق.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي علم البيانات للأمن السيبراني من المستوى الثالث. • أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الثاني.

جدول ٢٩: أخصائي علم البيانات للأمن السيبراني من المستوى الثاني

٢,٧,٢ أخصائي علم البيانات للأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: أخصائي علم البيانات للأمن السيبراني (CARD-CRD-005)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس يستخدم نماذج رياضية وأساليب وعمليات علمية لتصميم خوارزميات ونظم وتنفيذها؛ لاستخلاص مرئيات الأمن السيبراني، ومعارفه من مجموعات بيانات واسعة النطاق. يتحمل الفرد في هذا الدور مسؤولية تنفيذ الكثير من أعمال أخصائي علم البيانات للأمن السيبراني، ضمن مستوى أدنى، وتنفيذ المهمات المعقدة المتعلقة بها؛ لمراجعتها من قبل أخصائي علم البيانات للأمن السيبراني في المستوى الرابع والعمل تحت إشرافه. تشمل المهمات اختبار الفرضيات باستخدام العمليات الإحصائية، والعمل مع محللي النُظم، والمهندسين، والمبرمجين، وغيرهم؛ لتصميم تطبيقات الأمن السيبراني.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي علم البيانات للأمن السيبراني من المستوى الثاني. • أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي علم البيانات للأمن السيبراني من المستوى الرابع. • أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الثالث.

جدول ٣٠: أخصائي علم البيانات للأمن السيبراني من المستوى الثالث

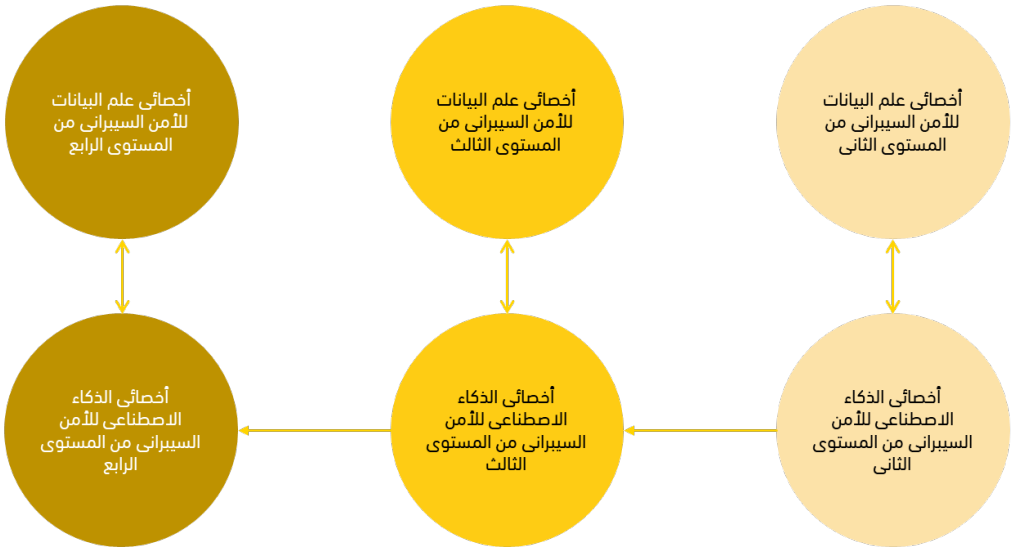
٣,٧,٢ أخصائي علم البيانات للأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: أخصائي علم البيانات للأمن السيبراني (CARD-CRD-005)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً، تستخدم نماذج رياضية، وأساليب وعمليات علمية؛ لتصميم الخوارزميات والنُظم وتنفيذها لتستخلص مرئيات ومعارف الأمن السيبراني من مجموعات بيانات متعددة واسعة النطاق. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال أخصائي علم البيانات للأمن السيبراني من المستوى الثالث، وضمان اكتمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية ذات الصلة. تشمل المهمات تطوير معايير البيانات والسياسات والإجراءات، وتزويد أصحاب المصلحة بتوصيات قابلة للتطبيق، مستمدة من تحليل البيانات والنتائج.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي علم البيانات للأمن السيبراني من المستوى الثالث. • أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الرابع.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الرابع.

جدول ٣١: أخصائي علم البيانات للأمن السيبراني من المستوى الرابع

٨,٢ أخصائي الذكاء الاصطناعي للأمن السيبراني

يستخدم أخصائي الذكاء الاصطناعي للأمن السيبراني نماذج الذكاء الاصطناعي وتقنياته (شاملاً أساليب التعلم الآلي) لتصميم خوارزميات ونظم وتنفيذها؛ لأتمتة وتحسين كفاءة وفعالية مهمات الأمن السيبراني. تعد الشهادات، أو التدريب في مجال الذكاء الاصطناعي، والتعلم الآلي، وتحليل البيانات، وتقنيات الأتمتة لتطبيقات الأمن السيبراني، ضرورية لهذا الدور.



شكل ١٠: الخريطة الوظيفية لأخصائي الذكاء الاصطناعي للأمن السيبراني

١,٨,٢ أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي: أخصائي الذكاء الاصطناعي للأمن السيبراني (CARD-CRD-006)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يستخدم نماذج الذكاء الاصطناعي وتقنياته (شاملاً تقنيات التعلم الآلي) لتصميم خوارزميات ونظم وتنفيذها؛ لأتمتة وتحسين كفاءة وفعالية مهمات الأمن السيبراني. يعمل الفرد في هذا الدور على تنفيذ بعض الأعمال الأساسية تحت الإشراف، مع تعزيز مهاراته من خلال التطبيق العملي، تشمل المهمات استخدام لغات برمجة مختلفة من مصادر مفتوحة؛ لكتابة الشفرات البرمجية، ولفتح الملفات، ولقراءتها، ولكتابة المخرجات في ملفات مختلفة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • أخصائي علم البيانات للأمن السيبراني من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الثالث. • أخصائي علم البيانات للأمن السيبراني من المستوى الثاني.

جدول ٣٢: أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الثاني

٢,٨,٢ أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: أخصائي الذكاء الاصطناعي للأمن السيبراني (CARD-CRD-006)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يستخدم نماذج الذكاء الاصطناعي وتقنياته (شاملاً تقنيات التعلم الآلي) لتصميم خوارزميات ونظم ومن ثم تنفيذها؛ لأتمتة وتحسين كفاءة وفعالية مهمات الأمن السيبراني. يتحمل الفرد في هذا الدور مسؤولية تنفيذ الكثير من أعمال أخصائي الذكاء الاصطناعي للأمن السيبراني على مستوى أدنى، وتنفيذ المهمات المعقدة المتعلقة بالعمل تحت الإشراف والمراجعة من قبل أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الرابع. تشمل المهمات توظيف أدوات التصور لإعداد عروض بيانية، ولوحات معلومات تعكس النتائج بوضوح، مع تنفيذ تحليل إحصائي متقدم، والاستفادة من خوارزميات التعلم الآلي؛ لاستخلاص المرئيات.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الثاني. • أخصائي علم البيانات للأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الرابع. • أخصائي علم البيانات للأمن السيبراني من المستوى الثالث.

جدول ٣٣: أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الثالث

٣,٨,٢ أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الرابع

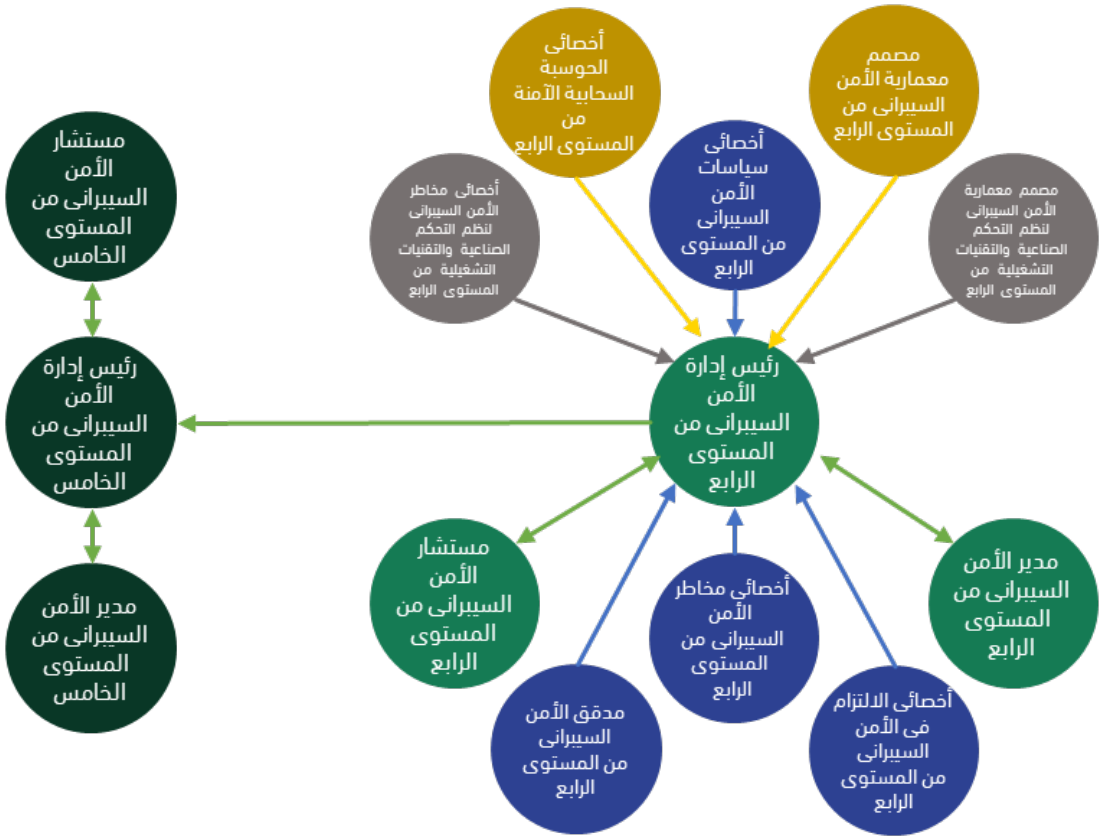
مسمى الدور الوظيفي: أخصائي الذكاء الاصطناعي للأمن السيبراني (CARD-CRD-006)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يتولى إدارة وحدة، تعنى باستخدام نماذج الذكاء الاصطناعي وتقنياته (شاملاً تقنيات التعلم الآلي) لتصميم خوارزميات ونظم وتنفيذها؛ لأتمتة كفاءة وفعالية وتحسين مهمات الأمن السيبراني. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الثالث، وضمان اكتمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية ذات الصلة. تشمل المهمات تطبيق المعرفة بالتعلم الآلي، والتحليلات المرئية الحاسوبية، والاستشعار عن بعد، ومعالجة البيانات الضخمة لحل المشكلات المعقدة، من خلال تطوير برمجيات لقياس كفاءة الخوارزميات والمناهج، ومواكبة أبحاث التحليلات المرئية الحاسوبية، والتعلُّم الآلي لنسخ تقنيات جديدة وتأسيسها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الثالث. • أخصائي علم البيانات للأمن السيبراني من المستوى الرابع.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي علم البيانات للأمن السيبراني من المستوى الرابع.

جدول ٣٤: أخصائي الذكاء الاصطناعي للأمن السيبراني من المستوى الرابع

٣. القيادة وتطوير الكوادر (LWD)

٣,١رئيس إدارة الأمن السيبراني

يتولى رئيس إدارة الأمن السيبراني، إدارة جهود الأمن السيبراني داخل المنظمة، ووضع الرؤية والإستراتيجية لمبادرات الأمن السيبراني، وتقديم المشورة؛ لقيادة إدارة المخاطر السيبرانية بفعالية. يتطلب هذا العمل الحصول على شهادات، أو تدريب في حوكمة الأمن السيبراني، وإدارة المخاطر، وإستراتيجية الأمن السيبراني، والدفاع، ووضع السياسات، والقيادة.



شكل ١١: الخريطة الوظيفية لرئيس إدارة الأمن السيبراني

١,١,٣ رئيس إدارة الأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: رئيس إدارة الأمن السيبراني (LWD-L-001)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	إدارة أعمال الأمن السيبراني داخل المنظمة، ووضع الرؤية، والتوجه بشأن الأمن السيبراني، والإستراتيجيات والموارد والأنشطة ذات العلاقة، وتقديم المشورة لمجلس الإدارة، بشأن أساليب الإدارة الفعّالة لمعالجة مخاطر الأمن السيبراني للمنظمة. يشرف الفرد في هذا الدور على جميع جوانب الأمن السيبراني في المنظمة لضمان أن التدابير المعمول بها تدعم احتياجات الأعمال الخاصة بها. تشمل المهمات التواصل الفعال مع الإدارة العليا، بشأن الجوانب المالية للأنشطة المتعلقة بالأمن السيبراني، ومواءمة إستراتيجية الأمن السيبراني الخاصة بالمنظمة، مع إستراتيجية أعمالها.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مستشار الأمن السيبراني من المستوى الرابع. • مصمم معمارية الأمن السيبراني من المستوى الرابع. • مُدقّق الأمن السيبراني من المستوى الرابع. • أخصائي الالتزام في الأمن السيبراني من المستوى الرابع. • مدير الأمن السيبراني من المستوى الرابع. • أخصائي سياسات الأمن السيبراني من المستوى الرابع. • أخصائي مخاطر الأمن السيبراني من المستوى الرابع. • أخصائي الحوسبة السحابية الآمنة من المستوى الرابع. • مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع. • أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • رئيس إدارة الأمن السيبراني من المستوى الخامس. • مستشار الأمن السيبراني من المستوى الرابع. • مدير الأمن السيبراني من المستوى الرابع

جدول ٣٥: رئيس إدارة الأمن السيبراني من المستوى الرابع

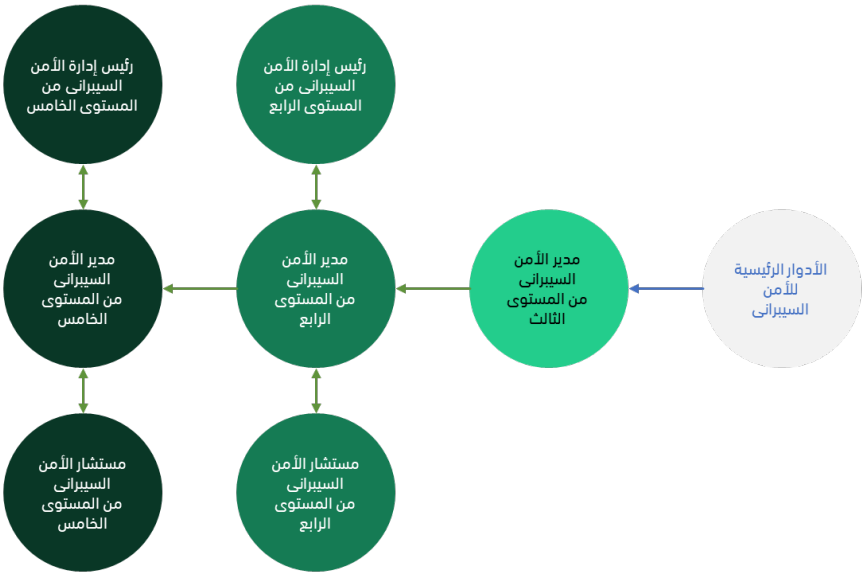
٢,١,٣ رئيس إدارة الأمن السيبراني من المستوى الخامس

مسمى الدور الوظيفي: رئيس إدارة الأمن السيبراني (LWD-L-001)	المستوى الوظيفي: المستوى الخامس
وصف الدور الوظيفي	إدارة أعمال الأمن السيبراني داخل المنظمة، ووضع الإستراتيجية والتوجه بشأن الأمن السيبراني، وكذلك وضع الإستراتيجيات والموارد والأنشطة ذات العلاقة وتقديم المشورة لمجلس الإدارة، حيال أساليب الإدارة الفعّالة، لمخاطر الأمن السيبراني للمؤسسة. يتواصل الفرد في هذا الدور مباشرةً مع مجلس الإدارة، ويكون مسؤولًا عن جميع جوانب الأمن السيبراني على مستوى المنظمة؛ لضمان كون التدابير المعمول بها تدعم احتياجات أعمالها. كما يعنى هذا الدور بالتقنيات والضوابط الأخرى المطبقة؛ لتوفير الأمن السيبراني أكثر من العناية بالأشخاص الذين جرى توظيفهم؛ لتنفيذ هذه الضوابط والحفاظ عليها. تشمل المهمات التعاون مع أصحاب المصلحة في المنظمة، ومع أطراف خارجية عند تحديد متطلبات استراتيجية الأمن السيبراني المستقبلية، وحضور الفعاليات الدولية للأمن السيبراني، وتمثيل المنظمة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • رئيس إدارة الأمن السيبراني من المستوى الرابع. • مدير الأمن السيبراني من المستوى الخامس. • مستشار الأمن السيبراني من المستوى الخامس.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مدير الأمن السيبراني من المستوى الخامس. • مستشار الأمن السيبراني من المستوى الخامس.

جدول ٣٦: رئيس إدارة الأمن السيبراني من المستوى الخامس

٢,٣ مدير الأمن السيبراني

يشرف مدير الأمن السيبراني على أمن نظم المعلومات ووظائفها داخل المنظمة، وقيادة فرق الأمن السيبراني، أو الوحدات، أو الوظائف على مستوى المنظمة. يتطلب هذا العمل الحصول على شهادات، أو تدريب في حوكمة الأمن السيبراني، وإدارة المخاطر، وإستراتيجية الأمن السيبراني، والدفاع، وتطوير السياسات، والقيادة.



شكل ١٢: الخريطة الوظيفية لمدير الأمن السيبراني

١,٢,٣ مدير الأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: مدير الأمن السيبراني (LWD-L-002)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول، يتولى إدارة الأمن السيبراني للوظائف والنُظم المعلوماتية داخل المنظمة، وكذلك قيادة الأمن السيبراني، سواء أكان ذلك على مستوى فريق، أم وحدة، أو وظيفة على مستوى المنظمة. يتولى الفرد في هذا الدور مسؤولية تنفيذ أعمال الإدارة العامة المتعلقة بالموظفين داخل كل فريق، بما في ذلك التقييمات السنوية وتقديم الدعم اليومي لأعضاء الفريق. تشمل المهمات الحصول على الموارد اللازمة؛ لتطوير عمليات فعالة وتنفيذها؛ لتحقيق الأهداف والإستراتيجية للأمن السيبراني، وتحديد الآثار المترتبة على التقنيات الجديدة، والتحديثات على الأمن السيبراني على مستوى المنظمة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الأدوار الرئيسية للأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مدير الأمن السيبراني من المستوى الرابع.

جدول ٣٧: مدير الأمن السيبراني من المستوى الثالث

٢,٢,٣ مدير الأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: مدير الأمن السيبراني (LWD-L-002)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	قيادة فريق، أو وحدة أمن سيبراني، أو وظيفة على مستوى المنظمة، ويعمل على إدارة أمن نظم المعلومات والعمليات المرتبطة بها، داخل المنظمة. يتولى الفرد في هذا الدور مسؤولية تنفيذ مهمات الإدارة العليا المتعلقة بالموظفين، ضمن عدة فرق، بما في ذلك الإدارة المالية والتنبؤ بالميزانية لوحدات المنظمة التي يكون مسؤولًا عنها. وتشمل المهمات ضمان توفير التدريب للتوعية بالأمن السيبراني لجميع الموظفين، وتعزيز قيمة الأمن السيبراني، وإظهارها لأطراف المصلحة داخل المنظمة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مدير الأمن السيبراني من المستوى الثالث. • رئيس إدارة الأمن السيبراني من المستوى الرابع. • مستشار الأمن السيبراني من المستوى الرابع.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مدير الأمن السيبراني من المستوى الخامس. • رئيس إدارة الأمن السيبراني من المستوى الرابع. • مستشار الأمن السيبراني من المستوى الرابع.

جدول ٣٨: مدير الأمن السيبراني من المستوى الرابع

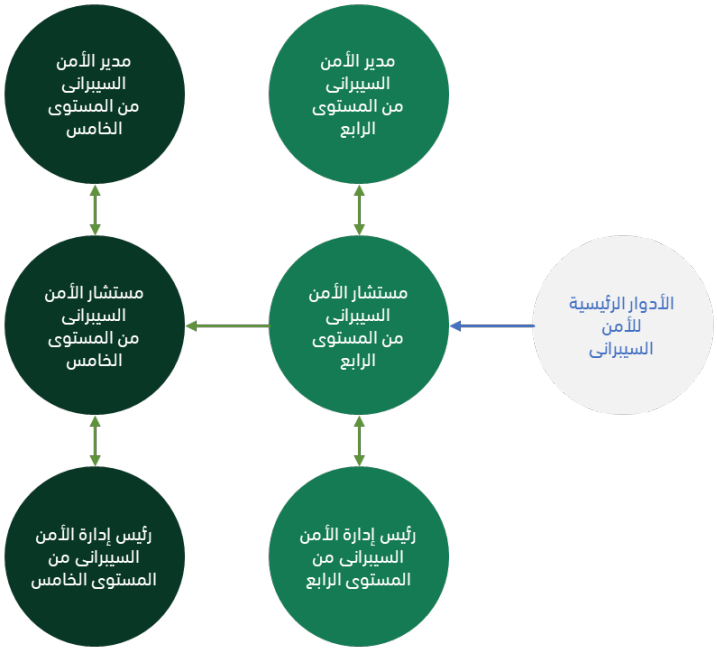
٣,٢,٣ مدير الأمن السيبراني من المستوى الخامس

مسمى الدور الوظيفي: مدير الأمن السيبراني (LWD-L-002)	المستوى الوظيفي: المستوى الخامس
وصف الدور الوظيفي	قيادة فريق، أو وحدة أمن سيبراني، أو وظيفة على مستوى المنظمة، أو العمل على أنه خبير استشاري، إذ يدير أمن نظم المعلومات والعمليات ذات الصلة داخل المنظمة. يتولى الفرد في هذا الدور مسؤولية التواصل المباشر مع مجلس الإدارة وإدارة جميع جوانب فرق الأمن السيبراني على مستوى المنظمة، مع العناية بالكفاءات البشرية وتطويرها أكثر من العناية بالحلول التقنية والضوابط الأمنية. وتشمل المهمات ضمان تحديد احتياجات الأمن السيبراني لجميع نظم تقنية المعلومات، والمشاركة في عمليات الشراء؛ لضمان تطبيق إستراتيجيات فعالة لإدارة مخاطر سلسلة الإمداد.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مدير الأمن السيبراني من المستوى الرابع. • رئيس إدارة الأمن السيبراني من المستوى الخامس. • مستشار الأمن السيبراني من المستوى الخامس.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • رئيس إدارة الأمن السيبراني من المستوى الخامس. • مستشار الأمن السيبراني من المستوى الخامس.

جدول ٣٩: مدير الأمن السيبراني من المستوى الخامس

٣,٣ مستشار الأمن السيبراني

يقوم مستشار الأمن السيبراني بتقديم الرأي والمشورة، لقيادة المنظمة، وقادة الأمن السيبراني، وفرقه في موضوعات الأمن السيبراني. يتطلب هذا الدور الحصول على شهادات، أو تدريب في استراتيجية الأمن السيبراني، والحوكمة، والتواصل بشأن المخاطر، والاستشارات المتعلقة بالسياسات. اعتمادًا على النطاق الاستشاري، قد يشمل التدريب ذو الصلة أيضًا تطوير البرمجيات الآمنة، وأمن الشبكات، وإدارة الحوادث، وأمن الحوسبة السحابية، أو حماية البيانات.



شكل ١٣: الخريطة الوظيفية لمستشار الأمن السيبراني

١,٣,٣ مستشار الأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: مستشار الأمن السيبراني (LWD-L-003)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	تقديم الرأي والمشورة، لقيادة المنظمة، وقادة وفرق الأمن السيبراني في موضوعات الأمن السيبراني. يعد الفرد في هذا الدور، الخبير المتخصص داخل الفريق، ومن ثم ينبغي أن يكون لديه مستوى عالٍ من المهارات الفنية، والمعرفة، والخبرة. تقديم المشورة والتوجيه للفرق / الوكالات / المؤسسات الخارجية، بالإضافة إلى توجيه أعضاء فريق العمل. وتشمل المهمات التواصل الفعال مع الإدارة العليا، بشأن مخاطر الأمن السيبراني، والجوانب المالية للأنشطة المتعلقة بالأمن السيبراني.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • رئيس إدارة الأمن السيبراني من المستوى الرابع. • مدير الأمن السيبراني من المستوى الرابع. • الأدوار الرئيسة للأمن السيبراني من المستوى الرابع.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مستشار الأمن السيبراني من المستوى الخامس. • رئيس إدارة الأمن السيبراني من المستوى الرابع. • مدير الأمن السيبراني من المستوى الرابع.

جدول ٤٠: مستشار الأمن السيبراني من المستوى الرابع

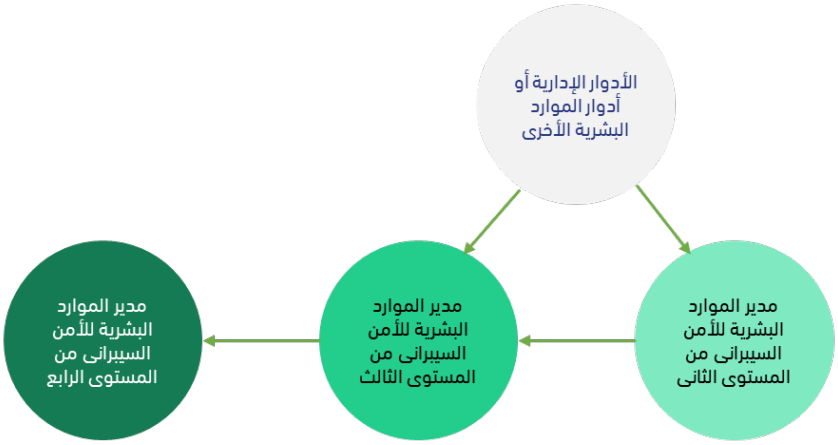
٢,٣,٣ مستشار الأمن السيبراني من المستوى الخامس

مسمى الدور الوظيفي: مستشار الأمن السيبراني (LWD-L-003)	المستوى الوظيفي: المستوى الخامس
وصف الدور الوظيفي	تقديم الرأي والمشورة، لقيادة المنظمة، وفرق الأمن السيبراني، وقادته في موضوعات الأمن السيبراني. يمثل الفرد في هذا الدور المنظمة في مناقشات/مفاوضات رفيعة المستوى تتعلق بالأمن السيبراني. الإسهام في إعداد الأوراق البحثية، والأبحاث الأكاديمية الأخرى. تشمل المهمات فهم الوضع الأمني السيبراني للمؤسسة، والتواصل حوله بوضوح أثناء عمليات التدقيق القانوني والتنظيمي، بالإضافة إلى إبراز مهمات الأمن السيبراني وإقناع أصحاب المصلحة بقيمته الإستراتيجية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية:: • مستشار الأمن السيبراني من المستوى الرابع. • رئيس إدارة الأمن السيبراني من المستوى الخامس. • مدير الأمن السيبراني من المستوى الخامس.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • رئيس إدارة الأمن السيبراني من المستوى الخامس. • مدير الأمن السيبراني من المستوى الخامس.

جدول ٤١: مستشار الأمن السيبراني من المستوى الخامس

٤,٣ مدير الموارد البشرية للأمن السيبراني

يقوم مدير الموارد البشرية للأمن السيبراني بوضع الخطط والإستراتيجيات، والتوجيهات؛ لدعم نمو وإدارة مختصي الأمن السيبراني وإدارته في المنظمة. يتطلب هذا الدور الحصول على شهادات، أو تدريب في التخطيط لمختصي الأمن السيبراني، وإدارة الموارد البشرية، وتدريبها، وتطويرها، بالإضافة إلى الإستراتيجية المؤسسية.



شكل ١٤: الخريطة الوظيفية لمدير الموارد البشرية للأمن السيبراني

١,٤,٣ مدير الموارد البشرية للأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي: مدير الموارد البشرية للأمن السيبراني (LWD-WD-001)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يتولى تطوير الخطط، والإستراتيجيات، والإرشادات داخل المنظمة؛ لدعم تطوير مختصي الأمن السيبراني وإدارتها. يعمل الفرد في هذا الدور على تنفيذ بعض الأعمال الأساسية في إدارة الموارد البشرية، مثل التوظيف والعناية بسجلات الموظفين، مع تطوير مهاراته من خلال التطبيق العملي. وتشمل المهمات تخصيص الموارد لمهمات الأمن السيبراني، والمساعدة في مراجعة فعالية مختصي الأمن السيبراني وتقييمها؛ لتحديد الفجوات في المهارات، ومتطلبات التدريب لهم.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • الأدوار الإدارية أو أدوار الموارد البشرية الأخرى.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مدير الموارد البشرية للأمن السيبراني من المستوى الثالث.

جدول ٤٢: مدير الموارد البشرية للأمن السيبراني من المستوى الثاني

٢,٤,٣ مدير الموارد البشرية للأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: مدير الموارد البشرية للأمن السيبراني (LWD-WD-001)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	يقوم كبير الممارسين بوضع الخطط، والإستراتيجيات، والتوجيه داخل المنظمة؛ لدعم إدارة مختصي الأمن السيبراني، وتطويرهم. يتحمل الفرد في هذا الدور مسؤولية توجيه مدير الموارد البشرية للأمن السيبراني من المستوى الثاني، فضلًا عن تنفيذ المهمات المعقدة المتعلقة بالعمل تحت إشراف مدير الموارد البشرية ومراجعته للأمن السيبراني من المستوى الرابع، وتتضمن المهمات التنسيق مع الخبراء؛ لضمان توافق معايير التأهيل مع احتياجات المنظمة والمعايير في هذا القطاع، إلى جانب إعداد متطلبات الالتحاق بمهن الأمن السيبراني، ومؤهلاته وعملياته، والإشراف عليها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مدير الموارد البشرية للأمن السيبراني من المستوى الثاني. • الأدوار الإدارية أو أدوار الموارد البشرية الأخرى.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مدير الموارد البشرية للأمن السيبراني من المستوى الرابع.

جدول ٤٣: مدير الموارد البشرية للأمن السيبراني من المستوى الثالث

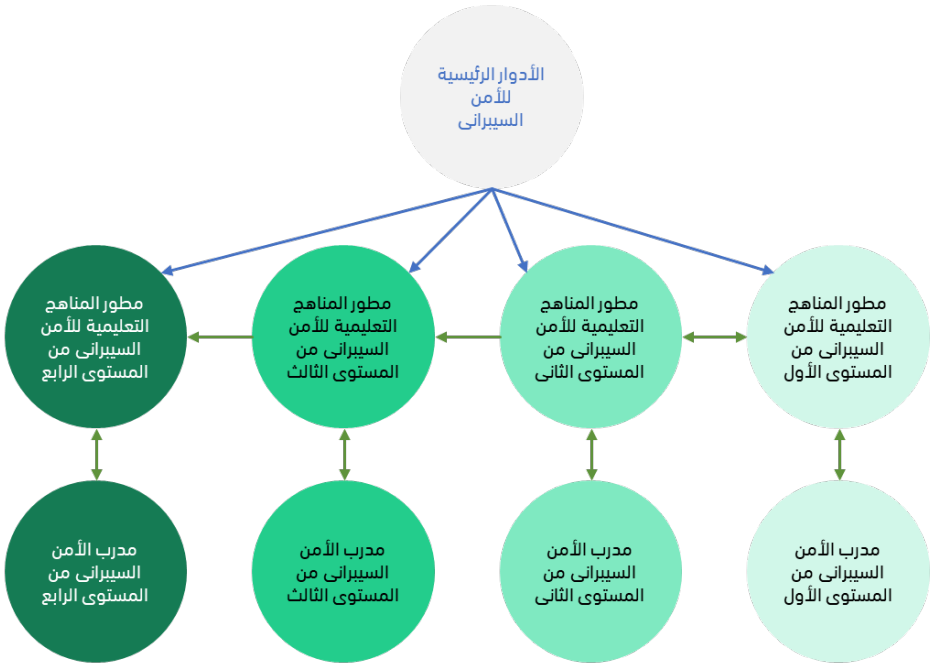
٣,٤,٣ مدير الموارد البشرية للأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: مدير الموارد البشرية للأمن السيبراني (LWD-WD-001)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يتولى إدارة وحدة، تعنى بتطوير الخطط والإستراتيجيات والإرشادات داخل المنظمة؛ لدعم تطوير مختصي الأمن السيبراني وإدارته. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال مدير الموارد البشرية للأمن السيبراني من المستوى الثالث، وضمان استكمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية ذات الصلة. تشمل المهمات تقديم التوجيهات بشأن السياسات (الخاصة بأمن المختصين) لإدارة الأمن السيبراني، وضمان إدارة وظائف الأمن السيبراني، وفقًا لسياسات الموارد البشرية للمؤسسة وتوجيهاتها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مدير الموارد البشرية للأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ٤٤: مدير الموارد البشرية للأمن السيبراني من المستوى الرابع

٠,٣ مُطوّر المناهج التعليمية للأمن السيبراني

يقوم مختصو المناهج التعليمية للأمن السيبراني بتطوير برامج التدريب ودوراته ومحتوياته، وأساليب التدريب وتقنياته، والتوعية والتعليم في شؤون الأمن السيبراني، وتخطيط البرامج وتنسيقها وتقييمها، وفقًا للاحتياجات التعليمية. يتطلب هذا الدور الحصول على شهادات، أو تدريبات في مجال التصميم التعليمي، وتطوير المناهج التعليمية، والموضوعات الأساسية للأمن السيبراني، وكذلك الحصول على التدريب، أو التوعية، أو الشهادات الخاصة بموضوعات محددة ذات صلة بمجالات تطوير المناهج الدراسية.



شكل ١٥: الخريطة الوظيفية لمُطوّر المناهج التعليمية للأمن السيبراني

١,٥,٣ مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الأول

مسمى الدور الوظيفي: مُطوّر المناهج التعليمية للأمن السيبراني (LUD-WD-002)	المستوى الوظيفي: المستوى الأول
وصف الدور الوظيفي	مساعدة الفريق في تطوير برامج التعليم والتوعية والتدريب للأمن السيبراني والمناهج ومحتوياتها وأساليب وتقنيات تقديمها، وكذلك التخطيط لها والتنسيق والتقييم، حسب الاحتياجات التعليمية. يؤدي الفرد في هذا الدور مهمات أساسية تحت إشراف مباشر، في حين أنه يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات دعم تصميم أساليب التدريب العملي وتنفيذها، وكتابة المواد التعليمية لتوفير التوجيه التفصيلي لموظفي المنظمة ووحداتها.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية. • مدرب الأمن السيبراني من المستوى الأول. • الأدوار الرئيسية للأمن السيبراني من المستوى الأول.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الثاني. • مدرب الأمن السيبراني من المستوى الأول.

جدول ٤٥: مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الأول

٢,٥,٣ مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي: مُطوّر المناهج التعليمية للأمن السيبراني (LUD-WD-002)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يقوم بتطوير برامج التدريب، والتوعية والتعليم، والتخطيط والتنسيق والتقييم، في مجال الأمن السيبراني، ومن ثم يقوم بتقييمها وتنسيقها، بالإضافة إلى الدورات والمحتوى، والأساليب، والطرق التعليمية، بناءً على الاحتياجات التعليمية. سيتولى أحد الأفراد في هذا الدور الإشراف على العمل الذي يقوم به مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الأول، وسيواصل تطوير مهاراته، من خلال التطبيق العملي. تتضمن المهمات تطوير تمارين تعلم تفاعلية وبيئة تعلم فعالة، وتطوير سياسات التدريب على الأمن السيبراني وأساليبه، أو المساعدة في وضعها.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الأول. • مدرب الأمن السيبراني من المستوى الثاني. • الأدوار الرئيسية للأمن السيبراني من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الثالث. • مدرب الأمن السيبراني من المستوى الثاني.

جدول ٤٦: مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الثاني

٣,٥,٣ مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: مُطوّر المناهج التعليمية للأمن السيبراني (LUD-WD-002)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يقوم بتطوير برامج التدريب والتوعية والتعليم في مجال الأمن السيبراني وتخطيط مناهجها، وتنسيقها وتقييمها، بالإضافة إلى الدورات، والمحتوى، والأساليب، والطرق التعليمية، بناءً على الاحتياجات التدريبية. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالعمل؛ لمراجعتها والعمل تحت إشراف مطور المناهج التعليمية للأمن السيبراني من المستوى الرابع. تشمل المهمات وضع أهداف، وغايات مناهج التدريب على الأمن السيبراني في المنظمة، وإجراء مراجعات دورية لمحتوى الدورة التدريبية، للتأكد من دقتها، واكتمالها، ومواءمتها مع التدريب.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الثاني. • مدرب الأمن السيبراني من المستوى الثالث. • الأدوار الرئيسية للأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الرابع. • مدرب الأمن السيبراني من المستوى الثالث.

جدول ٤٧: مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الثالث

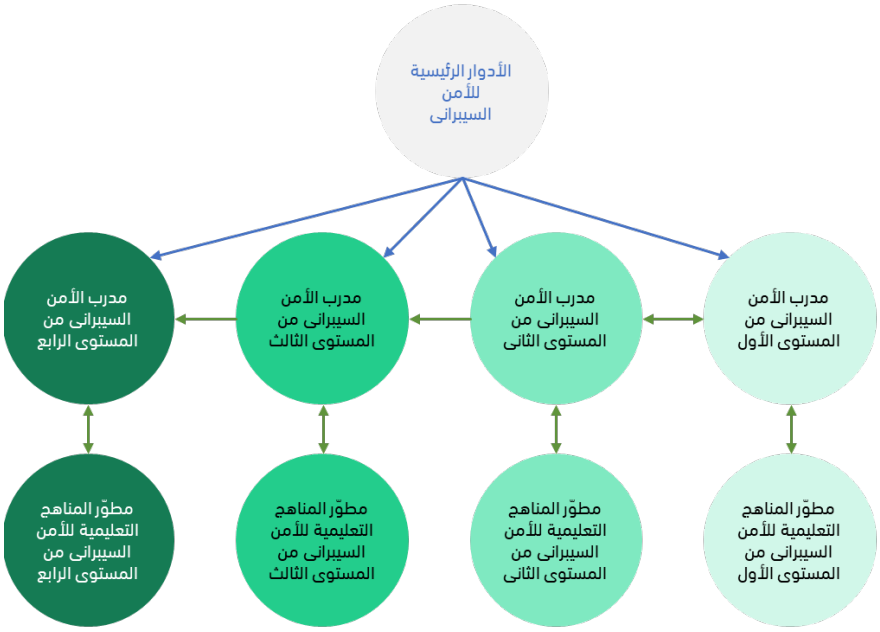
٤,٥,٣ مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: مُطوّر المناهج التعليمية للأمن السيبراني (LUD-WD-002)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يتولى إدارة وحدة، تعنى بتخطيط برامج التعليم والتوعية والتدريب للأمن السيبراني، وكذلك العمل على تطويرها، وتنسيقها، وتقييم البرامج والمناهج ومحتوياتها، وأساليبها وتقنيات تقديمها، حسب الاحتياجات التعليمية. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على الكثير من أعمال مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الثالث، وضمان استكمالها، وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. وتتضمن المهمات تحديد الأهداف الرئيسية لمناهج التدريب على الأمن السيبراني للمؤسسة، إلى جانب تقييم إستراتيجيات التدريس وأساليبه بالتعاون مع الخبراء، لضمان تحقيق أفضل نتائج في التعلم، والتطوير المؤسسي.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الثالث. • مدرب الأمن السيبراني من المستوى الرابع. • الأدوار الرئيسية للأمن السيبراني من المستوى الرابع.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مدرب الأمن السيبراني من المستوى الرابع.

جدول ٤٨: مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الرابع

٦,٣مدرب الأمن السيبراني

يقوم مدرب الأمن السيبراني بتعليم الأفراد، وتدريبهم، وتطويرهم، وتقييمهم في موضوعات الأمن السيبراني، والتوعية. يتطلب هذا الدور الحصول على شهادات، أو تدريبات تعليمية في مجال الأمن السيبراني، وأساليب التدريس، وتقييم التدريب، والمفاهيم الأساسية للأمن السيبراني، بالإضافة إلى الخبرات، أو الشهادات المتعلقة بالموضوعات التي يجري تدريسها.



شكل ١٦: الخريطة الوظيفية لمدرب الأمن السيبراني

١,٦,٣ مدرب الأمن السيبراني من المستوى الأول

مسمى الدور الوظيفي: مدرب الأمن السيبراني (LUD-WD-002)	المستوى الوظيفي: المستوى الأول
وصف الدور الوظيفي	تقديم الدعم للفريق في تعليم الأفراد، وتدريبهم، وتطوير مستوياتهم، واختبارهم في موضوعات الأمن السيبراني، والتوعية. يؤدي الفرد في هذا الدور بعض المهمات الأساسية تحت إشراف مباشر، بينما يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات تقديم الدعم في تصميم سيناريوهات التدريب العملي، وتنفيذها، والمساعدة في تطوير المناهج التدريبية، ومحتوى الدورة التدريبية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية. • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الأول. • الأدوار الرئيسية للأمن السيبراني من المستوى الأول.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مدرب الأمن السيبراني من المستوى الثاني. • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الأول.

جدول ٤٩: مدرب الأمن السيبراني من المستوى الأول

٢,٦,٣ مدرب الأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي: مدرب الأمن السيبراني (LUD-WD-003)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس، يقوم بتعليم الأفراد، وتدريبهم، وتطويرهم، واختبارهم في موضوعات الأمن السيبراني والتوعية. سيتولى الفرد في هذا الدور الإشراف على العمل الذي يقوم به مدرب الأمن السيبراني من المستوى الأول، ويواصل تطوير مهاراته، من خلال التطبيق العملي. وتشمل المهمات كتابة المواد التعليمية التي تساعد على تقديم التوجيه والمشورة للموظفين، أو وحدات المنظمة وتطوير الدورة التدريبية، والمساعدة في إعداد مهماتها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • مدرب الأمن السيبراني من المستوى الأول. • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الثاني. • الأدوار الرئيسية للأمن السيبراني من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مدرب الأمن السيبراني من المستوى الثالث. • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الثاني.

جدول ٥٠: مدرب الأمن السيبراني من المستوى الثاني

٣,٦,٣ مدرب الأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: مدرب الأمن السيبراني (LUD-WD-003)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يقوم بتعليم الأفراد، وتدريبهم، وتطويرهم، واختبارهم في موضوعات الأمن السيبراني والتوعية. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بهذا الدور، والعمل تحت إشراف مدرب الأمن السيبراني من المستوى الرابع ومراجعته، وتشمل المهمات إجراء تقييمات لمعرفة الاحتياجات التعليمية، وتحديد الشروط، وتطوير سياسات وأساليب التدريب على الأمن السيبراني، أو المساعدة في تطويرها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مدرب الأمن السيبراني من المستوى الثاني. • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الثالث. • الأدوار الرئيسية للأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مدرب الأمن السيبراني من المستوى الرابع. • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الثالث.

جدول ٥١: مدرب الأمن السيبراني من المستوى الثالث

٤,٦,٣ مدرب الأمن السيبراني من المستوى الرابع

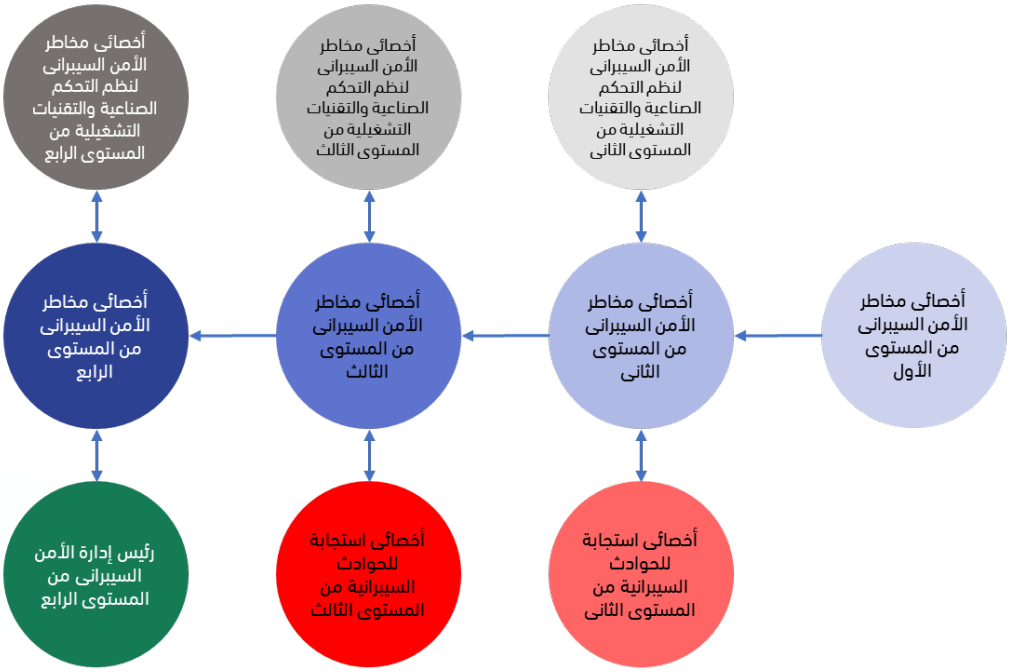
مسمى الدور الوظيفي: مدرب الأمن السيبراني (LUD-WD-003)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يتولى إدارة وحدة، تعنى بتعليم الأفراد، وتدريبهم، وتطويرهم، واختبارهم في موضوعات الأمن السيبراني والتوعية. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال مدرب الأمن السيبراني من المستوى الثالث، وضمان اكتمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية ذات الصلة. تشمل المهمات تصميم المناهج التدريبية، ومحتوى الدورات التدريبية، بناءً على متطلبات المنظمة ومختصيها، وضمان كون التدريب يلبي أهداف التدريب، أو التعليم، أو التوعية بالأمن السيبراني.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مدرب الأمن السيبراني من المستوى الثالث. • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الرابع. • الأدوار الرئيسية للأمن السيبراني من المستوى الرابع.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مُطوّر المناهج التعليمية للأمن السيبراني من المستوى الرابع.

جدول ٥٢: مدرب الأمن السيبراني من المستوى الرابع

٤ الحوكمة والمخاطر والالتزام والقوانين (GRCL)

١,٤ أخصائي مخاطر الأمن السيبراني

يقوم أخصائي مخاطر الأمن السيبراني بتحديد مخاطر الأمن السيبراني للمؤسسة وتقييمها وإدارتها لحماية أصول لمعلومات والتقنية، وفقًا لسياسات المنظمة وإجراءاتها، وكذلك وفقًا للقوانين واللوائح المعمول بها. يتطلب هذا العمل الحصول على شهادات، أو تدريب في إدارة المخاطر، وحوكمة الأمن السيبراني، والالتزام، وتقييم التهديدات.



شكل ١٧: الخريطة الوظيفية لأخصائي مخاطر الأمن السيبراني

١,١,٤ أخصائي مخاطر الأمن السيبراني من المستوى الأول

مسمى الدور الوظيفي: أخصائي مخاطر الأمن السيبراني (GRCL-GRC-001)	المستوى الوظيفي: المستوى الأول
وصف الدور الوظيفي	تقديم الدعم لفريق إدارة المخاطر أو الالتزام في تحديد مخاطر الأمن السيبراني للمؤسسة وتقييمها وإدارتها بهدف حماية أصولها المعلوماتية والتقنية بما يتسق مع السياسات والإجراءات التنظيمية والقوانين واللوائح ذات الصلة. يؤدي الفرد في هذا الدور بعض المهمات الأساسية تحت إشراف مباشر، بينما يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات إجراء تقييمات لمخاطر الأمن السيبراني والتعاون مع الآخرين لتنفيذ برنامج إدارة مخاطر الأمن السيبراني وتحديثه.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي مخاطر الأمن السيبراني من المستوى الثاني.

جدول ٥٣: أخصائي مخاطر الأمن السيبراني من المستوى الأول

٢,١,٤ أخصائي مخاطر الأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي: أخصائي مخاطر الأمن السيبراني (GRCL-GRC-001)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يتولى تحديد مخاطر الأمن السيبراني للمؤسسة وتقييمها وإدارتها؛ بهدف حماية أصولها المعلوماتية والتقنية، وفقًا لسياسات المنظمة وإجراءاتها، وكذلك القوانين واللوائح ذات العلاقة. سيتولى الفرد في هذا الدور الإشراف على العمل الذي يقوم به أخصائي مخاطر الأمن السيبراني من المستوى الأول، ويواصل تطوير مهاراته، من خلال التطبيق العملي. تشمل المهمات إجراء تحليل المخاطر عند تنفيذ تغييرات جوهرية على التطبيقات، أو النُظم، بالإضافة إلى دعم إطار إدارة المخاطر، من خلال تقديم المدخلات اللازمة وإثراء الوثائق المرتبطة به.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • أخصائي مخاطر الأمن السيبراني من المستوى الأول. • أخصائي استجابة للحوادث السيبرانية من المستوى الثاني. • أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي مخاطر الأمن السيبراني من المستوى الثالث. • أخصائي استجابة للحوادث السيبرانية من المستوى الثاني. • أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني.

جدول ٥٤: أخصائي مخاطر الأمن السيبراني من المستوى الثاني

٣,١,٤ أخصائي مخاطر الأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: أخصائي مخاطر الأمن السيبراني (GRCL-GRC-001)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول، يتولى تحديد مخاطر الأمن السيبراني للمؤسسة، وتقييمها، وإدارتها؛ لحماية أصولها المعلوماتية والتقنية، وفقًا لسياسات المنظمة وإجراءاتها، وكذلك القوانين واللوائح ذات العلاقة. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بهذا العمل، تحت إشراف أخصائي مخاطر الأمن السيبراني ومراجعته من المستوى الرابع. وتشمل المهمات العمل مع الآخرين لتنفيذ برنامج إدارة مخاطر الأمن السيبراني وتحديثه، وتكليف الأفراد بمهمات مرتبطة بتنفيذ إطار إدارة المخاطر.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي مخاطر الأمن السيبراني من المستوى الثاني. • أخصائي استجابة للحوادث السيبرانية من المستوى الثالث. • أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي مخاطر الأمن السيبراني من المستوى الرابع. • أخصائي استجابة للحوادث السيبرانية من المستوى الثالث. • أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث.

جدول ٥٥: أخصائي مخاطر الأمن السيبراني من المستوى الثالث

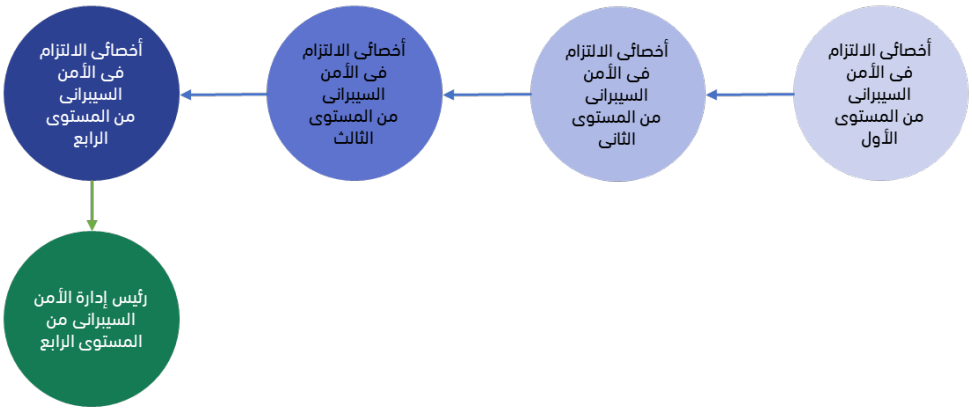
٤,١,٤ أخصائي مخاطر الأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: أخصائي مخاطر الأمن السيبراني (GRCL-GRC-001)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً لتحديد مخاطر الأمن السيبراني للمؤسسة، وتقييمها، وإدارتها؛ لحماية أصولها المعلوماتية والتقنية، وفقًا لسياسات المنظمة وإجراءاتها، وكذلك القوانين واللوائح ذات الصلة. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال أخصائي مخاطر الأمن السيبراني من المستوى الثالث، وضمان اكتمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية ذات الصلة. تشمل المهمات نقل مخاطر الأمن السيبراني، ووضعه العام إلى الإدارة العليا بوضوح وفعالية، والتأكد من تحديد هذه المخاطر، ومعالجتها، وفقًا لإطار حوكمة المخاطر في المنظمة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي مخاطر الأمن السيبراني من المستوى الثالث. • أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • رئيس إدارة الأمن السيبراني من المستوى الرابع. • أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع.

جدول ٥٦: أخصائي مخاطر الأمن السيبراني من المستوى الرابع

٢,٤ أخصائي الالتزام في الأمن السيبراني

يضمن أخصائي الالتزام للأمن السيبراني، التزام برنامج الأمن السيبراني في المنظمة بالمتطلبات، والسياسات، والمعايير المعمول بها. يتطلب هذا العمل الحصول على شهادات، أو تدريب في إدارة الالتزام، وتدقيق الأمن السيبراني، والأطر التنظيمية، وتقييم السياسات.



شكل ١٨: الخريطة الوظيفية لأخصائي الالتزام في الأمن السيبراني

١,٢,٤ أخصائي الالتزام في الأمن السيبراني من المستوى الأول

مسمى الدور الوظيفي: أخصائي الالتزام في الأمن السيبراني (GRCL-GRC-003)	المستوى الوظيفي: المستوى الأول
وصف الدور الوظيفي	مساندة فريق المخاطر أو الالتزام في ضمان توافق برنامج الأمن السيبراني للمؤسسة، مع المتطلبات، والسياسات، والمعايير ذات الصلة. يقوم الفرد في هذا الدور بتنفيذ بعض المهمات الأساسية تحت إشراف مباشر، مع الاستمرار في التعرف على متطلبات العمل. تشمل المهمات تقديم الدعم لأنشطة الالتزام على النحو المطلوب.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي الالتزام في الأمن السيبراني من المستوى الثاني.

جدول ٥٧: أخصائي الالتزام في الأمن السيبراني من المستوى الأول

٢,٢,٤ أخصائي الالتزام في الأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي: أخصائي الالتزام في الأمن السيبراني (GRCL-GRC-003)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس، يعمل على ضمان التزام برنامج الأمن السيبراني للمؤسسة بالمتطلبات والسياسات والمعايير المعمول بها. سيتولى الفرد في هذا الدور مسؤولية الإشراف الذي يقوم به أخصائي الالتزام في الأمن السيبراني من المستوى الأول ويواصل تطوير مهاراته من خلال التطبيق العملي، تشمل المهمات تقييم جوانب الأمن السيبراني للعقود لضمان التزامها بالمتطلبات المالية والتعاقدية والقانونية والتنظيمية، وضمان تقييم أي منتجات جرى تنفيذها لإدارة مخاطر الأمن السيبراني بشكل فعال، وتصاريح استخدامها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • أخصائي الالتزام في الأمن السيبراني من المستوى الأول.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي الالتزام في الأمن السيبراني من المستوى الثالث.

جدول ٥٨: أخصائي الالتزام في الأمن السيبراني من المستوى الثاني

٣,٢,٤ أخصائي الالتزام في الأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: أخصائي الالتزام في الأمن السيبراني (GRCL-GRC-003)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول، يعمل على ضمان التزام برنامج الأمن السيبراني للمؤسسة بالمتطلبات والسياسات والمعايير المعمول بها. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالعمل تحت إشراف أخصائي الالتزام بالأمن السيبراني من المستوى الرابع، ومراجعته تشمل المهمات مراقبة وتقييم امتثال النُظم لمعايير الأمن السيبراني وتقييمها، والمرونة التشغيلية والموثوقية، بالإضافة إلى إجراء تقييم تقني دقيق للتطبيقات والنُظم والشبكات، وتوثيق مدى التزامها بالمتطلبات الأمنية المتفق عليها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي الالتزام في الأمن السيبراني من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي الالتزام في الأمن السيبراني من المستوى الرابع.

جدول ٥٩: أخصائي الالتزام في الأمن السيبراني من المستوى الثالث

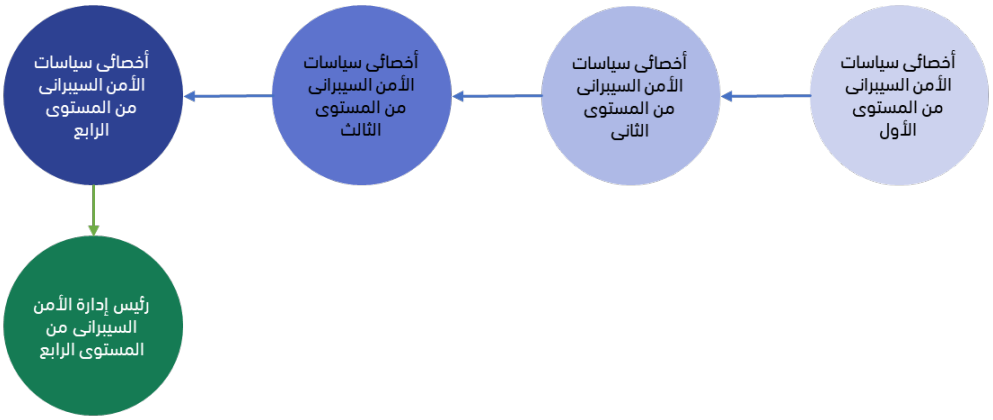
٤,٢,٤ أخصائي الالتزام في الأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: أخصائي سياسات الأمن السيبراني (GRCL-GRC-003)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً، تعنى بضمان التزام برامج الأمن السيبراني الخاصة بالمنظمة بالمتطلبات والسياسات والمعايير المعمول بها. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على الكثير من أعمال أخصائي الالتزام في الأمن السيبراني من المستوى الثالث، وضمان تنفيذها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تشمل المهمات تطوير عمليات الالتزام وإجراءات التدقيق على خدمات الأمن السيبراني المقدمة من أطراف أخرى والتعاون مع الهيئات التنظيمية ذات الصلة والجهات القانونية الأخرى في أي مراجعات أو تحقيقات تتعلق بالالتزام.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي الالتزام في الأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • رئيس إدارة الأمن السيبراني من المستوى الرابع.

جدول ٦٠: أخصائي الالتزام في الأمن السيبراني من المستوى الرابع

٣,٤ أخصائي سياسات الأمن السيبراني

يقوم أخصائي سياسات الأمن السيبراني بتطوير سياسات الأمن السيبراني وتحديثها؛ لدعم متطلبات الأمن السيبراني بالمنظمة ومواءمتها. يتطلب هذا العمل الحصول على شهادات، أو تدريب في مجال تطوير سياسات الأمن السيبراني، والالتزام بالنُظم، وأطر الحوكمة، والمواءمة الإستراتيجية لأهداف الأمن السيبراني.



شكل ١٩: الخريطة الوظيفية لأخصائي سياسات الأمن السيبراني

١,٣,٤ أخصائي سياسات الأمن السيبراني من المستوى الأول

مسمى الدور الوظيفي: أخصائي سياسات الأمن السيبراني (GRCL-GRC-003)	المستوى الوظيفي: المستوى الأول
وصف الدور الوظيفي	تقديم الدعم لفريق المخاطر، أو الالتزام في تطوير سياسات الأمن السيبراني، وتحديثها، والحفاظ عليها؛ لدعم متطلبات الأمن السيبراني للمؤسسة والمواءمة بشأنها. يؤدي الفرد في هذا الدور بعض المهمات الأساسية تحت إشراف مباشر، بينما يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات مراجعة عمليات التدقيق على برامج الأمن السيبراني ومشاريعه أو تنفيذها أو المشاركة فيها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي سياسات الأمن السيبراني من المستوى الثاني.

جدول ٦١: أخصائي سياسات الأمن السيبراني من المستوى الأول

٢,٣,٤ أخصائي سياسات الأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي: أخصائي سياسات الأمن السيبراني (GRCL-GRC-003)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يقوم بتطوير سياسات الأمن السيبراني، وتحديثها والحفاظ عليها؛ لدعم متطلبات الأمن السيبراني للمؤسسة، ومواءمتها معها. سوف يتولى الفرد في هذا الدور الإشراف على العمل الذي يقوم به أخصائي سياسات الأمن السيبراني من المستوى الأول ويواصل تطوير مهاراته من خلال التطبيق العملي. وتتضمن المهمات تطوير سياسات الأمن السيبراني، والوثائق ذات الصلة بها والمساعدة في مراجعة السياسات الحالية، والمقترحة، والوثائق ذات الصلة مع أصحاب المصلحة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • أخصائي سياسات الأمن السيبراني من المستوى الأول.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي سياسات الأمن السيبراني من المستوى الثالث.

جدول ٦٢: أخصائي سياسات الأمن السيبراني من المستوى الثاني

٣,٣,٤ أخصائي سياسات الأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: أخصائي سياسات الأمن السيبراني (GRCL-GRC-003)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يقوم بتطوير سياسات الأمن السيبراني وتحديثها والحفاظ عليها لدعم متطلبات الأمن السيبراني للمؤسسة ومواءمتها معها. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بهذا الدور، والعمل تحت إشراف أخصائي سياسات الأمن السيبراني من المستوى الرابع ومراجعته، تشمل المهمات تطوير سياسة الأمن السيبراني الخاصة بالمنظمة، ونشرها ومراقبة مدى فاعلية تنفيذ سياسات الأمن السيبراني ومبادئه وممارساته في تطبيق خدمات التخطيط والخدمات الإدارية على أرض الواقع.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي سياسات الأمن السيبراني من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي سياسات الأمن السيبراني من المستوى الرابع.

جدول ٦٣: أخصائي سياسات الأمن السيبراني من المستوى الثالث

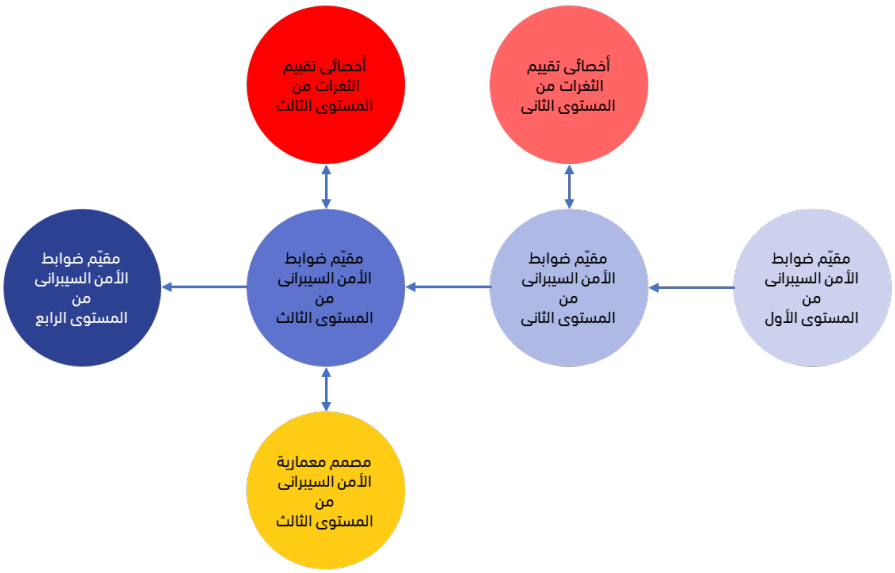
٤,٣,٤ أخصائي سياسات الأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: أخصائي سياسات الأمن السيبراني (GRCL-GRC-003)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً، تعنى بتطوير سياسات الأمن السيبراني، وتحديثها والحفاظ عليها؛ لدعم متطلبات الأمن السيبراني للمؤسسة والمواءمة معها. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال أخصائي سياسة الأمن السيبراني من المستوى الثالث، وضمان اكتمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية ذات الصلة. وتشمل المهمات ضمان التزام السياسات والعمليات الصادرة عن إدارة كوادر الأمن السيبراني للمتطلبات القانونية والتنظيمية وتعزيز الوعي بالسياسات والإستراتيجية السيبرانية، حسب الاقتضاء على مستوى إدارة المنظمة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي سياسات الأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • رئيس إدارة الأمن السيبراني من المستوى الرابع.

جدول ٦٤: أخصائي سياسات الأمن السيبراني من المستوى الرابع

٤,٤ مُقيّم ضوابط الأمن السيبراني

يقوم مُقيّم ضوابط الأمن السيبراني بتحليل ضوابط الأمن السيبراني وتقييمها؛ لتحديد مدى فاعليتها. يتطلب هذا العمل الحصول على شهادات، أو تدريب في تقييم ضوابط الأمن السيبراني، وتدقيق الأمن السيبراني، وتحليل المخاطر، وتقييم تدابير الأمن السيبراني.



شكل٢٠ : الخريطة الوظيفية لمُقيّم ضوابط الأمن السيبراني

١,٤,٤ مُقيّم ضوابط الأمن السيبراني من المستوى الأول

مسمى الدور الوظيفي: مُقيّم ضوابط الأمن السيبراني (GRCL-GRC-004)	المستوى الوظيفي: المستوى الأول
وصف الدور الوظيفي	مساعدة فريق التقييم في تحليل ضوابط الأمن السيبراني، وتقييم فاعليتها. يؤدي الفرد في هذا الدور بعض المهمات الأساسية تحت إشراف مباشر، بينما يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات تقييم فاعلية ضوابط الأمن السيبراني، وتقييم عملية إدارة الإعدادات.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مُقيّم ضوابط الأمن السيبراني من المستوى الثاني.

جدول ٦٥: مُقيّم ضوابط الأمن السيبراني من المستوى الأول

٢,٤,٤ مُقيّم ضوابط الأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي: مُقيّم ضوابط الأمن السيبراني (GRCL-GRC-004)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يقوم بتحليل ضوابط الأمن السيبراني، وتقييم فاعليتها. سيتولى الفرد في هذا الدور الإشراف على العمل الذي يقوم به مُقيّم ضوابط الأمن السيبراني من المستوى الأول، ويواصل تطوير مهاراته من خلال التطبيق العملي. تتضمن المهمات إجراء تقييمات دورية للأمن السيبراني، ورصد الثغرات في المعمارية الأمنية، وتقديم توصيات؛ لتعزيز إستراتيجيات الحد من المخاطر.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • مُقيّم ضوابط الأمن السيبراني من المستوى الأول. • أخصائي تقييم الثغرات من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مُقيّم ضوابط الأمن السيبراني من المستوى الثالث. • أخصائي تقييم الثغرات من المستوى الثاني.

جدول ٦٦: مُقيّم ضوابط الأمن السيبراني من المستوى الثاني

٣,٤,٤ مُقيّم ضوابط الأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: مُقيّم ضوابط الأمن السيبراني (GRCL-GRC-004)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول، يقوم بتحليل ضوابط الأمن السيبراني، وتقييم فاعليتها. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالدور الوظيفي، والعمل تحت إشراف مُقيّم ضوابط الأمن السيبراني ومراجعته من المستوى الرابع. تتضمن المهمات تخطيط مراجعات تراخيص الأمن السيبراني وتنفيذها، وتطوير حالات الضمان؛ لضمان الالتزام أثناء تثبيت النُظم والشبكات، إلى جانب مراجعة سجلات المخاطر؛ للتحقق من أن مستويات المخاطر تظل ضمن الحدود المقبولة لكل تطبيق، أو نظام، أو شبكة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مُقيّم ضوابط الأمن السيبراني من المستوى الثاني. • أخصائي تقييم الثغرات من المستوى الثالث. • مصمم معمارية الأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مُقيّم ضوابط الأمن السيبراني من المستوى الرابع. • مصمم معمارية الأمن السيبراني من المستوى الثالث. • أخصائي تقييم الثغرات من المستوى الثالث.

جدول ٦٧: مُقيّم ضوابط الأمن السيبراني من المستوى الثالث

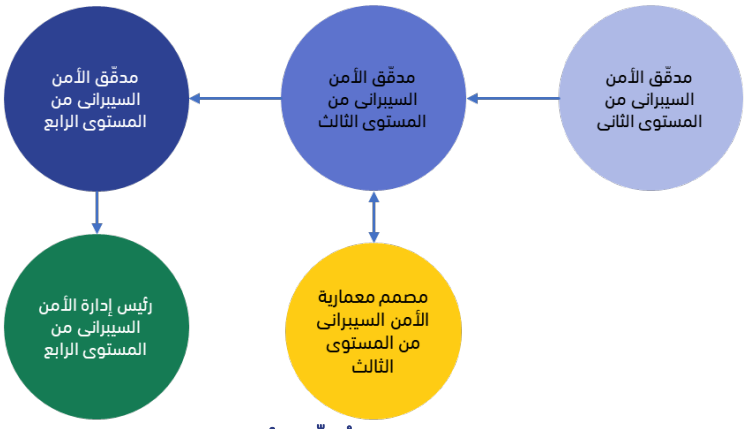
٤,٤,٤ مُقيّم ضوابط الأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: مُقيّم ضوابط الأمن السيبراني (GRCL-GRC-004)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً، تعنى بتحليل ضوابط الأمن السيبراني، وتقييم فاعليتها. يتحمل الفرد في هذا الدور مسؤولية الإشراف على معظم أعمال مُقيّم ضوابط الأمن السيبراني من المستوى الثالث، وضمان اكتمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية ذات الصلة. تشمل المهمات ضمان إدارة مخاطر الأمن السيبراني بفاعلية، ضمن إطار حوكمة المخاطر، والتأكد من تضمين متطلبات الأمن السيبراني في قرارات الاندماج، والاستحواذ، والتعاقد مع مزودي الخدمات الخارجيين، وأي أنشطة أخرى مع أطراف خارجية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مُقيّم ضوابط الأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ٦٨: مُقيّم ضوابط الأمن السيبراني من المستوى الرابع

٥,٤ مُدقّق الأمن السيبراني

يقوم مُدقّق الأمن السيبراني بمهمة تخطيط عمليات التدقيق الأمني السيبراني، وتنفيذها وإدارتها؛ لضمان التزام المنظمة بالمتطلبات التنظيمية، والسياسات، والمعايير، والضوابط الأمنية. يتطلب هذا العمل الحصول على شهادات، أو تدريب في مجال تدقيق الأمن السيبراني، وأطر الالتزام، وتحليل المخاطر، وتقييم الضوابط الأمنية. تشمل المسؤوليات التدقيق في إعدادات النُظم، وضمان توافقها مع المعايير والسياسات الأمنية، وتقديم تقارير تحليلية، تتضمن توصيات واضحة؛ لتعزيز الالتزام والأمان.



شكل ٢١: الخريطة الوظيفية لمُدقّق الأمن السيبراني

١,٥,٤ مُدقّق الأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي: مُدقّق الأمن السيبراني (GRCL-GRC-005)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يتولى تصميم عمليات التدقيق الخاصة بالأمن السيبراني وتنفيذها وإدارتها؛ بهدف تقييم مدى التزام المنظمة بالمتطلبات، والسياسات، والمعايير، والضوابط المعمول بها. وكذلك إعداد تقارير التدقيق وتقديمها إلى الأطراف المصرح لها. يقوم الفرد في هذا الدور بتطوير مهاراته من خلال التطبيق العملي. تتضمن المهمات تنفيذ تحليل للمخاطر، عند إجراء أي تغيير رئيسي في التطبيقات أو النُظم، بالإضافة إلى تتبع نتائج التدقيق والتوصيات؛ لضمان تنفيذ إجراءات فعالة، للحد من المخاطر المتوقعة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مُدقّق الأمن السيبراني من المستوى الثالث.

جدول ٦٩: مُدقّق الأمن السيبراني من المستوى الثاني

٢,٥,٤ مُدقّق الأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: مُدقّق الأمن السيبراني (GRCL-GRC-005)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول، يتولى تصميم عمليات التدقيق الخاصة بالأمن السيبراني، وتنفيذها وإدارتها؛ بهدف تقييم مدى التزام المنظمة بالمتطلبات، والسياسات، والمعايير، والضوابط المعمول بها، وإعداد تقارير التدقيق وتقديمها إلى الأطراف المصرح لها. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بهذا الدور، والعمل تحت إشراف مُدقّق الأمن السيبراني ومراجعته من المستوى الرابع. تشمل المسؤوليات إعداد تقارير شاملة عن تدقيق الأمن السيبراني، تتضمن تحليلًا للنتائج التقنية والإجرائية، مع اقتراح حلول فعالة، بالإضافة إلى ضمان الاحتفاظ بسجل تدقيق، يوثق جميع التدابير الأمنية المعتمدة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مُدقّق الأمن السيبراني من المستوى الثاني. • مصمم معمارية الأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مُدقّق الأمن السيبراني من المستوى الرابع. • مصمم معمارية الأمن السيبراني من المستوى الثالث.

جدول ٧٠: مُدقّق الأمن السيبراني من المستوى الثالث

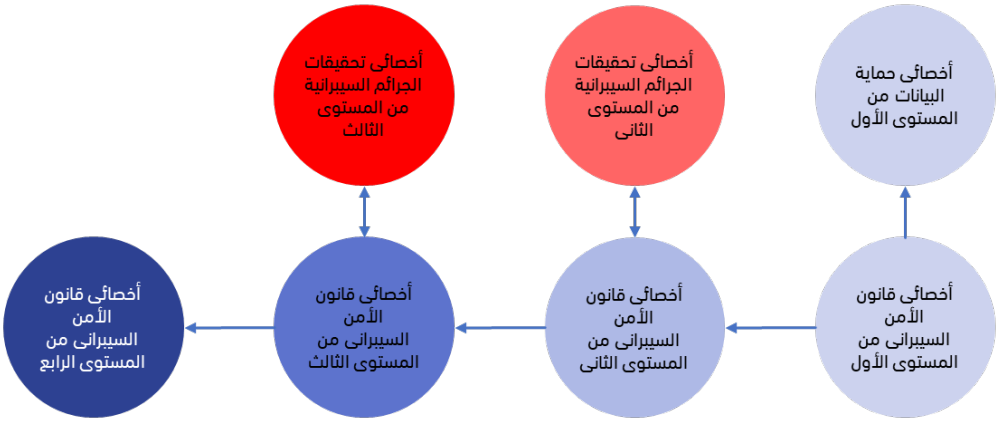
٣,٥,٤ مُدقّق الأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: مُدقّق الأمن السيبراني (GRCL-GRC-005)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً، تعنى بتصميم عمليات تدقيق الأمن السيبراني، وتنفيذها، وإدارتها؛ لتقييم مدى التزام المنظمة بالمتطلبات، والسياسات، والمعايير، والضوابط المعمول بها، وإعداد تقارير التدقيق، وتقديمها إلى الأطراف المصرح لها. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال مُدقّق الأمن السيبراني من المستوى الثالث، وضمان اكتمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية ذات الصلة. تشمل المهمات الإبقاء على معرفة محدثة بسياسات الالتزام ولوائحه المتعلقة بالدفاع السيبراني، مع تصميم عمليات تدقيق دقيقة، تضمن التزام الخدمات المقدمة من قبل مزودي الطرف الثالث للمعايير الأمنية المطلوبة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مُدقّق الأمن السيبراني من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • رئيس إدارة الأمن السيبراني من المستوى الرابع.

جدول ٧١: مُدقّق الأمن السيبراني من المستوى الرابع

٦,٤ أخصائي قانون الأمن السيبراني

يقدم أخصائي قانون الأمن السيبراني الخدمات القانونية المتعلقة بقوانين الأمن السيبراني وأنظمته. يتطلب هذا العمل الحصول على شهادات، أو تدريب في قوانين الأمن السيبراني وأنظمته، ولوائح الخصوصية، وتدقيق الأمن السيبراني، وأطر الالتزام، والجوانب القانونية المتعلقة بتطوير سياسات الأمن السيبراني.



شكل ٢٢: الخريطة الوظيفية لأخصائي قانون الأمن السيبراني

١,٦,٤ أخصائي قانون الأمن السيبراني من المستوى الأول

مسمى الدور الوظيفي: أخصائي قانون الأمن السيبراني (GRCL-LDP- 001)	المستوى الوظيفي: المستوى الأول
وصف الدور الوظيفي	دعم المنظمة، من خلال تقديم الخدمات القانونية في المواضيع المتعلقة بالقوانين، واللوائح السيبرانية. يؤدي الفرد في هذا الدور بعض المهمات الأساسية، تحت إشراف مباشر، بينما يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات اكتساب المعرفة العملية بالقضايا الدستورية التي تنشأ في القوانين، واللوائح، والسياسات، والاتفاقيات، والمعايير، والإجراءات ذات الصلة، والحفاظ عليها، والمساعدة في تنفيذ القوانين، واللوائح، والأوامر التنفيذية الجديدة، أو المحدثة، من حيث صلتها بسياسات الأمن السيبراني، وغيرها من الوثائق.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي قانون الأمن السيبراني من المستوى الثاني. • أخصائي حماية البيانات من المستوى الأول.

جدول ٧٢: أخصائي قانون الأمن السيبراني من المستوى الأول

٢,٦,٤ أخصائي قانون الأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي: أخصائي قانون الأمن السيبراني (GRCL-LDP- 001)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس، يقوم بتقديم الخدمات القانونية في المواضيع المتعلقة بالقوانين، واللوائح الإلكترونية. سيتولى أحد الأفراد في هذا المنصب الإشراف على العمل الذي يقوم به أخصائي قانون الأمن السيبراني في المستوى الأول مع مواصلة تطوير مهاراته من خلال التطبيق العملي. تشمل المهمات تفسير القوانين أو اللوائح أو السياسات أو المعايير أو الإجراءات وتطبيقها حسب الضرورة، والتوعية بقوانين ولوائح حماية البيانات، ومعايير الترخيص المعمول بها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • أخصائي قانون الأمن السيبراني من المستوى الأول. • أخصائي تحقيقات الجرائم السيبرانية من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي قانون الأمن السيبراني من المستوى الثالث. • أخصائي تحقيقات الجرائم السيبرانية من المستوى الثاني.

جدول ٧٣: أخصائي قانون الأمن السيبراني من المستوى الثاني

٣,٦,٤ أخصائي قانون الأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: أخصائي قانون الأمن السيبراني (GRCL-LDP- 001)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول في تقديم الخدمات القانونية في الموضوعات المتعلقة بالقوانين، ولوائح الأمن السيبراني. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالدور الوظيفي، والعمل تحت إشراف أخصائي قانون الأمن السيبراني في المستوى الرابع ومراجعته. تشمل المهمات تحليل العقود من منظور الأمن السيبراني؛ لضمان الالتزام بالمعايير المالية والقانونية والتنظيمية، بالإضافة إلى تقييم الوضع الأمني السيبراني للمؤسسة وتقديمه بوضوح، خلال عمليات المراجعة، والتدقيق القانونية، والتنظيمية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي قانون الأمن السيبراني من المستوى الثاني. • أخصائي تحقيقات الجرائم السيبرانية من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي قانون الأمن السيبراني من المستوى الرابع. • أخصائي تحقيقات الجرائم السيبرانية من المستوى الثالث.

جدول ٧٤: أخصائي قانون الأمن السيبراني من المستوى الثالث

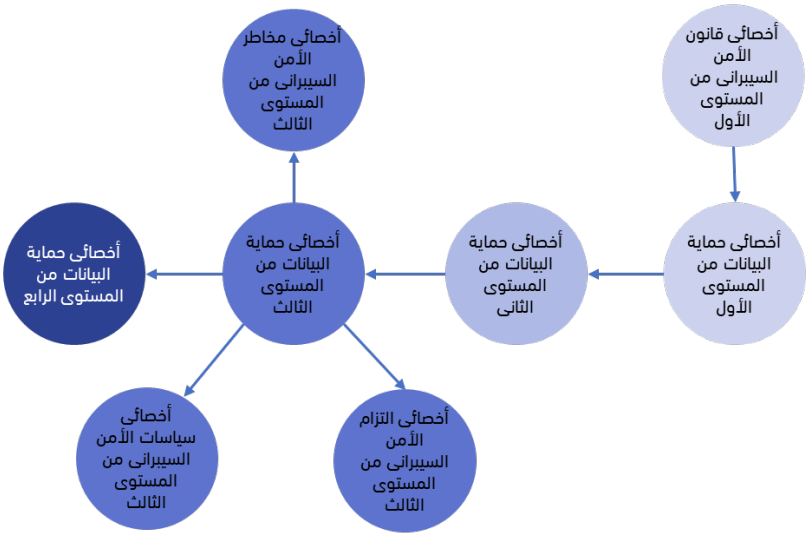
٤,٦,٤ أخصائي قانون الأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: أخصائي قانون الأمن السيبراني (GRCL-LDP- 001)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً، تعنى بتقديم الخدمات القانونية في الموضوعات المتعلقة بالقوانين، واللوائح الخاصة بالأمن السيبراني. يتحمل الفرد في هذا الدور مسؤولية الإشراف على معظم أعمال أخصائي قانون الأمن السيبراني من المستوى الثالث، وضمان اكتمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية ذات الصلة. تتضمن الأعمال تقديم المشورة المتخصصة في الأمن السيبراني؛ لدعم صياغة المرافعات القانونية، بما يضمن تحديد الانتهاكات المحتملة للقوانين، أو اللوائح، أو السياسات/التوجيهات بدقة. كما تشمل تقديم التوجيهات اللازمة فيما يخص الأمن السيبراني، عند إعداد المستندات القانونية، وغيرها من الوثائق ذات الصلة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي قانون الأمن السيبراني من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ٧٥: أخصائي قانون الأمن السيبراني من المستوى الرابع

٧,٤ أخصائي حماية البيانات

يدرس أخصائي حماية البيانات خطط البيانات الشخصية، والقوانين، واللوائح المتعلقة بحماية البيانات، ويحلل مخاطر حماية البيانات، ويقوم بتطوير برنامج الالتزام، والإشراف على تنفيذه؛ لحماية البيانات، والسياسات الداخلية للمؤسسة، يتطلب هذا العمل الحصول على شهادات، أو التدريب على لوائح حماية البيانات، وأطر الالتزام، وإستراتيجيات حماية البيانات الشخصية، كما يقدم دعمه في استجابة المنظمة لحوادث حماية البيانات.



شكل ٢٣: الخريطة الوظيفية لأخصائي حماية البيانات

١,٧,٤ أخصائي حماية البيانات من المستوى الأول

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي حماية البيانات (GRCL-LDP- 002)	المستوى الأول
وصف الدور الوظيفي	مساعدة فرق الحوكمة، والمخاطر، والالتزام، والشؤون القانونية، من خلال دراسة نظم البيانات الشخصية، وقوانين الخصوصية المعمول بها ولوائحها، وتحليل المخاطر التي تتعلق بحماية البيانات. كما يطور آليات الامتثال لحماية البيانات، ويشرف على تنفيذها داخل المنظمة، إلى جانب صياغة السياسات الداخلية ذات العلاقة، كما يسهم في إدارة استجابة المنظمة للحوادث الأمنية المتعلقة بحماية البيانات. يؤدي الفرد في هذا الدور بعض المهمات الأساسية، تحت إشراف مباشر، بينما يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات إجراء تقييمات لمخاطر حماية البيانات، وضمان حماية المعلومات الشخصية بشكل مناسب، وضمان تقديم التدريب، وأنشطة التوعية على أساس منتظم.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية. • أخصائي قانون الأمن السيبراني من المستوى الأول.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي حماية البيانات من المستوى الثاني.

جدول ٧٦: أخصائي حماية البيانات من المستوى الأول

٢,٧,٤ أخصائي حماية البيانات من المستوى الثاني

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي حماية البيانات (GRCL-LDP- 002)	المستوى الثاني
وصف الدور الوظيفي	ممارس في تحليل مخططات البيانات الشخصية، ودراسة القوانين واللوائح المنظمة لحماية البيانات، وتقييم المخاطر المرتبطة بها، كما يطور آليات الامتثال؛ لحماية البيانات، ويشرف على تنفيذها داخل المنظمة، إلى جانب صياغة السياسات الداخلية ذات العلاقة، كما يسهم في إدارة استجابة المنظمة للحوادث الأمنية المتعلقة بحماية البيانات. سيتولى الفرد في هذا الدور الإشراف على العمل الذي يقوم به أخصائي حماية البيانات من المستوى الأول، ويواصل تطوير مهاراته، من خلال التطبيق العملي، وتشمل المهمات العمل مع فرق العمل، والإدارة العليا؛ لضمان الوعي بأفضل الممارسات المتعلقة بحماية البيانات، وتطوير إجراءات الإبلاغ الذاتي عن أي دليل على انتهاكات حماية البيانات، ومن ثم توثيقها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • أخصائي حماية البيانات من المستوى الأول.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي حماية البيانات من المستوى الثالث.

جدول ٧٧: أخصائي حماية البيانات من المستوى الثاني

٣,٧,٤ أخصائي حماية البيانات من المستوى الثالث

مسمى الدور الوظيفي: أخصائي حماية البيانات (GRCL-LDP- 002)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول في تحليل مخططات البيانات الشخصية، ودراسة القوانين واللوائح المنظمة لحماية البيانات، وتقييم المخاطر المرتبطة بها، كما يطور آليات الامتثال لحماية البيانات ويشرف على تنفيذها داخل المنظمة، إلى جانب صياغة السياسات الداخلية ذات العلاقة، كما يسهم في إدارة استجابة المنظمة للحوادث الأمنية المتعلقة بحماية البيانات. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالدور الوظيفي، والعمل تحت إشراف ومراجعة أخصائي حماية البيانات من المستوى الرابع، وتشمل المهمات العمل مع فرق الشؤون القانونية، والموارد البشرية لوضع العقوبات المناسبة، لعدم الالتزام بسياسات حماية البيانات الخاصة بالمنظمة وإجراءاتها، وإنشاء إطار لإدارة المخاطر، والالتزام لحماية البيانات، والحفاظ عليه.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي حماية البيانات من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي حماية البيانات من المستوى الرابع. • أخصائي مخاطر الأمن السيبراني من المستوى الثالث. • أخصائي التزام الأمن السيبراني من المستوى الثالث. • أخصائي سياسات الأمن السيبراني من المستوى الثالث.

جدول ٧٨: أخصائي حماية البيانات من المستوى الثالث

٤,٧,٤ أخصائي حماية البيانات من المستوى الرابع

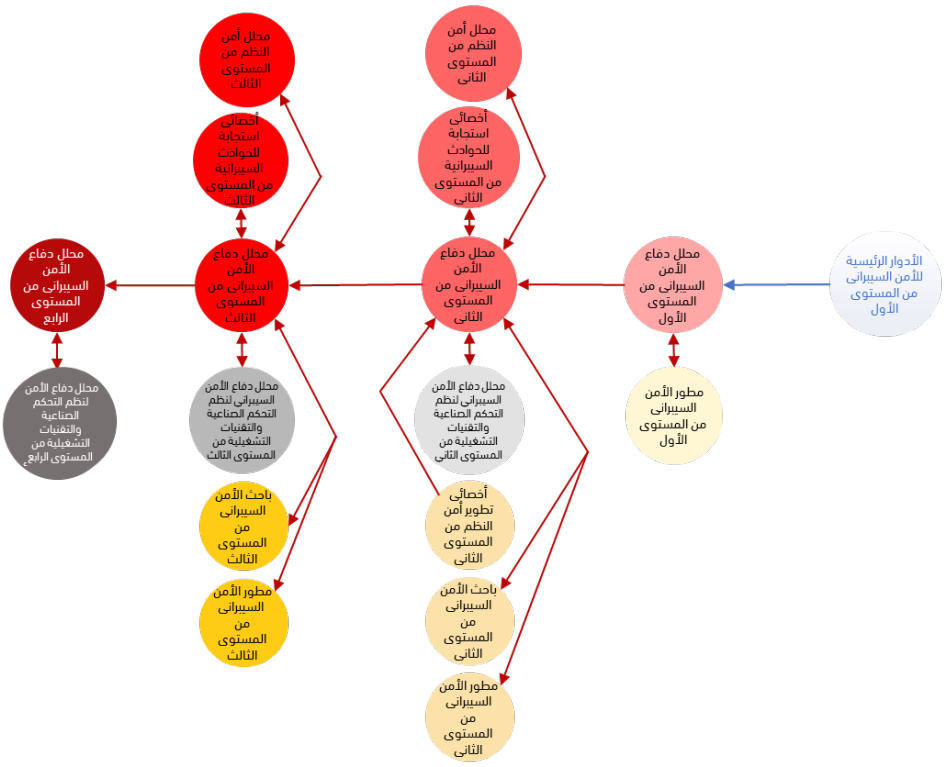
مسمى الدور الوظيفي: أخصائي حماية البيانات (GRCL-LDP- 002)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير مسؤول عن إدارة وحدة متخصصة في تحليل مخططات البيانات الشخصية، ودراسة القوانين واللوائح المنظمة لحماية البيانات، وتقييم المخاطر المرتبطة بها، كما يطور آليات الامتثال لحماية البيانات، ويشرف على تنفيذها داخل المنظمة، إلى جانب صياغة السياسات الداخلية ذات العلاقة، كما يسهم في إدارة استجابة المنظمة للحوادث الأمنية المتعلقة بحماية البيانات. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال أخصائي حماية البيانات من المستوى الثالث، وضمان استكمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية ذات الصلة، وتشمل المهمات توفير القيادة لبرنامج حماية البيانات في المنظمة، وتوجيه أخصائي حماية البيانات، والإشراف عليهم، وتنسيق برامج حماية البيانات مع الإدارة العليا؛ لضمان الاتساق على مستوى المنظمة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي حماية البيانات من المستوى الثالث.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ٧٩: أخصائي حماية البيانات من المستوى لرابع

٥ الحماية والدفاع (PD)

١,٥ محلل دفاع الأمن السيبراني

يستخدم محلل الدفاع عن الأمن السيبراني، البيانات من أدوات الدفاع السيبراني؛ لتحليل الأحداث داخل مؤسسته، بهدف الكشف عن التهديدات السيبرانية والحد منها. يتطلب هذا العمل الحصول على شهادات، أو تدريب في مجال الدفاع عن الشبكات، والكشف عن التهديدات، وتحليل الحوادث، وأدوات مراقبة الأمن السيبراني.



شكل ٢٤: الخريطة الوظيفية لمحلل دفاع الأمن السيبراني

١,١,٥ محلل دفاع الأمن السيبراني من المستوى الأول

مسمى الدور الوظيفي: محلل دفاع الأمن السيبراني (PD-D-001)	المستوى الوظيفي: المستوى الأول
وصف الدور الوظيفي	مساعدة الفريق، باستخدام البيانات التي جرى جمعها من أدوات الدفاع السيبراني؛ لتوفير المراقبة، والتصنيف الأول للأحداث التي تحدث داخل مؤسسته؛ للكشف عن التهديدات السيبرانية، والحد منها. يؤدي الفرد في هذا الدور بعض المهمات الأساسية تحت إشراف مباشر، بينما يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات المساعدة في إنشاء توقيعات لتنفيذ أدوات شبكة الأمن السيبراني للاستجابة للتهديدات الجديدة أو الملحوظة داخل البيئات، وتقديم تقارير موجزة عن فعاليات الشبكة وغيرها من الأنشطة ذات الصلة بالأمن السيبراني بما يتسق مع السياسات والمتطلبات التنظيمية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية. • الأدوار الرئيسية للأمن السيبراني من المستوى الأول. • مطور الأمن السيبراني من المستوى الأول.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مطور الأمن السيبراني من المستوى الأول. • محلل دفاع الأمن السيبراني من المستوى الثاني.

جدول ٨٠: محلل دفاع الأمن السيبراني من المستوى الأول

٢,١,٥ محلل دفاع الأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي:	المستوى الوظيفي:
محلل دفاع الأمن السيبراني (PD-D-001)	المستوى الثاني

وصف الدور الوظيفي	مساعدة الفريق باستخدام البيانات التي جرى جمعها من أدوات الدفاع السيبراني؛ لتوفير المراقبة والتصنيف الأول للأحداث التي تجري داخل مؤسسته، للكشف عن التهديدات السيبرانية والحد منها. يؤدي الفرد في هذا الدور بعض المهمات الأساسية تحت إشراف مباشر، بينما يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات المساعدة في إنشاء توقيعات؛ لتنفيذ أدوات شبكة الأمن السيبراني للاستجابة للتهديدات الجديدة، أو الملحوظة داخل البيئات، وتقديم تقارير موجزة عن فعاليات الشبكة، وغيرها من الأنشطة ذات الصلة بالأمن السيبراني بما يتسق مع السياسات والمتطلبات التنظيمية.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية • محلل دفاع الأمن السيبراني من المستوى الأول • مطور الأمن السيبراني من المستوى الثاني • أخصائي استجابة للحوادث السيبرانية من المستوى الثاني • باحث الأمن السيبراني من المستوى الثاني • محلل أمن النُظم من المستوى الثاني • أخصائي تطوير أمن النُظم من المستوى الثاني • محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • محلل دفاع الأمن السيبراني من المستوى الثالث • مطور الأمن السيبراني من المستوى الثاني • أخصائي استجابة للحوادث السيبرانية من المستوى الثاني • باحث الأمن السيبراني من المستوى الثاني • محلل أمن النُظم من المستوى الثاني • محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني

جدول ٨١: محلل دفاع الأمن السيبراني من المستوى الثاني

٣,١,٥ محلل دفاع الأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي:	المستوى الوظيفي:
محلل دفاع الأمن السيبراني (PD-D-001)	المستوى الثالث

وصف الدور الوظيفي	ممارس أول في الأمن السيبراني، يعتمد على البيانات المستخلصة من أدوات الدفاع السيبراني؛ لتحليل الأحداث داخل المنظمة، بهدف رصد التهديدات السيبرانية، والحد منها بفاعلية. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بهذا الدور، والعمل تحت إشراف محلل دفاع الأمن السيبراني، ومراجعته من المستوى الرابع. تشمل المهمات ربط المعلومات من مصادر متعددة؛ لفهم الوضع وتحديد فعالية الهجوم السيبراني الذي جرى لحظة حدوثه وإجراء مراجعات الأمن السيبراني، وتحديد الثغرات الأمنية في المعمارية الأمنية؛ لإثراء إستراتيجيات الحد من المخاطر.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية:	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية:
• محلل دفاع الأمن السيبراني من المستوى الثاني • مطور الأمن السيبراني من المستوى الثالث • باحث الأمن السيبراني من المستوى الثالث • محلل أمن النُظم من المستوى الثالث • محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • أخصائي استجابة للحوادث السيبرانية من المستوى الثالث	• محلل دفاع الأمن السيبراني من المستوى الرابع • أخصائي استجابة للحوادث السيبرانية من المستوى الثالث • باحث الأمن السيبراني من المستوى الثالث • محلل أمن النُظم من المستوى الثالث • محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • مطور الأمن السيبراني من المستوى الثالث

جدول ٨٢: محلل دفاع الأمن السيبراني من المستوى الثالث

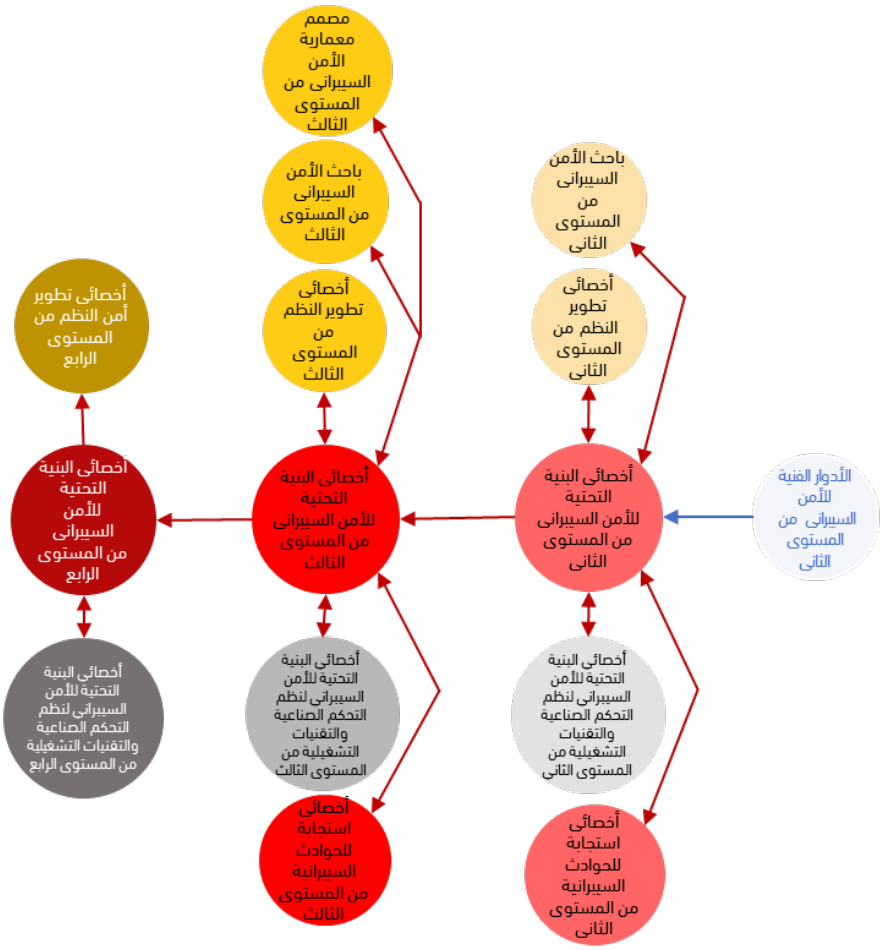
٤,١,٥ محلل دفاع الأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: محلل دفاع الأمن السيبراني (PD-D-001)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وِحدَة، تعنى باستخدام البيانات التي جرى استخلاصها من مجموعة أدوات الدفاع السيبراني؛ لتحليل الأحداث الواقعة داخل المنظمة، بهدف الكشف عن التهديدات والحد منها. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال محلل دفاع الأمن السيبراني من المستوى الثالث، وضمان استكمالها، وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تشمل المهمات تقديم توصيات بشأن الأمن السيبراني إلى صاحب الصلاحية استنادًا إلى التهديدات والثغرات الكبيرة وتقييم مدى ملاءمة ضوابط الوصول مقارنة بالسياسات التي تتخذها المنظمة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • محلل دفاع الأمن السيبراني من المستوى الثالث • محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع

جدول ٨٣: محلل دفاع الأمن السيبراني من المستوى الرابع

٢,٥ أخصائي البنية التحتية للأمن السيبراني

يقوم أخصائي البنية التحتية للأمن السيبراني، بفحص الأجهزة، والبرمجيات، وتنفيذها، ونشرها، وصيانتها، وإدارتها؛ لحماية نظم والشبكات، والدفاع عنها ضد التهديدات السيبرانية. يتطلب هذا العمل الحصول على شهادات، أو تدريب في إدارة النُظم والشبكات، وإدارة البنية التحتية للأمن السيبراني، وتنفيذ ضوابط الأمن السيبراني، وتشغيل الأجهزة/البرامج.



شكل ٢٥: الخريطة الوظيفية لأخصائي البنية التحتية للأمن السيبراني

١,٢,٥ أخصائي البنية التحتية للأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي البنية التحتية للأمن السيبراني (PD- D-002)	المستوى الثاني

وصف الدور الوظيفي	
	ممارس يساعد في تشغيل الأجهزة والبرمجيات لاختبارها وتنصيبها وإدارتها، وهي البرمجيات التي تحمي النُظم والشبكات من تهديدات الأمن السيبراني. يعمل الفرد في هذا الدور على تنفيذ المهمات الأساسية تحت الإشراف، مع تعزيز مهاراته من خلال التطبيق العملي. تشمل المهمات تقديم الدعم في إعداد البنية التحتية للأمن السيبراني وإداراتها، وفحص النُظم، والمساعدة في تحديث القواعد والتوقيعات لتطبيقات الدفاع السيبراني.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية • الأدوار الفنية للأمن السيبراني من المستوى الثاني • أخصائي استجابة للحوادث السيبرانية من المستوى الثاني • باحث الأمن السيبراني من المستوى الثاني • أخصائي تطوير أمن النُظم من المستوى الثاني • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث • أخصائي استجابة للحوادث السيبرانية من المستوى الثاني • باحث الأمن السيبراني من المستوى الثاني • أخصائي تطوير أمن النُظم من المستوى الثاني • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني

جدول ٨٤: أخصائي البنية التحتية للأمن السيبراني من المستوى الثاني

٢,٢,٥ أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي البنية التحتية للأمن السيبراني (PD- D-002)	المستوى الثالث

وصف الدور الوظيفي	ممارس أول يقوم بتنصيب الأجهزة والبرمجيات المستخدمة للدفاع وحماية النُظم والشبكات من التهديدات السيبرانية وفحصها وصيانتها وتشغيلها والإشراف عليها. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بهذا الدور، والعمل تحت إشراف مُدقّق الأمن السيبراني ومراجعته من المستوى الرابع، تشمل المهمات تنفيذ إدارة النُظم في تطبيقات ونظم الأمن السيبراني المتخصصة وإدارة تحديث القواعد والتوقيعات لتطبيقات الدفاع السيبراني.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية:	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية:
• أخصائي البنية التحتية للأمن السيبراني من المستوى الثاني • مصمم معمارية الأمن السيبراني من المستوى الثالث • أخصائي استجابة للحوادث السيبرانية من المستوى الثالث • باحث الأمن السيبراني من المستوى الثالث • أخصائي تطوير أمن النُظم من المستوى الثالث • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث	• أخصائي البنية التحتية للأمن السيبراني من المستوى الرابع • مصمم معمارية الأمن السيبراني من المستوى الثالث • أخصائي استجابة للحوادث السيبرانية من المستوى الثالث • باحث الأمن السيبراني من المستوى الثالث • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • أخصائي تطوير أمن النُظم من المستوى الثالث

جدول ٨٥: أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث

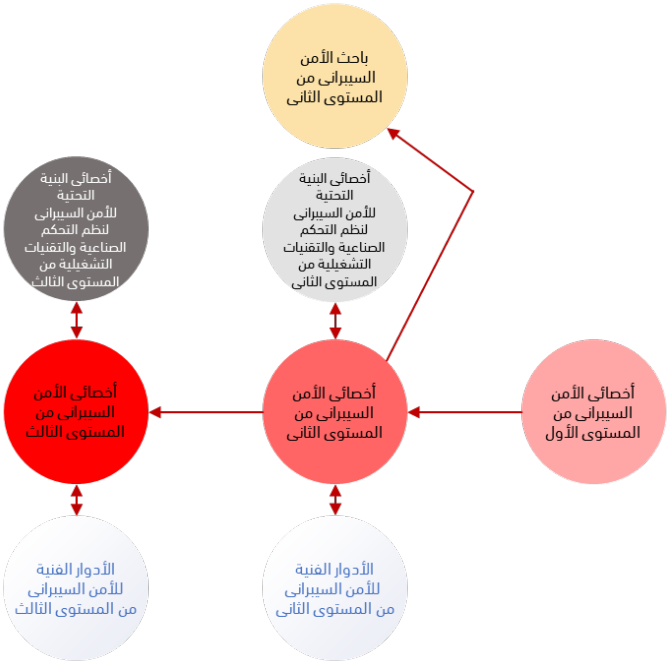
٣,٢,٥ أخصائي البنية التحتية للأمن السيبراني من المستوى الرابع

مسمى الدور الوظيفي: أخصائي البنية التحتية للأمن السيبراني (PD- D-002)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً لإدارة الأجهزة والبرمجيات واختبارها وتنفيذها ونشرها وصيانتها وهي الأمور التي تحمي النُظم والشبكات من تهديدات الأمن السيبراني. يتحمل الفرد في هذا الدور مسؤولية الإشراف على معظم أعمال أخصائي البينة التحتية للأمن السيبراني من المستوى الثالث، وضمان اكتمالها، وفقًا للمعايير المناسبة، وضمن الأطر الزمنية ذات الصلة. تشمل المهمات تحديد وترتيب أولويات وتنسيق حماية البنية التحتية والموارد الأساسية للدفاع السيبراني والعمل على ترتيبها وتنسيقها، وتنفيذ إطار إدارة المخاطر ومتطلبات التقييم الأمني والتراخيص لنظم الدفاع السيبراني المخصصة داخل المنظمة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع • أخصائي تطوير أمن النُظم من المستوى الرابع	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع • أخصائي تطوير أمن النُظم من المستوى الرابع

جدول ٨٦: أخصائي البنية التحتية للأمن السيبراني من المستوى الرابع

٣,٥ أخصائي الأمن السيبراني

يقدم أخصائي الأمن السيبراني الدعم العام للأمن السيبراني، ويساعد في مختلف مهمات الأمن السيبراني. يتطلب هذا العمل الحصول على شهادات، أو تدريب في أساسيات الأمن السيبراني، وتحليل التهديدات، وتقييم الثغرات، ودعم عمليات الأمن السيبراني.



شكل ٢٦: الخريطة الوظيفية لأخصائي الأمن السيبراني

١,٣,٥ أخصائي الأمن السيبراني من المستوى الأول

مسمى الدور الوظيفي: أخصائي أمن سيبراني (PD-D-003)	المستوى الوظيفي: المستوى الأول
وصف الدور الوظيفي	دعم الفريق من خلال تقديم الدعم العام في الأمن السيبراني. والمساعدة في مهمات الأمن السيبراني. يؤدي الفرد في هذا الدور بعض المهمات الأساسية تحت إشراف مباشر، بينما يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات ربط بيانات الحوادث لتحديد الثغرات وتقديم تقارير موجزة عن الأحداث التي تقع في الشبكة وغيرها من الأنشطة ذات الصلة بالأمن السيبراني، بما يتسق مع السياسات والمتطلبات المؤسسية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي الأمن السيبراني من المستوى الثاني.

جدول ٨٧: أخصائي الأمن السيبراني من المستوى الأول

٢,٣,٥ أخصائي الأمن السيبراني من المستوى الثاني

مسمى الدور الوظيفي: أخصائي أمن سيبراني (PD-D-003)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يعمل على تقديم الدعم العام للأمن السيبراني، والمساعدة في مهمات الأمن السيبراني. سيتولى الفرد في هذا الدور الإشراف على العمل الذي يقوم به أخصائي الأمن السيبراني من المستوى الأول، ويواصل تطوير مهاراته من خلال التطبيق العملي. تشمل المهمات تحليل ملفات السجل من مصادر متعددة؛ لتحديد التهديدات المحتملة لأمن الشبكة وتحليل اتجاهات الدفاع السيبراني والإبلاغ عنها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية • أخصائي الأمن السيبراني من المستوى الأول • الأدوار الفنية للأمن السيبراني من المستوى الثاني • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي الأمن السيبراني من المستوى الثالث • الأدوار الفنية للأمن السيبراني من المستوى الثاني • باحث الأمن السيبراني من المستوى الثاني • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني

جدول ٨٨: أخصائي الأمن السيبراني من المستوى الثاني

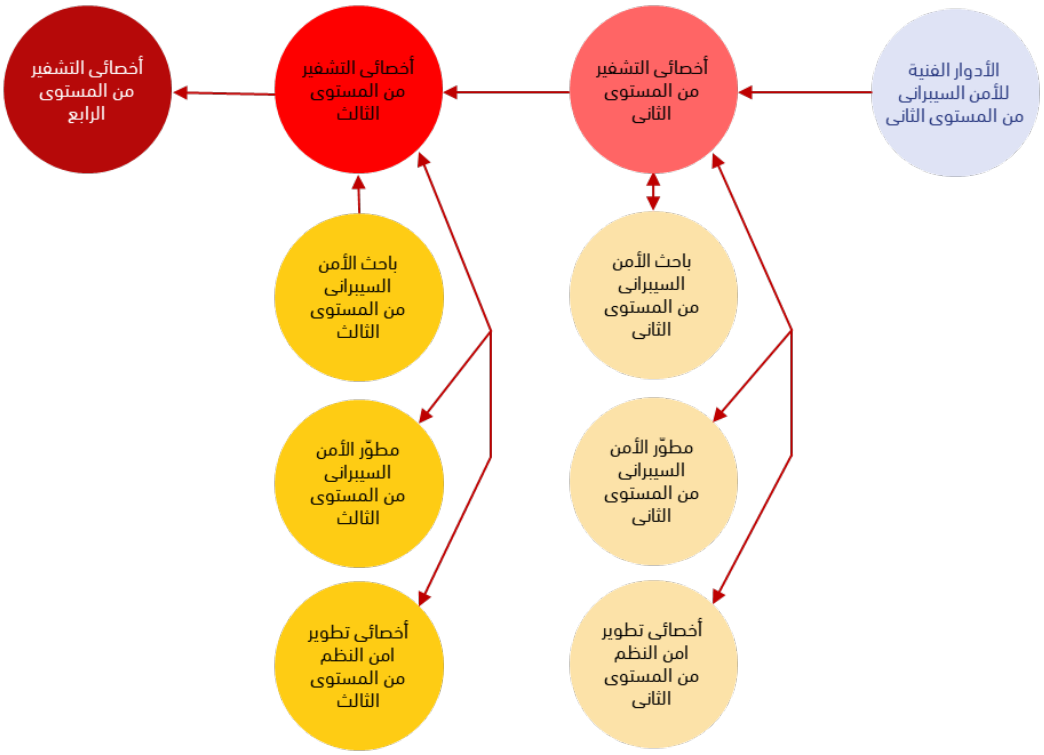
٣,٣,٥ أخصائي الأمن السيبراني من المستوى الثالث

مسمى الدور الوظيفي: أخصائي أمن سيبراني (PD-D-003)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يتولى إدارة الفريق أو توجيه الآخرين في تقديم الدعم العام في مجال الأمن السيبراني. قيادة مهمات الأمن السيبراني. يتحمل الفرد في هذا الدور مسؤولية الإشراف على معظم أعمال أخصائي البنية التحتية للأمن السيبراني من المستوى الثاني، وضمان اكتمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تشمل المهمات تقييم مستوى الأمن السيبراني ومراقبته، وفحص الممارسات والنُظم في المنظمة، وإجراء تقييمات للمخاطر والثغرات الفنية وغير الفنية للبيئات التقنية في المنظمة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي الأمن السيبراني من المستوى الثاني • الأدوار الفنية للأمن السيبراني من المستوى الثالث • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • الأدوار الفنية للأمن السيبراني من المستوى الثالث • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث

جدول ٨٩: أخصائي الأمن السيبراني من المستوى الثالث

٤,٥ أخصائي التشفير

يقوم أخصائي التشفير بتحليل نظم وخوارزميات التشفير وتطويرها وتقييمها، وتحديد نقاط الضعف والتوصية بالتحسينات. ويتطلب هذا العمل الحصول على شهادات، أو تدريب في تصميم نظم التشفير، وتقنيات التشفير وفك التشفير، وإدارة البيانات الآمنة، وتحليل خوارزمية التشفير.



شكل ٢٧: الخريطة الوظيفية لأخصائي التشفير

١,٤,٥ أخصائي التشفير من المستوى الثاني

مسمى الدور الوظيفي: أخصائي التشفير (PD-P-001)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يساعد في تطوير خوارزميات التشفير ونظمه وتقييمها لحماية البيانات والاتصالات في المنظمة. يعمل الفرد في هذا الدور على تنفيذ بعض المهمات الأساسية تحت الإشراف، مع تعزيز مهاراته من خلال التطبيق العملي، تشمل المهمات تشفير البيانات وفك تشفيرها، ودعم تنفيذ تدابير التشفير، وتحليل فاعلية نظم التشفير الحالية.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية • الأدوار الفنية للأمن السيبراني من المستوى الثاني • مطور الأمن السيبراني من المستوى الثاني • باحث الأمن السيبراني من المستوى الثاني • أخصائي تطوير أمن النُظم من المستوى الثاني	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي التشفير من المستوى الثالث • مطور الأمن السيبراني من المستوى الثاني • باحث الأمن السيبراني من المستوى الثاني • أخصائي تطوير أمن النُظم من المستوى الثاني

جدول ٩٠: أخصائي التشفير من المستوى الثاني

٢,٤,٥ أخصائي التشفير من المستوى الثالث

مسمى الدور الوظيفي: أخصائي التشفير (PD-P-001)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يتولى إدارة الفريق أو توجيه الآخرين عن تطوير نظم التشفير وخوارزمياته، وتقييمها وتحليلها وتحديد نقاط ضعفها وسبل تحسينها. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالعمل لمراجعتها من قبل أخصائي التشفير من المستوى الرابع والعمل تحت إشرافه. تشمل المهمات فك التشفير الفني للبيانات المضبوطة وتنفيذ تدابير أمن النُظم وفقًا للإجراءات المعمول بها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي التشفير من المستوى الثاني • مطور الأمن السيبراني من المستوى الثالث • باحث الأمن السيبراني من المستوى الثالث • أخصائي تطوير أمن النُظم من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي التشفير من المستوى الرابع • مطور الأمن السيبراني من المستوى الثالث • باحث الأمن السيبراني من المستوى الثالث • أخصائي تطوير أمن النُظم من المستوى الثالث

جدول ٩١: أخصائي التشفير من المستوى الثالث

٣,٤,٥ أخصائي التشفير من المستوى الرابع

مسمى الدور الوظيفي: أخصائي التشفير (PD-P-001)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدة التشفير المسؤولة عن تطوير نظم التشفير وخوارزمياته، وتقييمها وتحليلها وتحديد نقاط ضعفها وسبل تحسينها. يتحمل الفرد في هذا الدور مسؤولية الإشراف على الكثير من أعمال أخصائي التشفير من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تشمل المهمات ضمان توافق قدرات الحماية والكشف مع إستراتيجية الأمن السيبراني والسياسات والوثائق الأخرى ذات الصلة، وتطوير قدرات إدارة البيانات الآمنة لدعم المختصين في تنقلاتهم.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي التشفير من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ٩٢: أخصائي التشفير من المستوى الرابع

0,0 أخصائي إدارة الهويّة والوصول

يتولى أخصائي إدارة الهويّة والوصول إدارة الهويات والوصول إلى الموارد من خلال تنفيذ نظم وعمليات تحديد الهوية والتوثيق والتصريح. يستلزم هذا العمل امتلاك شهادات أو تدريب متخصص في إدارة دورة حياة الهوية، ووضع سياسات التحكم في الوصول، وتنفيذ إجراءات المصادقة، وإدارة صلاحيات الوصول المميز.

شكل ٢٨: الخريطة الوظيفية لأخصائي إدارة الهويّة والوصول

1,0,0 أخصائي إدارة الهويّة والوصول من المستوى الثاني

مسمى الدور الوظيفي: أخصائي إدارة الهويّة والوصول (PD-P-002)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس يساعد في إدارة هوية الأفراد والكيانات، وصلاحيات وصولهم إلى الموارد من خلال تطبيق نظم وعمليات المصادقة، والتحقق والتوثيق والتصريح. يعمل الفرد في هذا الدور على تنفيذ بعض المهمات الأساسية تحت الإشراف، مع تعزيز مهاراته من خلال التطبيق العملي، تشمل المهمات المساعدة في تنفيذ حلول إدارة الوصول إلى الهوية ودعم الجهات المعنية لمعالجة الفجوات في نظام إدارة الوصول إلى الهوية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي إدارة الهويّة والوصول من المستوى الثالث

جدول ٩٣: أخصائي إدارة الهويّة والوصول من المستوى الثاني

٢,٥,٥ أخصائي إدارة الهويّة والوصول من المستوى الثالث

مسمى الدور الوظيفي: أخصائي إدارة الهوّية والوصول (PD-P-002)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يتولى إدارة هوية الأفراد والكيانات، وصلاحيات وصولهم إلى الموارد من خلال تطبيق نظم المصادقة وعملياتها، وكذلك التحقق والتوثيق والتصريح. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالدور الوظيفي لمراجعتها من قبل أخصائي إدارة الهويّة والوصول في المستوى الرابع والعمل تحت إشرافه. تشمل المهمات العمل مع فرق أخرى لتصميم حلول إدارة الوصول إلى الهوية وتطويرها وتوفيرها، والعمل مع أصحاب المصلحة لتحديد الفجوات ومعالجتها في تنفيذ إدارة الوصول إلى الهوية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي إدارة الهويّة والوصول من المستوى الثاني	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي إدارة الهويّة والوصول من المستوى الرابع

جدول ٩٤: أخصائي إدارة الهويّة والوصول من المستوى الثالث

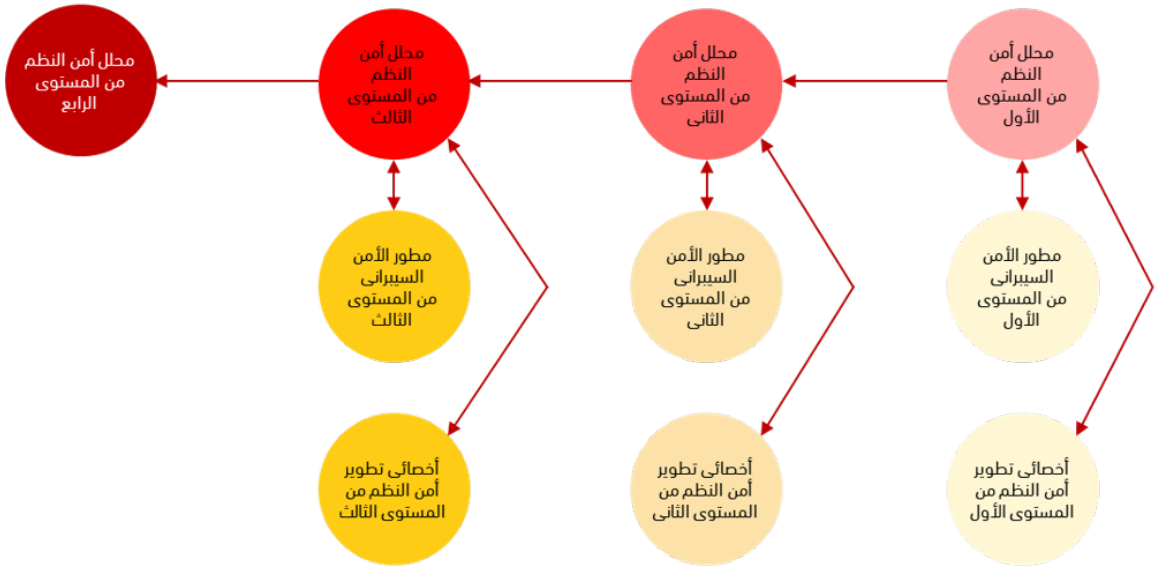
٣,٥,٥ أخصائي إدارة الهويّة والوصول من المستوى الرابع

مسمى الدور الوظيفي: أخصائي إدارة الهويّة والوصول (PD-P-002)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدة لإدارة هوية الأفراد والكيانات والوصول إلى الموارد من خلال تطبيق نظم تخديد الهوية وعملياتها، وكذلك التوثيق والتصريح. يتحمل الفرد في هذا الدور مسؤولية الإشراف على معظم أعمال أخصائي إدارة الهويّة والوصول من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تشمل المهمات ضمان اتباع عمليات تنفيذ إدارة الوصول إلى الهوية لمعايير وسياسات المنظمة وتوجيه أعضاء الفريق وتقديم المشورة لهم بشأن نظم وإجراءات إدارة الوصول إلى الهوية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي إدارة الهويّة والوصول من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ٩٥: أخصائي إدارة الهويّة والوصول من المستوى الرابع

٦,٠ محلل أمن النُظم

يقوم محلل أمن النُظم بتطوير أمن النُظم واختباره وصيانته، وتحليل أمن العمليات والنُظم المدمجة. ويتطلب هذا العمل الحصول على شهادات، أو تدريب في تحليل أمن النُظم، وإدارة الثغرات الأمنية، وعمليات النُظم الآمنة، ودورة حياة تطوير النُظم الآمنة.



شكل ٢٩: الخريطة الوظيفية لمحلل أمن النُظم

١,٦,٥ محلل أمن النُظم من المستوى الأول

مسمى الدور الوظيفي:	المستوى الوظيفي:
محلل أمن النُظم (PD-P-003)	المستوى الأول

وصف الدور الوظيفي	يساعد الفريق في تطوير أمن النُظم واختباره وصيانته، ويوفر التحليل الأساسي لأمن العمليات والنُظم المتكاملة. يؤدي الفرد في هذا الدور بعض المهمات الأساسية تحت إشراف مباشر، بينما يواصل اكتساب المعرفة بمتطلبات الوظيفة، تشمل المهمات تطبيق التحديثات الأمنية على المنتجات التجارية وفقًا للجدول الزمني الذي تحدده الإدارة المسؤولة والتحقق من وجود الحد الأدنى من المتطلبات الأمنية لجميع التطبيقات.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية • مطور الأمن السيبراني من المستوى الأول • أخصائي تطوير أمن النُظم من المستوى الأول	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • محلل أمن النُظم من المستوى الثاني • مطور الأمن السيبراني من المستوى الأول • أخصائي تطوير أمن النُظم من المستوى الأول

جدول ٩٦: محلل أمن النُظم من المستوى الأول

٢,٦,٥ محلل أمن النُظم من المستوى الثاني

مسمى الدور الوظيفي:	المستوى الوظيفي:
محلل أمن النُظم (PD-P-003)	المستوى الثاني

وصف الدور الوظيفي	ممارس يقوم بتطوير أمن النُظم وفحصها والحفاظ عليها وتحليل أمن العمليات والنُظم المتكاملة. سيتولى الفرد في هذا الدور الإشراف على العمل الذي يقوم به محلل أمن النُظم من المستوى الأول، ويواصل تطوير مهاراته من خلال التطبيق العملي. تتضمن المهمات تطوير العمليات والإجراءات الخاصة بالتحديث اليدوي لبرمجيات النظام وتصحيحها استنادًا إلى متطلبات الإطار الزمني الحالي والمتوقع لتصحيح البيئة التشغيلية للنظام وتطبيق السياسات الأمنية على التطبيقات التي تتفاعل مع بعضها.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية • محلل أمن النُظم من المستوى الأول • مطور الأمن السيبراني من المستوى الثاني • أخصائي تطوير أمن النُظم من المستوى الثاني	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • محلل أمن النُظم من المستوى الثالث • مطور الأمن السيبراني من المستوى الثاني • أخصائي تطوير أمن النُظم من المستوى الثاني

جدول ٩٧: محلل أمن النُظم من المستوى الثاني

٣,٦,٥ محلل أمن النُظم من المستوى الثالث

مسمى الدور الوظيفي: محلل أمن النُظم (PD-P-003)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يقوم بتطوير أمن النُظم واختبارها وصيانتها. وتحليل أمن العمليات والنُظم المتكاملة. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالدور الوظيفي؛ لمراجعتها من قبل محلل أمن النُظم من المستوى الرابع والعمل تحت إشرافه. تشمل المهمات العمل مع أصحاب المصلحة لحل حوادث الأمن السيبراني وقضايا الالتزام في الثغرات الأمنية وتطبيق مبادئ المعمارية الأمنية الموجهة نحو الخدمات لتلبية متطلبات السرية والنزاهة والتوافر الخاصة بالمنظمة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • محلل أمن النُظم من المستوى الثاني • مطور الأمن السيبراني من المستوى الثالث • أخصائي تطوير أمن النُظم من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • محلل أمن النُظم من المستوى الرابع • مطور الأمن السيبراني من المستوى الثالث • أخصائي تطوير أمن النُظم من المستوى الثالث

جدول ٩٨: محلل أمن النُظم من المستوى الثالث

٤,٦,٥ محلل أمن النُظم من المستوى الرابع

مسمى الدور الوظيفي:	المستوى الوظيفي:
محلل أمن النُظم (PD-P-003)	المستوى الرابع

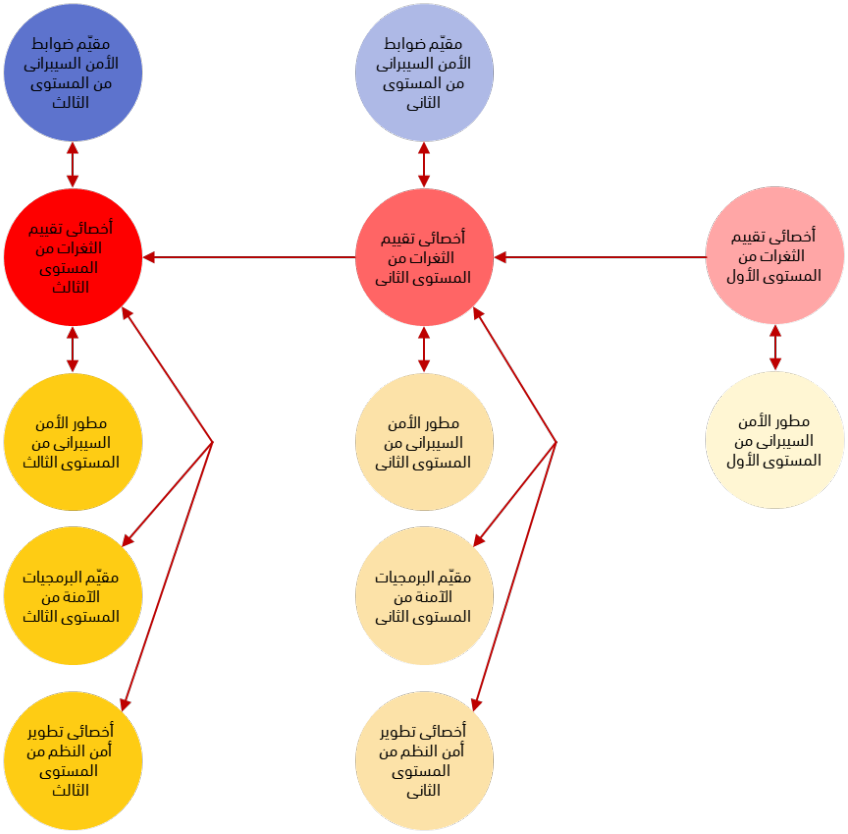
وصف الدور الوظيفي	خبير يدير وحدَة لإدارة الخبراء، لتطوير أمن النُظم واختباره وصيانته، وتحليل أمن العمليات والنُظم المتكاملة. يتحمل الفرد في هذا الدور مسؤولية الإشراف على الكثير من أعمال محلل أمن النُظم من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. وستتضمن المهمات تقديم توصيات بشأن الأمن السيبراني إلى القيادة استنادًا إلى التهديدات والثغرات الكبيرة وضمان دمج الحلول الشاملة في بيئة آمنة وتنفيذها.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • محلل أمن النُظم من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ٩٩: محلل أمن النُظم من المستوى الرابع

٧,٥ أخصائي تقييم الثغرات

يقوم أخصائي تقييم الثغرات بإجراء تقييمات للنظم والشبكات لتحديد الإعدادات الغير متوافقة مع السياسات المقبولة وتقييم فعالية البنية الدفاعية المتعمقة مقابل نقاط الثغرات المعروفة. ويتطلب هذا العمل الحصول على شهادات أو تدريب في تقييم الثغرات، ومنهجيات اختبار الاختراق، وتحليل المخاطر، واستخدام أدوات مسح نظم الثغرات الأمنية واختبارها.



شكل ٣٠: الخريطة الوظيفية لأخصائي تقييم الثغرات

١,٧,٥ أخصائي تقييم الثغرات من المستوى الأول

مسمى الدور الوظيفي: أخصائي تقييم الثغرات (PD-VA-001)	المستوى الوظيفي: المستوى الأول
وصف الدور الوظيفي	المساعدة في إجراء تقييمات الثغرات للنظم والشبكات. وتحديد الأماكن التي تتعارض مع الإعدادات المقبولة أو السياسات المعمول بها، وكذلك قياس فعالية البنية الدفاعية المتعمقة ضد الثغرات المعروفة. يؤدي الفرد في هذا الدور بعض المهمات الأساسية تحت إشراف مباشر، بينما يواصل اكتساب المعرفة بمتطلبات الوظيفة، تتضمن المهمات استخدام أدوات اختبار الأمان ومسح الشفرات البرمجية لإجراء مراجعات تفصيلية للشيفرة، إلى جانب تنفيذ تقييمات شاملة للمخاطر والثغرات الأمنية، سواء أكانت تقنية أم غير تقنية، ضمن بيئة تقنية المعلومات الخاصة بالمنظمة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الأول من المؤهلات العلمية • الأدوار الرئيسية للأمن السيبراني من المستوى الأول. • مطور الأمن السيبراني من المستوى الأول	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي تقييم الثغرات من المستوى الثاني • مطور الأمن السيبراني من المستوى الأول

جدول ١٠٠: أخصائي تقييم الثغرات من المستوى الأول

٢,٧,٥ أخصائي تقييم الثغرات من المستوى الثاني

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي تقييم الثغرات (PD-VA-001)	المستوى الثاني
وصف الدور الوظيفي	ممارس يقوم بتقييم الثغرات الأمنية في النُظم والشبكات. وتحديد الأماكن التي تتعارض مع الإعدادات المقبولة أو السياسات المعمول بها، وقياس فعالية البنية الدفاعية المتعمقة ضد الثغرات المعروفة. سيتولى المختص في هذا الدور الإشراف على العمل الذي يقوم به أخصائي تقييم الثغرات، ويواصل تطوير مهاراته من خلال التطبيق العملي. تتضمن المهمات مراجعة سياسات الدفاع السيبراني وإعداداته للمؤسسة؛ لضمان توافقها مع اللوائح والتوجيهات التنظيمية، إلى جانب إعداد مجموعة أدوات تدقيق متخصصة في الدفاع السيبراني وصيانتها، وتكون مستندة إلى أفضل الممارسات العالمية، لدعم عمليات التدقيق في الأمن السيبراني.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية:	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية:
• الخريج الحاصل على المستوى الثاني من المؤهلات العلمية • أخصائي تقييم الثغرات من المستوى الأول • مطور الأمن السيبراني من المستوى الثاني • أخصائي تطوير أمن النُظم من المستوى الثاني • مُقيّم البرمجيات الآمنة من المستوى الثاني • مُقيّم ضوابط الأمن السيبراني من المستوى الثاني	• أخصائي تقييم الثغرات من المستوى الثالث • مطور الأمن السيبراني من المستوى الثاني • أخصائي تطوير أمن النُظم من المستوى الثاني • مُقيّم البرمجيات الآمنة من المستوى الثاني • مُقيّم ضوابط الأمن السيبراني من المستوى الثاني

جدول ١٠١: أخصائي تقييم الثغرات من المستوى الثاني

٣,٧,٥ أخصائي تقييم الثغرات من المستوى الثالث

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي تقييم الثغرات (PD-VA-001)	المستوى الثالث

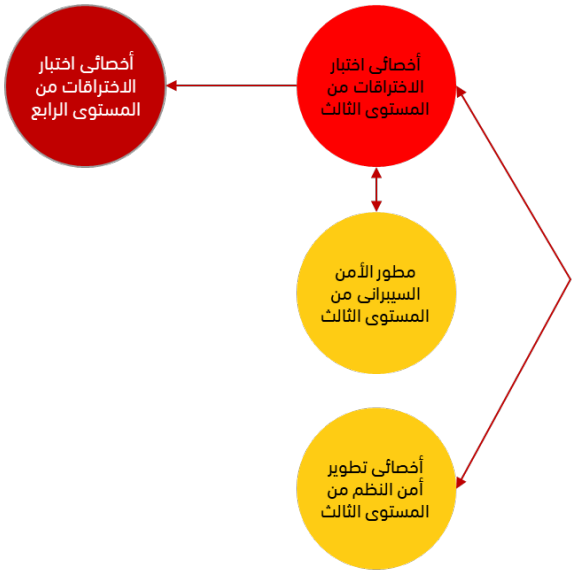
وصف الدور الوظيفي	ممارس أول يقوم بتقييم الثغرات الأمنية في النُظم والشبكات. وتحديد الأماكن التي تتعارض مع الإعدادات المقبولة أو السياسات المعمول بها، وقياس فعالية البنية الدفاعية المتعمقة ضد الثغرات المعروفة. يتحمل الفرد في هذا الدور مسؤولية الإشراف على الكثير من أعمال أخصائي تقييم الثغرات من المستوى الثاني، وضمان استكمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تتضمن المهمات متابعة أحدث السياسات واللوائح ووثائق الالتزام المتعلقة بالدفاع السيبراني، لا سيما تلك المرتبطة بتدقيق الأمن السيبراني، مع تقديم توصيات بحلول أمنية فعالة من حيث التكلفة لمعالجة المخاطر التي يجري تحديدها من خلال الاختبار والمراجعة. عادةً ما يعمل أخصائي تقييم الثغرات من المستوى الثالث تحت إشراف أخصائي اختبار الاختراقات من المستوى الرابع، والذي سيضمن، بالإضافة إلى توفير الإدارة العامة للموظفين، ما يلي: • تحديد الثغرات وتصنيفها وتقييمها بشكل مناسب. • تنفيذ خطط الإغلاق بشكل فعال.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي تقييم الثغرات من المستوى الثاني • مطور الأمن السيبراني من المستوى الثالث • أخصائي تطوير أمن النُظم من المستوى الثالث • مُقيّم البرمجيات الآمنة من المستوى الثالث • مُقيّم ضوابط الأمن السيبراني من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مطور الأمن السيبراني من المستوى الثالث • أخصائي تطوير أمن النُظم من المستوى الثالث • مُقيّم البرمجيات الآمنة من المستوى الثالث • مُقيّم ضوابط الأمن السيبراني من المستوى الثالث

جدول ١٠٢: أخصائي تقييم الثغرات من المستوى الثالث

٨,٥ أخصائي اختبار الاختراقات

يجري أخصائي اختبار الاختراقات اختبارات اختراق معتمدة على نظم الكمبيوتر والشبكات والمنشآت المادية، باستخدام أساليب تهديد واقعية لتقييم حالتها الأمنية وكشف الثغرات المحتملة. يتطلب هذا العمل الحصول على شهادات، أو تدريب في منهجيات اختبار الاختراق، وأساليب القرصنة الأخلاقية، واستغلال الثغرات، وعمليات اختبار الاختراقات لتقييم الفجوات الأمنية.



شكل ٣١: الخريطة الوظيفية لأخصائي اختبار الاختراقات

١,٨,٥ أخصائي اختبار الاختراقات من المستوى الثالث

مسمى الدور الوظيفي: أخصائي اختبار الاختراقات (PD-VA-002)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يقوم بتنفيذ محاولات اختراق مصرح بها لنظم الحاسبات أو الشبكات والمنشآت المادية باستخدام أساليب تهديد واقعية لتقييم حالتها الأمنية وكشف الثغرات المحتملة. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بمهمته لمراجعتها والعمل تحت إشراف أخصائي اختبار الاختراقات من المستوى الرابع ومراجعته، تشمل المهمات جمع المعلومات عن تكوين الشبكة واستخدامها من خلال التحليل الفني والأبحاث المفتوحة المصدر وتوثيق النتائج ومحاكاة أساليب الهندسة الاجتماعية الضارة التي يستخدمها المهاجمون لاختراق النظام والكشف عن الثغرات والفجوات الأمنية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مطور الأمن السيبراني من المستوى الثالث • أخصائي تطوير أمن النُظم من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي اختبار الاختراقات من المستوى الرابع • مطور الأمن السيبراني من المستوى الثالث • أخصائي تطوير أمن النُظم من المستوى الثالث

جدول ١٠٣: أخصائي اختبار الاختراقات من المستوى الثالث

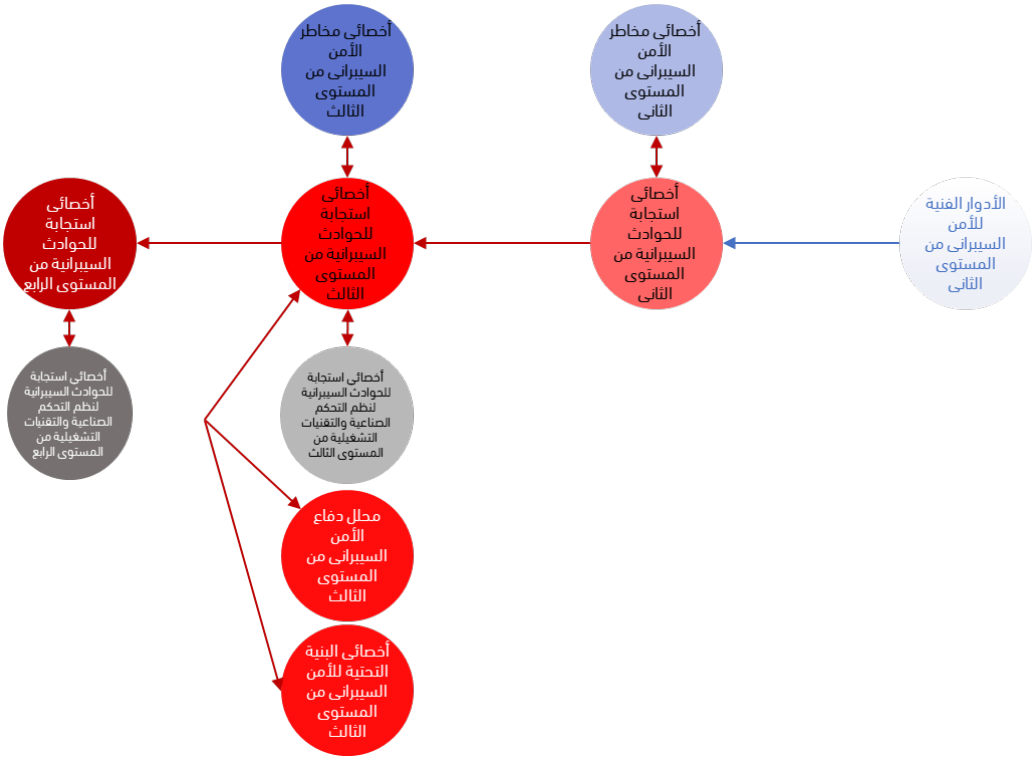
٢,٨,٥ أخصائي اختبار الاختراقات من المستوى الرابع

مسمى الدور الوظيفي: أخصائي اختبار الاختراقات (PD-VA-002)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وِحدَة تعنى بتنفيذ محاولات اختراق مصرح بها لنظم الحاسبات أو الشبكات والمنشآت المادية باستخدام أساليب تهديد واقعية لتقييم حالتها الأمنية وكشف الثغرات المحتملة. يتحمل الفرد في هذا الدور مسؤولية الإشراف على معظم أعمال أخصائي اختبار الاختراقات من المستوى الثالث، بالإضافة إلى عمل أخصائي تقييم الثغرات الأمنية في المستوى الثالث، وضمان استكماله وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. يوفر هذا العمل الإشراف على إدارة الثغرات، وضمان أن يقوم أخصائي اختبار الاختراقات وأخصائي تقييم الثغرات بمعالجة الثغرات بالطريقة والأطر الزمنية الأكثر ملاءمةً. تتضمن المهمات توثيق نتائج اختبارات الاختراق وتقييم الثغرات الأمنية، مع تحديد مستوى المخاطر، وتقديم الإستراتيجيات المناسبة للحد منها، وتوفير التفاصيل الفنية اللازمة لإعادة اختبار النتائج، إلى جانب مراعاة المتطلبات التجارية عند وضع إستراتيجيات الأمن السيبراني والتوصيات ذات الصلة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي اختبار الاختراقات من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ١٠٤: أخصائي اختبار الاختراقات من المستوى الرابع

٩,٥ أخصائي استجابة للحوادث السيبرانية

يقوم أخصائي استجابة للحوادث السيبرانية بمباشرة حوادث الأمن السيبراني وتحليلها والاستجابة لها. يتطلب هذا العمل الحصول على شهادات، أو تدريب في التعامل مع الحوادث والاستجابة لها، والمعلومات الجنائية الرقمية، وتحليل البرمجيات الضارة، ومراقبة أمن الشبكات، وعمليات مركز العمليات الأمنية (SOC) للكشف عن حوادث الأمن السيبراني وتحليلها والحد منها بشكل فعال.



شكل ٣٢: الخريطة الوظيفية لأخصائي استجابة للحوادث السيبرانية

١,٩,٥ أخصائي استجابة للحوادث السيبرانية من المستوى الثاني

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي استجابة للحوادث السيبرانية (PD-IR-001)	المستوى الثاني

وصف الدور الوظيفي	ممارس يقوم بمباشرة حوادث الأمن السيبراني وتحليلها والاستجابة لها. يعمل الفرد في هذا الدور على تنفيذ المهمات الأساسية تحت الإشراف، مع تعزيز مهاراته من خلال التطبيق العملي. تتضمن المهمات جمع بيانات الحوادث وتحليلها، وفرز التنبيهات الأمنية للكشف عن الاختراقات، وربط البيانات لتحديد الثغرات الأمنية، بالإضافة إلى تنفيذ إجراءات الاستجابة وفقًا لخطة استجابة للحوادث المعتمدة.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية • الأدوار الفنية للأمن السيبراني من المستوى الثاني • أخصائي مخاطر الأمن السيبراني من المستوى الثاني	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي استجابة للحوادث السيبرانية من المستوى الثالث • أخصائي مخاطر الأمن السيبراني من المستوى الثاني

جدول ١٠٥: أخصائي استجابة للحوادث السيبرانية من المستوى الثاني

٢,٩,٥ أخصائي استجابة للحوادث السيبرانية من المستوى الثالث

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي استجابة للحوادث السيبرانية (PD-IR-001)	المستوى الثالث

وصف الدور الوظيفي	ممارس أول يقوم بمباشرة حوادث الأمن السيبراني وتحليلها والاستجابة لها. يتحمل الفرد في هذا الدور مسؤولية تنفيذ مهمات متقدمة في مجال الأمن السيبراني، مع مراجعتها من قِبل أخصائي استجابة للحوادث السيبرانية من المستوى الرابع والعمل بتوجيهاته، ويشمل ذلك تحليل الأدلة الرقمية وربطها. تشمل المسؤوليات تقييم خطورة الحوادث السيبرانية والإبلاغ عنها، مع تقييم تأثيرها المحتمل واتخاذ قرارات سريعة لاحتوائها والحد منها. كما تتطلب تحديد نطاق الحادث وتنفيذ إستراتيجيات فعالة للقضاء عليه، مع إجراء تحليلات متعمقة للأدلة الرقمية المستخرجة من الأجهزة والشبكات؛ لفهم جذور المشكلة ومنع تكرارها.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية:	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية:
• أخصائي استجابة للحوادث السيبرانية من المستوى الثاني • أخصائي مخاطر الأمن السيبراني من المستوى الثالث • أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • محلل دفاع الأمن السيبراني من المستوى الثالث • أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث	• أخصائي استجابة للحوادث السيبرانية من المستوى الرابع • أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • أخصائي مخاطر الأمن السيبراني من المستوى الثالث • محلل دفاع الأمن السيبراني من المستوى الثالث • أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث

جدول ١٠٦: أخصائي استجابة للحوادث السيبرانية من المستوى الثالث

٣,٩,٥ أخصائي استجابة للحوادث السيبرانية من المستوى الرابع

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي استجابة للحوادث السيبرانية (PD-IR-001)	المستوى الرابع

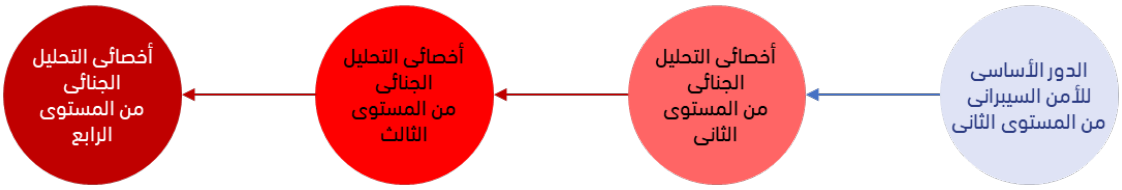
وصف الدور الوظيفي	خبير يدير وحدةً للتحقيق في حوادث الأمن السيبراني وتحليلها والاستجابة لها. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال أخصائي استجابة للحوادث السيبرانية من المستوى الثالث، وضمان استكمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تتضمن المهمات تشكيل فريق الاستجابة للحوادث وتكليفه، وقيادة جميع أنشطة الاستجابة وتنسيقها، بالإضافة إلى تقديم الإرشاد والاستشارات أثناء الحوادث. كما تشمل وضع خطط المعالجة، وإدارة تنفيذها، وتحديد محفزات المعالجة والتوقيت المناسب لتطبيقها.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي استجابة للحوادث السيبرانية من المستوى الثالث • أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع

جدول ١٠٧: أخصائي استجابة للحوادث السيبرانية من المستوى الرابع

١٠,٥ أخصائي التحليل الجنائي الرقمي

يقوم أخصائي التحليل الجنائي الرقمي بجمع الأدلة الرقمية وتحليلها للتحقيق في حوادث الأمن السيبراني واستخلاص معلومات قابلة للتنفيذ للحد من الثغرات في النظام والشبكة. يتطلب هذا العمل الحصول على شهادات أو تدريب في التعامل مع الأدلة الرقمية، وتحليل الأدلة الجنائية، وتحليل البرمجيات الضارة، وتحليل حركة البيانات على الشبكة.



شكل ٣٣: الخريطة الوظيفية لأخصائي التحليل الجنائي الرقمي

١,١٠,٥ أخصائي التحليل الجنائي الرقمي من المستوى الثاني

مسمى الدور الوظيفي: أخصائي التحليل الجنائي الرقمي (PD-IR-002)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	يقوم الممارس بجمع وتحليل الأدلة الرقمية، والتحقيق في حوادث الأمن السيبراني لاستخلاص معلومات مفيدة للحد من الثغرات في النظام والشبكة. سيتولى الفرد في هذا الدور الإشراف على العمل الذي يقوم به أخصائي من المستوى الأول، ويواصل تطوير مهاراته من خلال التطبيق العملي. تشمل المهمات ضمان اتباع إجراءات جمع الأدلة الإلكترونية وتحريزها، ونقلها، وتخزينها مع الحفاظ على سلسلة حماية الأدلة وإجراء التحليل الجنائي الأولي في بيئات نظم التشغيل المتعددة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية • دور الأمن السيبراني الأساسي من المستوى الثاني	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي التحليل الجنائي الرقمي من المستوى الثالث

جدول ١٠٨: أخصائي التحليل الجنائي الرقمي من المستوى الثاني

٢,١٠,٥ أخصائي التحليل الجنائي الرقمي من المستوى الثالث

مسمى الدور الوظيفي: أخصائي التحليل الجنائي الرقمي (PD-IR-002)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يقوم بإدارة الفريق أو توجيه الآخرين عن جمع الأدلة الرقمية وتحليلها، التحقيق في حوادث الأمن السيبراني لاستخلاص معلومات مفيدة تعمل على معالجة ثغرات النُظم والشبكات. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالدور الوظيفي لمراجعتها من قبل أخصائي التحليل الجنائي الرقمي من المستوى الرابع والعمل تحت إشرافه. تشمل المهمات دعم فرق الاستجابة السريعة للحوادث من خلال تنفيذ عمليات التحليل الجنائي الرقمي، وربط الهجمات السيبرانية وتتبعها، وتحليل التهديدات، وتطبيق إستراتيجيات معالجة النُظم. كما تتطلب تقديم تقارير فنية مفصلة تسلط الضوء على أبرز النتائج وفقًا للمعايير والإجراءات المعتمدة.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي التحليل الجنائي الرقمي من المستوى الثاني	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي التحليل الجنائي الرقمي من المستوى الرابع

جدول ١٠٩: أخصائي التحليل الجنائي الرقمي من المستوى الثالث

٣,١٠,٥ أخصائي التحليل الجنائي الرقمي من المستوى الرابع

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي التحليل الجنائي الرقمي (PD-IR-002)	المستوى الرابع

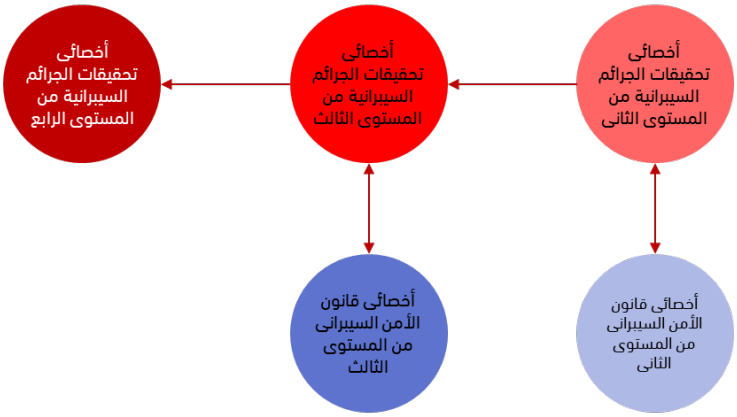
وصف الدور الوظيفي	خبير يدير وحدةً لجمع الأدلة الرقمية وتحليلها، أو التحقيق في حوادث الأمن السيبراني لاستخلاص معلومات مفيدة للحد من الثغرات في النُظم والشبكات. يتحمل الفرد في هذا الدور مسؤولية الإشراف على معظم أعمال أخصائي التحليل الجنائي الرقمي من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تشمل المهمات ضمان اتباع سلسلة حماية الأدلة لجميع وسائل الإعلام الرقمية المكتسبة وفقًا للقانون الوطني أو السياسات التنظيمية حسب الاقتضاء، والعمل بوصفه خبيرًا تقنيًا في دعم إنفاذ القانون، وشرح تفاصيل الحوادث وتحليل الأدلة الجنائية حسب الحاجة.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي التحليل الجنائي الرقمي من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ١١٠: أخصائي التحليل الجنائي الرقمي من المستوى الرابع

١١,٥ أخصائي تحقيقات الجرائم السيبرانية

يقوم أخصائي تحقيقات الجرائم السيبرانية بتعريف الدلائل الرقمية وجمعها وفحصها والحفاظ عليها، باستخدام أساليب تحرٍ واستقصاء موثقة ومقننة. يتطلب هذا العمل الحصول على شهادات أو تدريب في مجال التحليل الجنائي الرقمي، ومنهجيات التحقيق في الجرائم السيبرانية، والتعامل مع الأدلة، والجوانب القانونية للجرائم السيبرانية.



شكل ٣٤: الخريطة الوظيفية لأخصائي تحقيقات الجرائم السيبرانية

١,١١,٥ أخصائي تحقيقات الجرائم السيبرانية من المستوى الثاني

مسمى الدور الوظيفي: أخصائي تحقيقات الجرائم السيبرانية (PD-IR-003)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	ممارس متخصص في تحديد الأدلة وجمعها وفحصها وحفظها باستخدام أساليب التحليل والتحقيق الخاضعة للرقابة والتوثيق. يقوم الفرد في هذا الدور بتنفيذ بعض المهمات الأساسية لهذا العمل، ويواصل تطوير مهاراته من خلال التطبيق العملي، تشمل المسؤوليات استجواب الضحايا والشهود للكشف عن تفاصيل الجرائم السيبرانية، مع توثيق وجمع الأدلة الرقمية بطريقة تضمن سلامتها وإمكانية استخدامها في الإجراءات القانونية لملاحقة الجناة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية. • أخصائي قانون الأمن السيبراني من المستوى الثاني.	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي تحقيقات الجرائم السيبرانية من المستوى الثالث. • أخصائي قانون الأمن السيبراني من المستوى الثاني.

جدول ١١١: أخصائي تحقيقات الجرائم السيبرانية من المستوى الثاني

٢,١١,٥ أخصائي تحقيقات الجرائم السيبرانية من المستوى الثالث

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي تحقيقات الجرائم السيبرانية (PD-IR-003)	المستوى الثالث

وصف الدور الوظيفي	ممارس أول يتولى إدارة الفريق أو توجيه الآخرين حول تعريف الأدلة وجمعها وفحصها والحفاظ عليها، باستخدام أساليب تحرٍ واستقصاء موثقة ومقننة. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالدور الوظيفي والعمل تحت إشراف أخصائي تحقيقات الجرائم السيبرانية ومراجعته من المستوى الرابع. تشمل المهمات تحديد ما إذا كان حادث الأمن السيبراني قد يشكل انتهاكًا للقانون الذي يتطلب إجراءً قانونيًا محددًا وتحديد مدى التهديدات والمخاطر الناشئة عنها والتوصية بإجراءات أو تدابير مضادة للحد منها.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية:	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية:
• أخصائي تحقيقات الجرائم السيبرانية من المستوى الثاني • أخصائي قانون الأمن السيبراني من المستوى الثالث	• أخصائي تحقيقات الجرائم السيبرانية من المستوى الرابع • أخصائي قانون الأمن السيبراني من المستوى الثالث

جدول ١١٢: أخصائي تحقيقات الجرائم السيبرانية من المستوى الثالث

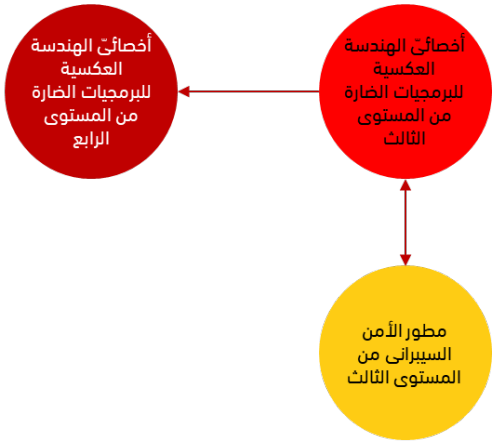
٣,١١,٥ أخصائي تحقيقات الجرائم السيبرانية من المستوى الرابع

مسمى الدور الوظيفي: أخصائي تحقيقات الجرائم السيبرانية (PD-IR-003)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً لتحديد الأدلة وجمعها وفحصها والحفاظ عليها باستخدام أساليب التحليل والتحقيق الخاضعة للرقابة والتوثيق. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال أخصائي تحقيقات الجرائم السيبرانية من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تتضمن المهمات تقديم الدعم في التحقيقات الجنائية إلى السلطات القانونية خلال العملية القضائية وتوثيق التحقيق بما يتسق مع المعايير والمتطلبات القانونية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي تحقيقات الجرائم السيبرانية من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ١١٣: أخصائي تحقيقات الجرائم السيبرانية من المستوى الرابع

١٢,٥ أخصائي الهندسة العكسية للبرمجيات الضارة

يتولى أخصائي الهندسة العكسية للبرمجيات الضارة فك شفرة البرامج الضارة وتحليل بنيتها العميقة للكشف عن آليات عملها وتأثيرها المحتمل ونوايا الجهات المهاجمة. كما يوصي الأخصائي بأساليب الحد من مخاطر الحوادث المتوقعة وإجراءات الاستجابة لها. يتطلب هذا العمل الحصول على شهادات أو تدريب في مجال تحليل البرمجيات الضارة، والهندسة العكسية، والمعلومات الاستباقية المتعلقة بالتهديدات.



شكل ٣٥: الخريطة الوظيفية لأخصائيّ الهندسة العكسية للبرمجيات الضارة

١,١٢,٥ أخصائي الهندسة العكسية للبرمجيات الضارة من المستوى الثالث

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي الهندسة العكسية للبرمجيات الضارة (PD-IR-004)	المستوى الثالث

وصف الدور الوظيفي	ممارس أول يقوم بفك شفرة البرمجيات الضارة وإعادتها إلى صيغة برمجية مفهومة، بهدف فهم كيفية عملها وأثرها ونوايا الجهات المهاجمة، ويوصي بأساليب الحد من مخاطر الحوادث وإجراءات الاستجابة لها. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالعمل لمراجعتها والعمل تحت إشراف أخصائي الهندسة العكسية للبرمجيات الضارة من المستوى الرابع. تشمل المهمات تحديد أدوات الهندسة العكسية وتطويرها لتعزيز القدرات وكشف الثغرات ومراجعة تهديدات الأمن السيبراني وتحليلها، لتزويد أصحاب المصلحة بالمعلومات اللازمة للاستجابة للتهديدات

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية:	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية:
• مطور الأمن السيبراني من المستوى الثالث	• أخصائي الهندسة العكسية للبرمجيات الضارة من المستوى الرابع • مطور الأمن السيبراني من المستوى الثالث

جدول ١١٤: أخصائي الهندسة العكسية للبرمجيات الضارة من المستوى الثالث

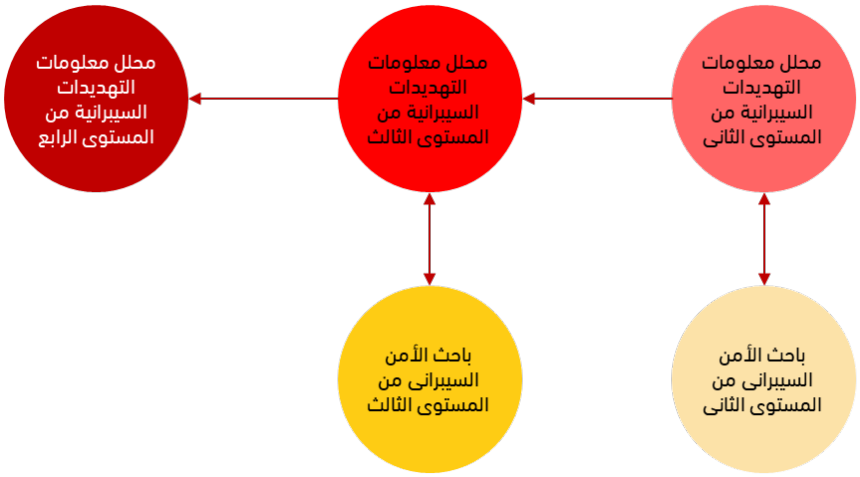
٢,١٢,٥ أخصائي الهندسة العكسية للبرمجيات الضارة من المستوى الرابع

مسمى الدور الوظيفي: أخصائي الهندسة العكسية للبرمجيات الضارة (PD-IR-004)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً لتحليل البرمجيات الضارة، وفهم كيفية عملها، وتأثيرها، ونوايا الجهات المهاجمة، والتوصية بأساليب الحد من مخاطر الحوادث وإجراءات الاستجابة لها. يتحمل الفرد في هذا الدور مسؤولية الإشراف على الكثير من أعمال أخصائي الهندسة العكسية للبرمجيات الضارة من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تشمل المهمات تقديم المعلومات الاستباقية للدعم الاستخباراتي الحالي لأصحاب المصلحة الداخلية / الخارجية الهامة حسب الاقتضاء، وتقديم إشعارات في الوقت المناسب بنوايا الجهات المهاجمة المهمة، أو الأنشطة التي قد تؤثر على أهداف المنظمة أو مواردها أو قدراتها.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي الهندسة العكسية للبرمجيات الضارة من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ١١٥: أخصائي الهندسة العكسية للبرمجيات الضارة من المستوى الرابع

١٣,٥ محلّل معلومات التهديدات السيبرانية

يقوم محلل معلومات التهديدات السيبرانية بجمع وتحليل المعلومات ذات المصادر المتعددة وتحليلها؛ لتطوير فهم عميق لتهديدات الأمن السيبراني والأساليب والتقنيات والإجراءات الخاصة بجهات التهديد. يعنى هذا الدور بتحليل مؤشرات الاختراق وتحديده (IOCs) لإعطاء المؤسسات قدرة استباقية على كشف التهديدات السيبرانية والتصدي لها، مما يضمن بيئة رقمية أكثر أمانًا وحماية أقوى للنظم والشبكات. يتطلب هذا العمل مؤهلات متقدمة أو تدريبًا متخصصًا في المعلومات الاستباقية، وتحليل الأساليب والتقنيات المستخدمة في الهجمات (TTP) بالإضافة إلى تطوير مؤشرات الاختراق (IOC) لتعزيز الدفاعات الرقمية.



شكل٣٦ : الخريطة الوظيفية لمحلل معلومات التهديدات السيبرانية

١,١٣,٥ محلل معلومات التهديدات السيبرانية من المستوى الثاني

مسمى الدور الوظيفي: محلّل معلومات التهديدات السيبرانية (PD-TM-001)	المستوى الوظيفي: المستوى الثاني
وصف الدور الوظيفي	يقوم الممارس بجمع المعلومات ذات المصادر المتعددة المصادر حول التهديدات السيبرانية وتحليلها لتطوير الفهم العميق والوعي بالتهديدات السيبرانية وأساليب الجهات الفاعلة وأساليبها وإجراءاتها، واستخلاص المؤشرات التي تساعد المؤسسات على اكتشاف الحوادث السيبرانية والتنبؤ بها وحماية النُظم والشبكات من التهديدات السيبرانية وإعداد التقارير بشأنها. يقوم الفرد في هذا الدور بتنفيذ بعض المهمات الأساسية لهذا العمل ويواصل تطوير مهاراته من خلال التطبيق العملي، تتضمن المهمات مراقبة المواقع ذات المصدر المفتوح لرصد أي محتوى عدائي موجّه ضد مصالح المنظمة أو شركائها، إضافةً إلى متابعة أنشطة الجهات المهددة والإبلاغ عنها لتلبية متطلبات المعلومات الاستباقية للتهديدات والتقارير الخاصة بالمنظمة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية • باحث الأمن السيبراني من المستوى الثاني	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • محلل معلومات التهديدات السيبرانية من المستوى الثالث • باحث الأمن السيبراني من المستوى الثاني

جدول ١١٦: محلل معلومات التهديدات السيبرانية من المستوى الثاني

٢,١٣,٥ محلل معلومات التهديدات السيبرانية من المستوى الثالث

مسمى الدور الوظيفي:	المستوى الوظيفي:
محلّل معلومات التهديدات السيبرانية (PD-TM-001)	المستوى الثالث

وصف الدور الوظيفي	ممارس أول يتولى إدارة الفريق أو توجيه الآخرين عن جمع معلومات عن التهديدات السيبرانية من مصادر مختلفة وتحليلها لتكوين فهم وإدراك عميقين للتهديدات السيبرانية، والخطط والأساليب والإجراءات التي يتبعها المخترقون، لاستنباط مؤشرات من شأنها مساعدة المؤسسات في الكشف عن الحوادث السيبرانية وتوثيقها والتنبؤ بها، وحماية النُظم والشبكات من التهديدات السيبرانية. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالعمل لمراجعتها والعمل تحت إشراف محلّل معلومات التهديدات السيبرانية من المستوى الرابع. تشمل المهمات تنسيق مصادر المعلومات الاستباقية الخاصة بالتهديدات السيبرانية والتحقق منها وإدارتها، وتغذية وتحديد الفجوات في المعلومات الاستباقية المتعلقة بالتهديدات، وتقييم آثارها على المنظمة.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية:	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية:
• محلل معلومات التهديدات السيبرانية من المستوى الثاني • باحث الأمن السيبراني من المستوى الثالث	• محلل معلومات التهديدات السيبرانية من المستوى الرابع • باحث الأمن السيبراني من المستوى الثالث

جدول ١١٧: محلل معلومات التهديدات السيبرانية من المستوى الثالث

٣,١٣,٥ محلل معلومات التهديدات السيبرانية من المستوى الرابع

مسمى الدور الوظيفي:	المستوى الوظيفي:
محلّل معلومات التهديدات السيبرانية (PD-TM-001)	المستوى الرابع

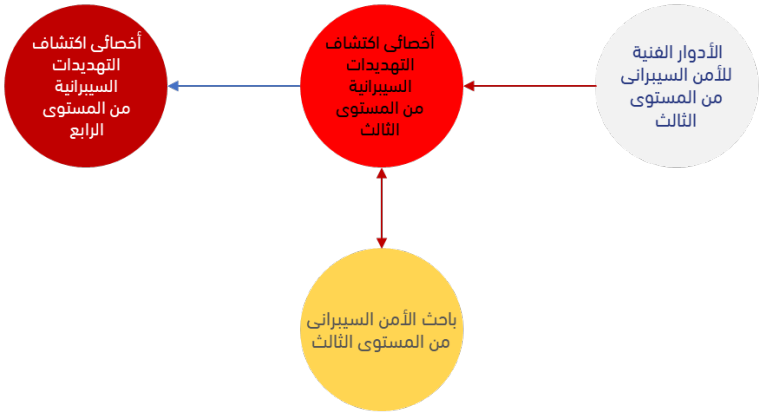
وصف الدور الوظيفي	خبير يدير وحدةً لإدارة تعنى بجمع المعلومات وتحليلها ذات مصادر متعددة عن تهديدات الأمن السيبراني لتطوير الفهم العميق والوعي بالتهديدات السيبرانية وأساليب الجهات الفاعلة وأساليبها وإجراءاتها، واستخلاص المؤشرات التي تساعد المؤسسات على اكتشاف الحوادث السيبرانية والتنبؤ بها وحماية النُظم والشبكات من التهديدات السيبرانية والإبلاغ عنها. يتحمل الفرد في هذا الدور مسؤولية الإشراف على معظم أعمال محلّل معلومات التهديدات السيبرانية من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تشمل المهمات تقديم الدعم المتواصل من خلال توفير المعلومات لأصحاب المصلحة الداخلية/الخارجية المهمة حسب الاقتضاء، وإعداد ملخصات وتقديمها عن التهديدات المحددة التي تواجه المنظمة.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • محلل معلومات التهديدات السيبرانية من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ١١٨: محلّل معلومات التهديدات السيبرانية من المستوى الرابع

١٤,٥ أخصائي اكتشاف التهديدات السيبرانية

يبحث أخصائي اكتشاف التهديدات السيبرانية عن التهديدات غير المكتشفة بشكل استباقي داخل النُظم والشبكات، ويحدد مؤشرات الاختراق، ويوصي بإستراتيجيات فعالة للحد منها. يتطلب هذا العمل الحصول على شهادات أو تدريب في مجال البحث عن التهديدات السيبرانية، والاستجابة المتقدمة للحوادث، والتحليل الجنائي الرقمي.



شكل٣٧ : الخريطة الوظيفية لأخصائي اكتشاف التهديدات السيبرانية

١,١٤,٥ أخصائي اكتشاف التهديدات السيبرانية من المستوى الثالث

مسمى الدور الوظيفي: أخصائي اكتشاف التهديدات السيبرانية (PD-TM-002)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يقوم بالبحث الاستباقي عن التهديدات غير المكتشفة في الشبكات والنُظم، وتحديد مؤشرات الاختراق، وتقديم التوصيات عن خطط التعامل معها. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالدور الوظيفي لمراجعتها والعمل تحت إشراف أخصائي اكتشاف التهديدات السيبرانية من المستوى الرابع. تشمل المسؤوليات فحص بيانات السجلات وتحليلها من مصادر مختلفة لرصد أي تهديدات أمنية قد تستهدف الشبكة، مع تتبع الأنشطة الضارة؛ لكشف نقاط الضعف المستغلة، وأساليب الهجوم المستخدمة، ومدى تأثيرها على النُظم والمعلومات الحساسة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • باحث الأمن السيبراني من المستوى الثالث • الأدوار الفنية للأمن السيبراني من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي اكتشاف التهديدات السيبرانية من المستوى الرابع • باحث الأمن السيبراني من المستوى الثالث

جدول ١١٩: أخصائي اكتشاف التهديدات السيبرانية من المستوى الثالث

٢,١٤,٥ أخصائي اكتشاف التهديدات السيبرانية من المستوى الرابع

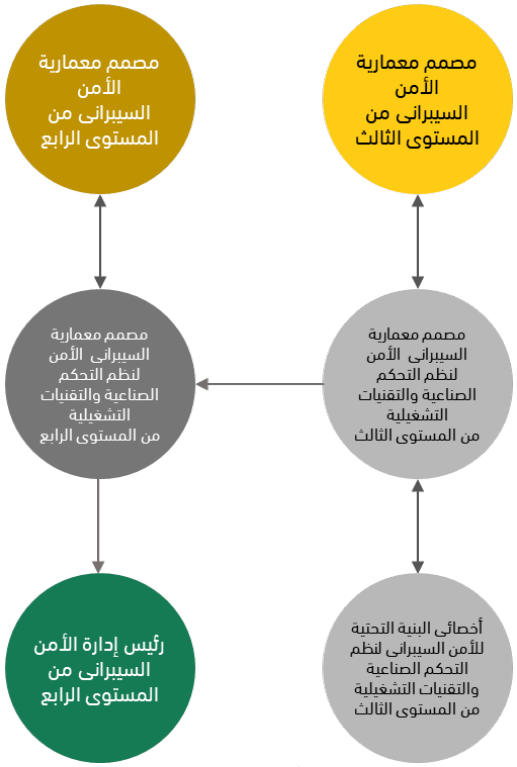
مسمى الدور الوظيفي: أخصائي اكتشاف التهديدات السيبرانية (PD-TM-002)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً للبحث بشكل استباقي عن التهديدات غير المكتشفة في الشبكات والنُظم، وتحديد مؤشرات الاختراق والتوصية بخطط الحد من آثارها. سيتولى الفرد في هذا الدور مسؤولية الإشراف على معظم أعمال أخصائي اكتشاف التهديدات السيبرانية من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تتضمن المهمات تعزيز الوعي بقضايا الأمن السيبراني مع الإدارة العليا لضمان دمج الأمن السيبراني ضمن الأهداف الإستراتيجية للمؤسسة، بالإضافة إلى إنشاء قنوات اتصال فعالة والحفاظ عليها مع أصحاب المصلحة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي اكتشاف التهديدات السيبرانية من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي أي دور من الأدوار الوظيفية في مجال تخصص القيادة من المستوى الرابع.

جدول ١٢٠: أخصائي اكتشاف التهديدات السيبرانية من المستوى الرابع

٦ نظم التحكم الصناعية والتقنيات التشغيلية (ICS/OT)

١,٦مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية

يقوم مصمم معمارية الأمن السيبراني بتصميم نظم التحكم الصناعية والتقنيات التشغيلية ويشرف على تطوير نظم وشبكات الأمن السيبراني وإعدادها وتنفيذها في بيئات نظم التحكم الصناعية (ICS) والتقنيات التشغيلية (OT). ويتطلب هذا العمل الحصول على شهادات أو تدريب في مجال الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية، وتصميم البنية التحتية الآمنة، وإدارة المخاطر، والإعدادات الآمنة، وتقييم مخاطر الأمن السيبراني، التعافي من الكوارث، ودمج الأمن في بيئات نظم التحكم الصناعية والتقنيات التشغيلية.



شكل٣٨ : الخريطة الوظيفية لمصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية

١,١,٦مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث

مسمى الدور الوظيفي: مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية (ICSOT- ICSOT-001)	المستوى الوظيفي: المستوى الثالث
وصف الدور الوظيفي	ممارس أول يقوم بتصميم نظم الأمن السيبراني وشبكاته في بيئة نظم التحكم الصناعية والتقنيات التشغيلية والإشراف على إعداداتها وتطويرها وتنفيذها. سوف يتولى الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالدور الوظيفي لمراجعتها من قبل مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية في المستوى الرابع والعمل تحت إشرافه. تشمل المهمات ترجمة المفاهيم والقدرات المقترحة لنظم التحكم الصناعية (ICS) والتقنيات التشغيلية (OT) إلى حلول تقنية قابلة للتنفيذ، مع العمل جنبًا إلى جنب مع الفرق بشكل مرن، لتطوير نماذج أولية سريعة، وإجراء دراسات جدوى، واستكشاف إمكانيات التقنيات الحديثة؛ لتعزيز الكفاءة التشغيلية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مصمم معمارية الأمن السيبراني من المستوى الثالث • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • مصمم معمارية الأمن السيبراني نظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع • مصمم معمارية الأمن السيبراني من المستوى الثالث • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث

جدول ١٢١: مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث

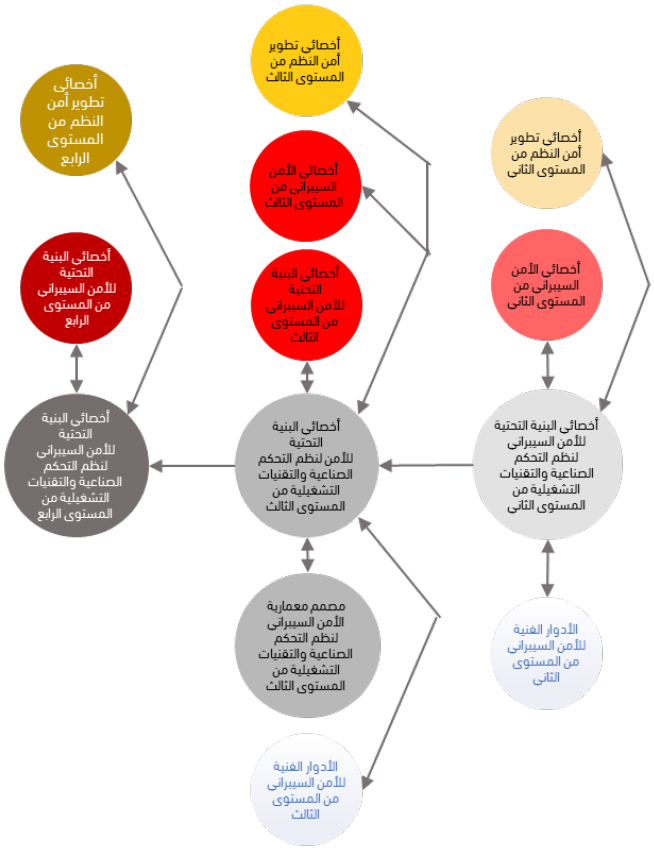
٢,١,٦ مصمم معمارية الأمن السيبراني نظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع

مسمى الدور الوظيفي:	المستوى الوظيفي:
مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية (ICSOT- ICSOT-001)	المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً لتصميم نظم الأمن السيبراني وشبكاته، والإشراف على إعداداتها وتطويرها وتنفيذها. سيتولى الفرد في هذا الدور الوظيفي مسؤولية الإشراف على الكثير من أعمال مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة ضمن الأطر الزمنية ذات الصلة. تشمل المسؤوليات وضع إستراتيجية واضحة لاستعادة نظم التحكم الصناعية والتقنيات التشغيلية بعد الكوارث، من خلال تحديد أولويات الوظائف التشغيلية الحيوية وترتيبها. كما تتطلب ضمان توافق النُظم والمعماريات المكتسبة أو المطورة مع معايير الأمن السيبراني الخاصة بالمنظمة، لضمان استمرارية الأعمال وتعزيز المرونة التشغيلية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • مصمم معمارية الأمن السيبراني من المستوى الرابع	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • رئيس إدارة الأمن السيبراني من المستوى الرابع • مصمم معمارية الأمن السيبراني من المستوى الرابع

جدول ١٢٢: مصمم معمارية الأمن السيبراني نظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع

٢,٦ أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية

يقوم أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية بتنصيب الأجهزة والبرمجيات واختبارها وتشغيلها وصيانتها وإداراتها، وذلك لحماية النُظم والشبكات والدفاع عنها ضد التهديدات السيبرانية في بيئات نظم التحكم الصناعية والتقنية التشغيلية. ويتطلب هذا العمل الحصول على شهادات، أو تدريب في مجال الأمن السيبراني في نظم التحكم الصناعية والتقنيات التشغيلية، وإدارة النُظم والشبكات، وإدارة البنية التحتية للأمن السيبراني في نظم التحكم الصناعية والتقنيات التشغيلية، وتنفيذ الضوابط الأمنية، وتشغيل الأجهزة/البرمجيات.



شكل ٣٩: الخريطة الوظيفية لأخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية

١,٢,٦ أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية (ICSOT-ICSOT-002)	المستوى الثاني

وصف الدور الوظيفي	ممارس يعمل على تشغيل الأجهزة والبرمجيات واختبارها وصيانتها وإداراتها، وهي الأجهزة التي تحمي النُظم والشبكات وتحميها وتدافع عنها ضد التهديدات السيبرانية في بيئات نظم التحكم الصناعية والتقنيات التشغيلية. يقوم الفرد في هذا الدور بتنفيذ بعض المهمات الأساسية لهذا العمل ويواصل تطوير مهاراته من خلال التطبيق العملي، تشمل المهمات تنفيذ أعمال الاستجابة للحوادث لدعم فرق الاستجابة للحوادث القابلة للنشر، بما في ذلك جمع الأدلة الجنائية، وربط الهجمات السيبرانية وتتبعها، وتحليل التهديدات، وإصلاح النظام وتقييم فعالية ضوابط الأمن السيبراني.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية • الأدوار الفنية للأمن السيبراني من المستوى الثاني • أخصائي الأمن السيبراني من المستوى الثاني • أخصائي تطوير أمن النُظم من المستوى الثاني	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • أخصائي الأمن السيبراني من المستوى الثاني • أخصائي تطوير أمن النُظم من المستوى الثاني

جدول ١٢٣: أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني

٢,٢,٦ أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية (ICSOT-ICSOT-002)	المستوى الثالث

وصف الدور الوظيفي	ممارس أول يتولى إدارة الفريق أو توجيه الآخرين حول صيانة الأجهزة والبرمجيات المستخدمة للدفاع وفحصها وتنصيبها وحماية النُظم والشبكات من التهديدات السيبرانية في بيئة نظم التحكم الصناعية والتقنيات التشغيلية وتشغيلها والإشراف عليها. سوف يتولى الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالعمل لمراجعتها من قبل أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع والعمل تحت إشرافه. تشمل المهمات اختيار الضوابط الأمنية لنظم التحكم الصناعية والتقنيات التشغيلية وتوثيق الوصف الوظيفي للتنفيذ في خطة أمنية وتنفيذ ضوابط التحكم الصناعية والتقنيات التشغيلية المحددة في خطة أمنية أو وثائق أخرى للنظام.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية:	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية:
• أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني • الأدوار الفنية للأمن السيبراني من المستوى الثالث • أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث • أخصائي الأمن السيبراني من المستوى الثالث • مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • أخصائي تطوير أمن النُظم من المستوى الثالث	• أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع • أخصائي البنية التحتية للأمن السيبراني من المستوى الثالث • أخصائي الأمن السيبراني من المستوى الثالث • مصمم معمارية الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • أخصائي تطوير أمن النُظم من المستوى الثالث

جدول ١٢٤: أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث

٣,٢,٦ أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية (ICSOT-ICSOT-002)	المستوى الرابع

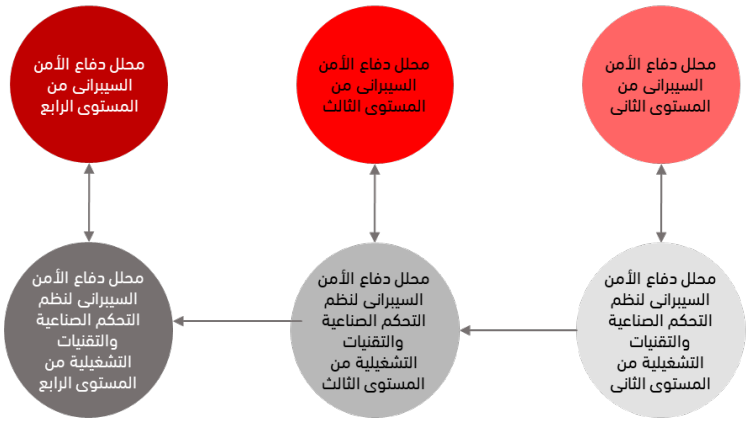
وصف الدور الوظيفي	خبير يدير وحدةً، تعنى بتنصيب الأجهزة والبرمجيات واختبارها وتشغيلها وصيانتها وكذلك إدارة الأجهزة والبرمجيات التي تحمي النُظم والشبكات وتدافع عنها ضد الهجمات السيبرانية في بيئات نظم التحكم الصناعية والتقنيات التشغيلية. يتحمل الفرد في هذا الدور مسؤولية الإشراف على معظم أعمال أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. سوف تشمل الأعمال التعاون مع أصحاب المصلحة لضمان تلبية برامج استمرارية الأعمال والتعافي من الكوارث للمتطلبات التنظيمية وتعزيز قيمة الأمن السيبراني وإظهارها لأصحاب المصلحة داخل المنظمة.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • أخصائي البنية التحتية للأمن السيبراني من المستوى الرابع • أخصائي تطوير أمن النُظم من المستوى الرابع	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الاتية: • أخصائي البنية التحتية للأمن السيبراني من المستوى الرابع • أخصائي تطوير أمن النُظم من المستوى الرابع

جدول ١٢٥: أخصائي البنية التحتية للأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع

٣,٦ محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية

يقوم محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية باستخدام البيانات، التي جرى جمعها من مجموعة متنوعة من أدوات الأمن السيبراني لتحليل الأحداث الواقعة في بيئة نظم التحكم الصناعية والتقنيات التشغيلية بهدف الكشف عن التهديدات السيبرانية والتعامل معها. ويتطلب هذا العمل الحصول على شهادات، أو تدريب في مجال الأمن السيبراني في نظم التحكم الصناعية والتقنيات التشغيلية، والدفاع عن الشبكات، وكشف التهديدات، وتحليل الحوادث، وأدوات مراقبة الأمن السيبراني المصممة خصيصًا لبيئات التحكم الصناعية والتقنيات التشغيلية.



شكل ٤٠: الخريطة الوظيفية لمحلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية

١,٣,٦ محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني

مسمى الدور الوظيفي:	المستوى الوظيفي:
محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية (ICSOT-ICSOT-003)	المستوى الثاني

وصف الدور الوظيفي	يستخدم الممارس البيانات التي جرى جمعها من مجموعة متنوعة من أدوات الأمن السيبراني لتحليل الأحداث التي داخل بيئات نظم التحكم الصناعية والتقنيات التشغيلية للكشف عن مهددات الأمن السيبراني والحد منها. يقوم الفرد في هذا الدور بتنفيذ بعض المهمات الأساسية لهذا العمل ويواصل تطوير مهاراته من خلال التطبيق العملي، تتضمن المهمات ربط المعلومات المستمدة من مصادر متعددة لفهم السياق وتقييم فعالية الهجوم المرصود، بالإضافة إلى الكشف الفوري عن الهجمات المحتملة، والأنشطة غير الطبيعية، وحالات إساءة الاستخدام، وإصدار التنبيهات اللازمة، مع التمييز بين الأنشطة الضارة والأنشطة العادية.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية • محلل دفاع الأمن السيبراني من المستوى الثاني	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • محلل دفاع الأمن السيبراني من المستوى الثاني

جدول ١٢٦: محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني

٢,٣,٦ محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث

مسمى الدور الوظيفي:	المستوى الوظيفي:
محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية (ICSOT-ICSOT-003)	المستوى الثالث
وصف الدور الوظيفي	ممارس يقوم باستخدام البيانات التي جرى جمعها من مجموعة متنوعة من أدوات الأمن السيبراني لتحليل الأحداث التي تجري داخل بيئات نظم التحكم الصناعية والتقنيات التشغيلية للكشف عن تهديدات الأمن السيبراني والحد من آثارها. سيتولى الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالدور الوظيفي؛ لمراجعتها من قبل محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع والعمل تحت إشرافه. تشمل المهمات إجراء مراجعات الأمن السيبراني وتحديد الفجوات الأمنية في البنية الأمنية لتوجيه إستراتيجيات الحد من المخاطر وتحديد المؤشرات والتحذيرات من خلال البحث والتحليل والارتباط عبر مجموعات البيانات المتعددة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني • محلل دفاع الأمن السيبراني من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع • محلل دفاع الأمن السيبراني من المستوى الثالث

جدول ١٢٧: محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث

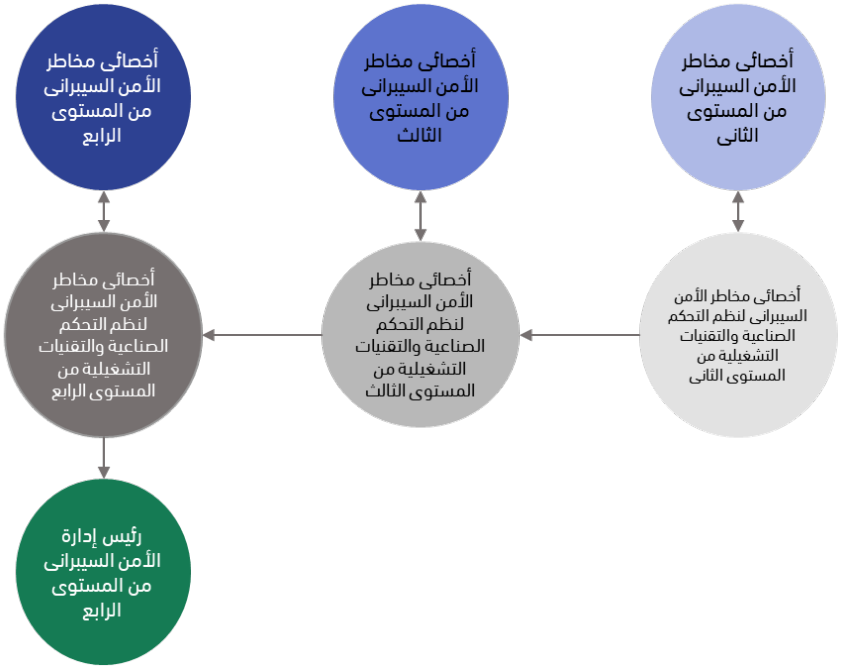
٣,٣,٦ محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع

مسمى الدور الوظيفي: محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية (ICSOT-ICSOT-003)	المستوى الوظيفي: المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً لاستخدام البيانات التي جرى جمعها من مجموعة متنوعة من أدوات الأمن السيبراني لتحليل الأحداث التي تجري داخل بيئات التحكم الصناعية والتقنيات التشغيلية للكشف عن التهديدات السيبرانية والحد منها. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تشمل المهمات تقديم توصيات بشأن الأمن السيبراني إلى القيادة؛ استنادًا إلى التهديدات والثغرات الكبيرة والعمل مع أصحاب المصلحة لحل حوادث الأمن السيبراني وقضايا الالتزام الخاصة بالثغرات الأمنية.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • محلل دفاع الأمن السيبراني من المستوى الرابع	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • محلل دفاع الأمن السيبراني من المستوى الرابع

جدول ١٢٨: محلل دفاع الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع

٤,٦ أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية

يقوم أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية بإدارة مخاطر الأمن السيبراني وتحديدها وتقييمها، وذلك ضمن بيئات نظم التحكم الصناعية والتقنيات التشغيلية. يتضمن العمل تقييم فاعلية ضوابط الأمن السيبراني الحالية وتقديم ملحوظات وتوصيات قابلة للتنفيذ. تعد الشهادات أو التدريب في مجال الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية وحوكمة الأمن السيبراني والالتزام وتقييم التهديدات الخاصة ببيئات نظم التحكم الصناعية والتقنيات التشغيلية ضروريةً لهذا لمنصب.



شكل ٤١: الخريطة الوظيفية لأخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية

١,٤,٦ أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية (ICSOT- ICSOT-004)	المستوى الثاني
وصف الدور الوظيفي	ممارس يقوم بتحديد مخاطر الأمن السيبراني وتقييمها وإداراتها في بيئات نظم التحكم الصناعية والتقنيات التشغيلية والعمل على تقييم فاعلية ضوابط الأمن السيبراني الحالية وتحليلها، وتقديم الملحوظات والتوصيات بناءً على التقييمات. يقوم الفرد في هذا الدور بتنفيذ بعض المهمات الأساسية لهذا العمل، ويواصل تطوير مهاراته من خلال التطبيق العملي، تتضمن المهمات تقديم مدخلات لإطار إدارة المخاطر والوثائق ذات الصلة وإجراء تقييمات لمخاطر الأمن السيبراني.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • الخريج الحاصل على المستوى الثاني من المؤهلات العلمية • أخصائي مخاطر الأمن السيبراني من المستوى الثاني	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • أخصائي مخاطر الأمن السيبراني من المستوى الثاني

جدول ١٢٩: أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني

٢,٤,٦ أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية (ICSOT- ICSOT-004)	المستوى الثالث

وصف الدور الوظيفي	ممارس أول يقوم بإدارة مخاطر الأمن السيبراني وتقييمها وتحديدها في بيئات نظم التحكم الصناعية والتقنيات التشغيلية وتقييم وتحليل فاعلية ضوابط الأمن السيبراني الحالية وتقديم الملحوظات والتوصيات، بناءً على التقييمات. سيتولى الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بهذا الدور، والعمل تحت إشراف أخصائي مخاطر الأمن السيبراني ومراجعته في نظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع تتضمن المهمات ضمان تحديد المخاطر السيبرانية وإدارتها بشكل مناسب من خلال عملية حوكمة المخاطر في المنظمة، بالإضافة إلى التعاون مع المسؤولين في المنظمة لضمان أن بيانات أدوات المراقبة المستمرة توفر رؤية واضحة حول مستويات المخاطر.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثاني • أخصائي مخاطر الأمن السيبراني من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع • أخصائي مخاطر الأمن السيبراني من المستوى الثالث

جدول ١٣٠: أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث

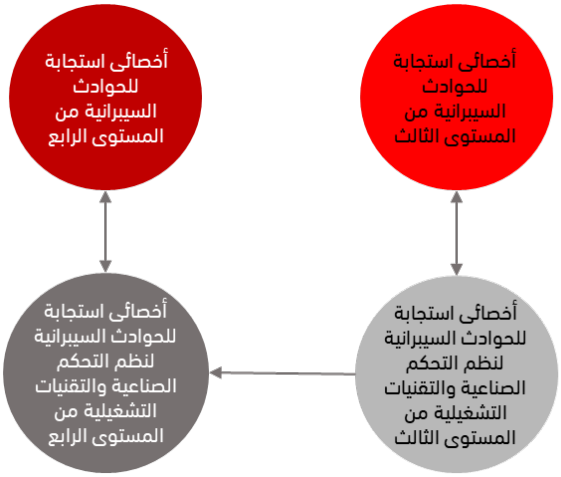
٣,٤,٦ أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية (ICSOT-004 -ICSOT)	المستوى الرابع
وصف الدور الوظيفي	خبير يدير وحدةً لتحديد مخاطر الأمن السيبراني وتقييمها وإداراتها في بيئات نظم التحكم الصناعية والتقنيات التشغيلية وتقييم فاعلية ضوابط الأمن السيبراني الحالية وتحليلها، وتقديم الملحوظات والتوصيات بناءً على التقييمات. سيتولى الفرد في هذا الدور الوظيفي مسؤولية الإشراف على معظم أعمال أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. وتشمل المهمات ضمان كون القرارات المتعلقة بالأمن السيبراني تستند إلى مبادئ سليمة لإدارة المخاطر ووضع استراتيجية لإدارة المخاطر للمؤسسة تتضمن تحديد مدى تحمل المخاطر.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • أخصائي مخاطر الأمن السيبراني من المستوى الرابع	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي مخاطر الأمن السيبراني من المستوى الرابع • رئيس إدارة الأمن السيبراني من المستوى الرابع

جدول ١٣١: أخصائي مخاطر الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع

٥,٦ أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية

يقوم أخصائي استجابة للحوادث السيبرانية بمباشرة حوادث الأمن السيبراني وتحليلها والاستجابة لها في بيئات نظم التحكم الصناعية والتقنيات التشغيلية. يتطلب هذا العمل الحصول على شهادات، أو تدريب في مجال الأمن السيبراني لنظم التحكم الصناعية والتقنيات التشغيلية، والتعامل مع الحوادث والاستجابة لها، والتحليل الجنائي الرقمي، وتحليل البرامج الضارة، ومراقبة أمن الشبكات، وعمليات مركز العمليات الأمنية.



شكل٤٢ : الخريطة الوظيفية لأخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية

١,٥,٦ أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث

اسم الدور الوظيفي:	المستوى الوظيفي:
أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية (ICSOT-ICSOT-005)	المستوى الثالث
وصف الدور الوظيفي	ممارس أول، يقوم بمباشرة حوادث الأمن السيبراني وتحليلها والاستجابة لها. يتحمل الفرد في هذا الدور مسؤولية تنفيذ المهمات المعقدة المتعلقة بالدور الوظيفي والعمل تحت إشراف ومراجعة أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع ICS/OT. تتضمن المهمات تطبيق مبادئ الدفاع ذات الطبقات المتعددة وفقًا لسياسات المنظمة وكذلك الممارسات، وذلك إضافةً إلى جمع الأدلة الرقمية للاختراقات واستخدام البيانات المكتشفة للحد من حوادث الأمن السيبراني المحتملة داخل المنظمة.
التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية: • أخصائي استجابة للحوادث السيبرانية من المستوى الثالث	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية: • أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع • أخصائي استجابة للحوادث السيبرانية من المستوى الثالث

جدول ١٣٢: أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث

٢,٥,٦ أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع

مسمى الدور الوظيفي:	المستوى الوظيفي:
أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية (ICSOT-ICSOT-005)	المستوى الرابع

وصف الدور الوظيفي	خبير يدير وحدةً للتحقيق في حوادث الأمن السيبراني وتحليلها والاستجابة لها. يتحمل الفرد في هذا الدور الوظيفي مسؤولية الإشراف على الكثير من أعمال أخصائي استجابة للحوادث السيبرانية من المستوى الثالث، وضمان اكتمالها وفقًا للمعايير المناسبة وضمن الأطر الزمنية ذات الصلة. تشمل المهمات كتابة تقنيات الدفاع السيبراني ونشرها والتوجيه، وكذلك مشاركة تقارير ما بعد الحادث مع الدوائر المعنية والعمل بوصفه خبيرًا فنيًا في دعم إنفاذ القانون، وشرح تفاصيل الحوادث وتحليل الأدلة الجنائية حسب الحاجة.

التقدم الوظيفي (المسار)	
سيكون الفرد قد انتقل من الأدوار الوظيفية الآتية:	الخطوة الوظيفية اللاحقة للفرد في هذا الدور الوظيفي، هي واحدة من الخطوات الآتية:
• أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الثالث • أخصائي استجابة للحوادث السيبرانية من المستوى الرابع	• أخصائي استجابة للحوادث السيبرانية من المستوى الرابع

جدول ١٣٣: أخصائي استجابة للحوادث السيبرانية لنظم التحكم الصناعية والتقنيات التشغيلية من المستوى الرابع


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority