الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

الإطار التنظيمي لترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدَار

Regulatory Framework for Licensing Managed Security Operations Center (MSOC) Services
(RFMSOC-1:2024)

إشارة المشاركة: أبيض
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 – 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.

أبيض – غير محدود

قائمة المحتويات

الصفحة

١. المقدمة

تُعد الهيئة الوطنية للأمن السيبراني؛ بموجب تنظيمها الصادر بالأمر الملكي الكريم ذي الرقم (٦٨٠١) في ١٤٣٩/٢/١١هـ الجهة المختصّة في المملكة بالأمن السيبراني، والمرجع الوطني في شؤونه. وتهدف إلى تعزيزه؛ حمايةً للمصالح الحيوية للدولة، وأمنها الوطني، والبنى التحتية الحساسة، والقطاعات ذات الأولوية، والخدمات والأنشطة الحكومية. وتشمل اختصاصات الهيئة ومهماتها وضع السياسات وآليات الحوكمة، والأطر، والمعايير، والضوابط، والإرشادات المتعلقة بالأمن السيبراني، وتعميمها على الجهات ذات العلاقة، ومتابعة الالتزام بها، وتحديثها، والترخيص بمزاولة الأفراد والجهات غير الحكومية، للأنشطة، والعمليات المتعلقة بالأمن السيبراني، التي تحددها الهيئة، وتحفيز نمو قطاع الأمن السيبراني في المملكة، وتشجيع الابتكار والاستثمار فيه.

ولأهمية خدمات مركز عمليات الأمن السيبراني المُدَار، في تعزيز الأمن السيبراني للجهات الوطنية، ولوجود حاجة إلى إرساء أطر، ومعايير واضحة؛ تحدد نطاق هذا النوع من الخدمات، والالتزامات الواقعة على مقدم الخدمة، ولتحقيق إستراتيجية الهيئة في مرحلتها الثانية (2.0)؛ فقد أصدرت الهيئة الوطنية للأمن السيبراني هذا الإطار؛ بهدف الترخيص لتقديم خدمات مركز عمليات الأمن السيبراني المُدار، والذي يبين المسؤوليات والالتزامات، الواقعة على المرخص له، عند تقديم هذا النوع من الخدمات؛ إضافة إلى قصر تقديمها على جهات مؤهلة لذلك. كما شمل الإطار متطلبات التأهيل للأفراد للعمل بوصفهم محللي مراكز عمليات الأمن السيبراني المُدارة.

٢. التعريفات

يكون للمصطلحات المستخدمة في هذا الإطار المعاني المبينة أمام كل منها؛ ما لم يقتض السياق خلاف ذلك:

المصطلح	التعريف
الهيئة	الهيئة الوطنية للأمن السيبراني.
الجهات	هي الجهات الحكومية، أو الخاصة الربحية، أو غير الربحية، أو أي شكل آخر من أشكال الجهات.
الإطار	هو الإطار التنظيمي لترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدَار، الصادر عن الهيئة.
البنية التحتية الوطنية الحساسة	هي تلك العناصر الأساسية للبنية التحتية، أي (الأصول، والمرافق، والنظم، والشبكات، والعمليات، والعاملون الأساسيون الذين يقومون بتشغيلها ومعالجتها) والتي قد يؤدي فقدانها أو تعرضها لانتهاكات أمنية إلى: ١- أثر سلبي كبير على توافر الخدمات الأساسية، أو تكاملها، أو تسليمها، بما في ذلك الخدمات التي يمكن أن تؤدي في حال تعرضت سلامتها للخطر؛ إلى خسائر كبيرة في الممتلكات و/ أو الأرواح و/ أو الإصابات، مع مراعاة الآثار الاقتصادية و/ أو الاجتماعية الكبيرة. ٢- تأثير كبير على الأمن الوطني و/ أو الدفاع الوطني و/ أو اقتصاد الدولة أو مقدراتها الوطنية.
مركز عمليات الأمن السيبراني	هو مركز يقدم خدمات العمليات، المتعلقة بمراقبة أحداث الأمن السيبراني في المنظومة التقنية للجهة، وتؤدي إلى اكتشاف التهديدات السيبرانية، ومعرفة كيفية حدوثها، وتقديم التوصيات في كيفية معالجتها، واتخاذ الإجراءات اللازمة لاحتوائها.
خدمات مركز عمليات الأمن السيبراني المُدَار	هي الخدمات التي تحصل عليها الجهة المستفيدة من مقدم الخدمة؛ بهدف مراقبة أحداث الأمن السيبراني في المنظومة التقنية لديها؛ لاكتشاف التهديدات السيبرانية، ومعرفة كيفية حدوثها، وتقديم التوصيات في كيفية معالجتها، ليتم تطبيقها من قبل الجهة المستفيدة. وتشمل هذه الخدمات؛ العمليات، وفرق العمل، والأنظمة ذات الصلة، وغيرها.
الترخيص	هو وثيقة تُصدرها الهيئة؛ تسمح بموجبها لمقدم الخدمة بممارسة نشاط تقديم خدمات مركز عمليات الأمن السيبراني المُدَار في المملكة؛ وذلك وفقًا لما تُحدّده الهيئة.
مقدم الخدمة	الجهة المرخصة من الهيئة، لتقديم خدمات مركز عمليات الأمن السيبراني المُدار في المملكة؛ وفقًا للإطار.
الجهة المستفيدة	هي الجهة التي تتعاقد مع مقدم الخدمة، بهدف الحصول على خدمات مركز عمليات الأمن السيبراني المُدَار.
مقدم خدمة الحوسبة السحابية	أي شخص طبيعي، أو معنوي (مثل الشركات) مرخص من الجهة المختصة في المملكة بتقديم خدمات الحوسبة السحابية إلى العموم، سواء أكان ذلك بشكل مباشر، أو غير مباشر؛ من خلال مراكز بيانات (سواء أكانت داخل المملكة أو خارجها) ويديرها بنفسه بشكل كلي أو جزئي.
السياسة	السياسة الوطنية لمراكز عمليات الأمن السيبراني المُدَارة، الصادرة عن الهيئة.
شهادة التأهيل	هي وثيقة تصدرها الهيئة لشخص طبيعي، تقضي بأهليته للعمل محللاً في مراكز عمليات الأمن السيبراني المُدَارة لدى مقدم الخدمة.
محلل مركز عمليات الأمن السيبراني المُدَار	أي شخص طبيعي، حاصل على شهادة تأهيل، للعمل محللاً في مركز عمليات الأمن السيبراني المُدَار.

٣. أهداف الإطار

يهدف الإطار التنظيمي لترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدَار؛ إلى تنظيم تقديم هذه الخدمات؛ من خلال إطار عمل واضح، يحدد المسؤوليات، والالتزامات على المرخص له؛ بما يؤدي إلى تعزيز كفاءة تلك الخدمات، حين تقديمها إلى الجهات الوطنية المختلفة. ويمكن إيجاز الأهداف التي يسعى هذا الإطار إلى تحقيقها في الآتي:

١. الإسهام في تعزيز الأمن السيبراني في المملكة؛ من خلال تقديم خدمات مركز عمليات الأمن السيبراني المُدَار بجودة عالية، وبأسعار تنافسية، وفق متطلبات محددة.
٢. قيام الجهات الوطنية في المملكة، بالوفاء بالتزاماتها تجاه مسؤولية أمنها السيبراني؛ من خلال جهات مرخصة، ومؤهلة لتقديم خدمات الأمن السيبراني لها.
٣. تحفيز نمو قطاع الأمن السيبراني في المملكة، وتعزيز تنافسيته، والجهات العاملة فيه.
٤. تشجيع الابتكار، والاستثمار في قطاع الأمن السيبراني؛ من خلال دعم توفير حلول ومنتجات مبتكرة تلبي الطلب المتزايد، في تقديم خدمات مركز عمليات الأمن السيبراني المُدَار.
٥. حماية حقوق الجهات الوطنية المستفيدة؛ من خدمات الأمن السيبراني، المقدمة بموجب هذا الإطار.
٦. تعزيز تنمية القدرات البشرية الوطنية، المتخصصة في تقديم خدمات مركز عمليات الأمن السيبراني المُدَار.

٤. نطاق تطبيق الإطار

ينطبق هذا الإطار على:

١. أي جهة، ترغب في تقديم خدمات مركز عمليات الأمن السيبراني المُدَار، في المملكة العربية السعودية.
٢. الأفراد الذي يعملون، أو يرغبون في العمل لدى مقدمي الخدمات بوصفهم محللين في مراكز عمليات الأمن السيبراني المُدَارة، بالمملكة العربية السعودية.

٥. أحكام ترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدَار

٥,١ طلب الحصول على الترخيص والمحافظة عليه وتجديده

٥,١,١ يجب للحصول على ترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدَار؛ التقدّم بطلب للهيئة، واستيفاء المتطلبات المنصوص عليها في الملاحق (ب) و (ج) و (د) و (هـ) و (و) من هذا الإطار، بحسب مستوى الترخيص.

٥,١,٢ تكون مدة ترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدَار خمس (٥) سنوات تبدأ من تاريخ إصداره.

٥,١,٣ يجب على مقدم الخدمة، الاستمرار بالوفاء بالمتطلبات المنصوص عليها في الملاحق (ب) و (ج) و (د) و (هـ) و (و) للمحافظة على الترخيص، الصادر له بحسب مستواه.

٥,١,٤ يجوز لمقدم الخدمة التقدّم بطلب لتجديد الترخيص، في موعد لا يتجاوز (٩٠) يوم تقويمي قبل تاريخ انتهاء الترخيص، وفي موعد أقصاه (٣٠) يوم تقويمي قبل تاريخ انتهاء الترخيص، واستيفاء جميع المتطلبات التنظيمية ذات العلاقة المنصوص عليها في هذا الإطار وأي متطلبات أخرى تفرضها الهيئة.

٥,١,٥ في حال عدم رغبة مقدم الخدمة في تجديد الترخيص، أو في حال رفض الهيئة لطلب التجديد الذي تقدّم به، أو في حال كون مقدم الخدمة قد قام بتقديم طلب لإلغاء الترخيص (في أي من هذه الحالات)، فيتوجّب عليه

عدم استقبال أي تعاقدات جديدة داخلة في نطاق الترخيص، وأن يُشعر الجهات المستفيدة من خدماته بذلك، وفق ما تقرره الهيئة.

٥,٢ التنازل عن الترخيص

٥,٢,١ لا يجوز لمقدم الخدمة التنازل عن الترخيص الصادر له، دون الحصول على موافقة خطية مسبقة من الهيئة.

٥,٢,٢ يجب على مقدم الخدمة الذي يرغب في التنازل عن الترخيص الصادر له؛ التقدّم بطلب خطي إلى الهيئة يتضمّن الأسباب والحيثيات لطلب التنازل؛ وتقديم أي معلومات أو وثائق إضافية تطلبها الهيئة، أثناء دراسة الطلب.

٥,٢,٣ تصدر الهيئة قرارها في شأن الطلب ويتوجّب على مقدم الخدمة التقيّد به.

٥,٣ إلغاء الترخيص وتعليقه

٥,٣,١ يجب على مقدم الخدمة الذي يرغب في إلغاء الترخيص الصادر له؛ التقدّم بطلب خطي إلى الهيئة، يتضمّن الأسباب والحيثيات لطلب الإلغاء؛ وكذلك تقديم أي معلومات أو وثائق إضافية تطلبها الهيئة أثناء دراسة الطلب. وتصدر الهيئة -بعد تلقي طلب الإلغاء المكتمل من مقدم الخدمة- قرارها في شأن الطلب؛ ويتوجّب على مقدم الخدمة التقيّد به.

٥,٣,٢ تحتفظ الهيئة -وفقًا لتقديرها- بحق إلغاء ترخيص مقدم الخدمة أو تعليقه؛ في الحالات التي تستلزم ذلك، ومن تلك الحالات -على سبيل المثال لا الحصر-:

أ. عدم الالتزام بالأحكام المنصوص عليها في هذا الإطار، وما يطرأ عليه من تعديلات.

ب. عدم الالتزام بأي وثائق أو متطلبات تنظيمية صادرة عن الهيئة، ويشمل ذلك القرارات، والتنظيميات، والأطر والتعليمات، والتوجيهات، والتعاميم، والضوابط وما في حكمها.

ج. تكرار حالات عدم الوفاء بالالتزامات المقررة على مقدم الخدمة بموجب هذا الإطار، وتنظيمات الهيئة ذات العلاقة.

٥,٣,٣ يحتسب تعليق الترخيص الصادر في حق مقدم الخدمة ضمن مدة سريان الترخيص، ولا يكون له تأثير في تاريخ انتهاء الترخيص.

٥,٣,٤ ستقوم الهيئة برفع تعليق الترخيص؛ وفقًا لتقديرها المطلق، وبعد اتخاذ مقدم الخدمة الإجراءات التصحيحية اللازمة، المفروضة عليه من الهيئة، وقبولها منه.

٥,٣,٥ لا يُسمح لمقدم الخدمة، بأي شكل كان؛ تقديم خدماته الداخلة، في نطاق الترخيص، عند انتهاء الترخيص الصادر له، أو إلغائه أو تعليقه.

٦. التزامات مقدّم الخدمة

يجب على مقدم الخدمة في كل الأحوال الالتزام بأحكام هذا الإطار، والقرارات، والتنظيميات، والأطر والضوابط، والتعليمات، والتوجيهات، والتعاميم، وما في حكمها؛ الصادرة عن الهيئة. كما يجب عليه الالتزام بما يلي:

٦,١ الأنظمة واللوائح، والتنظيمات، والتعليمات، المعمول بها في المملكة العربية السعودية.

٦,٢ البدء بتقديم الخدمات المرخص بها خلال (٣) أشهر من تاريخ إصدار الترخيص في الحد الأقصى؛ ما لم تقرر الهيئة خلاف ذلك.

٦,٣ الربط مع مركز عمليات الأمن السيبراني الوطني بالهيئة؛ وفقًا للتعليمات والمتطلّبات التي تحددها الهيئة، ويتحمّل مقدم الخدمة تكلفة الربط، وأي نفقات تشغيلية لازمة لذلك، طوال فترة سريان الترخيص.

٦,٤ التقيّد بمتطلبات التوطين، وإبقاء جميع المرافق لديه والبيانات، داخل المملكة العربية السعودية.

٦,٥ تنفيذ خدمات مركز عمليات الأمن السيبراني المُدَار وتشغيله، وتقديم الخدمات للجهات المستفيدة من داخل المملكة.

٦,٦ المتطلبات الفنية التي تضعها الهيئة لبناء مركز عمليات الأمن السيبراني المُدَار وتشغيله، وما يطرأ عليها من تحديثات.

٦,٧ أن تكون معالجة البيانات المتعلقة بخدمات مركز عمليات الأمن السيبراني المُدَار وتخزينها، داخل المملكة.

٦,٨ تنفيذ ما تجري مشاركته من الهيئة من توصيات أو متطلبات سيبرانية وأمنية؛ بما في ذلك التنبيهات السيبرانية، وقواعد رصد التهديدات، ومؤشرات الاختراق. وتزويد الهيئة بالنتائج، وفق المتطلبات، والمدة المقررة منها.

٦,٩ تزويد الهيئة بالتقارير الدورية -وفق ما تقرره- وأي معلومات أخرى تطلبها، والتقيّد بالمهل، والكيفية والنماذج المقررة لذلك، وتشمل التقارير -على سبيل المثال لا الحصر- التهديدات السيبرانية، ومؤشرات الاختراق، والثغرات والتنبيهات السيبرانية، وإجراءات التعامل معها، وكذلك التهديدات السيبرانية التي جرى احتواؤها؛ وإجراءات ذلك.

٦,١٠ عدم نشر أي بيانات متعلقة بالأمن السيبراني، والمعلومات ذات الصلة، قبل الحصول على موافقة خطية من الهيئة.

٦,١١ عدم نشر و/ أو مشاركة أي بيانات خاصة بالجهات المستفيدة من خدماته، في نطاق الترخيص، أو تلك المتعلقة بالفضاء السيبراني السعودي؛ مع أي جهة؛ بأي مسوغ، ولأي مسوّغ بما فيها الجهات الحكومية أو الخاصة، داخل المملكة وخارجها؛ ويكون نشرها مشروطاً بموافقة خطية من الهيئة.

٦,١٢ النص في تعاقداته، ذات الصلة بهذا الإطار؛ مع الجهات المستفيدة على الأحكام التي تعالج حالات انتهاء الترخيص، أو عدم تجديده، أو إلغائه.

٦,١٣ تطبيق الإجراءات اللازمة، في حال انتهاء العلاقة التعاقدية أو إنهائها، مع الجهات المستفيدة، وفق ما تقرره الهيئة، والتي تشمل في الحد الأدنى ما يلي:

٦,١٣,١ إخطار الجهة المستفيدة برغبته بإنهاء التعاقد معها، في موعد لا يقل عن (٢٧٠) يومًا؛ قبل تاريخ إيقاف تقديم خدمات مركز عمليات الأمن السيبراني المُدَار إليها.

٦,١٣,٢ إذا كانت الجهة المستفيدة من الجهات المشمولة بتطبيق السياسة؛ فيتعين أيضًا على مقدم الخدمة من المستوى الأول، إشعار الهيئة في موعد لا يقل عن (٢٧٠) يومًا، قبل تاريخ إيقاف تقديم خدمات مركز عمليات الأمن السيبراني المُدَار إليها.

٦,١٤ إبلاغ الهيئة فورًا بأي تغيير في المعلومات، أو البيانات ذات الصلة بطلب الترخيص و/ أو مقدم الخدمة، و/ أو عند اكتشاف أي معلومات غير دقيقة أو مخالفة للواقع، لما جرى إبلاغ الهيئة بها، مع بيان الأسباب التي دعت لتقديمها بشكل غير دقيق، أو غير صحيح، وسبب التغيّر فيها.

٦,١٥ إبلاغ الهيئة فورًا بأي إجراء قانوني أو تنظيمي ضده قد يؤثر على تقديم الخدمات؛ بغض النظر عن الجهة التنظيمية أو الاختصاص، وسواء أكان من داخل المملكة أم كان خارجها.

٦,١٦ الاحتفاظ بسجلات دقيقة وكاملة عن أحداث الأمن السيبراني لمدة (١٨) شهر ماضية، لكل جهة مستفيدة من خدماته.

٦,١٧ الاحتفاظ بسجلات خدمات مركز عمليات الأمن السيبراني المُدَار المقدمة للجهات المستفيدة، لمدة (٥) سنوات من تاريخ تقديم تلك الخدمات؛ على أن تشمل -على سبيل المثال لا الحصر- تاريخ تقديم الخدمة، واسم الجهة المستفيدة من الخدمة، وبيانات محللي مركز عمليات الأمن السيبراني المُدَار العاملين لديه، الذين شاركوا في تقديم الخدمة، وأي طرف ثالث له علاقة في تقديم أي جزء من خدمات المركز بأي شكل كان لصالحه؛ وفق النماذج المقرّة من الهيئة لذلك.

٦,١٨ تقديم قوائم مالية مدققة من مراجع حسابات مستقل -مرخص بشكل نظامي، وفقاً لأنظمة المملكة- تظهر الإيرادات من تقديم خدمات مركز عمليات الأمن السيبراني المُدَار لكل سنة مالية طوال فترة الترخيص.

٦,١٩ التعاون التام مع الهيئة عند مباشرة اختصاصاتها التنظيمية والرقابية عليه بوصفه مرخص له، وإتاحة جميع الموارد الممكنة الخاصة به، لتنفيذ أي متطلبات للرقابة، والتفتيش من الهيئة، بما يشمل المراجعة والتحقق، وإجراء التقييمات السيبرانية، وأي متطلّب آخر على أعماله وأنظمته أي كانت.

٦,٢٠ تزويد الهيئة بجميع الوثائق، والبيانات، والمعلومات، والتقارير، التي تثبت التزامه بتنظيمات الهيئة ومتطلباتها، وتشمل -دون حصر- ما يلي:

أ. معلومات الأداء المالي لأعمال مركز عمليات الأمن السيبراني المُدَار، بما في ذلك الإيرادات ومصادرها، ورأس المال، والاستثمارات التقنية، واستثمارات البنية التحتية، ونفقات التدريب والتطوير.

ب. معلومات عمليات مركز عمليات الأمن السيبراني المُدَار، والجهات المستفيدة من الخدمات، وأسماء تلك الجهات وعددها، ونوع الخدمات المقدمة لها، والاجتماعات والتعاملات معها، وسجلات الأنشطة ذات الصلة بمركز عمليات الأمن السيبراني المُدَار، وغير ذلك.

ج. معلومات العاملين لديه المعنيين بتقديم خدمات مركز عمليات الأمن السيبراني المُدَار، وتشمل عدد الموظفين، وبيانات السير الذاتية، والمؤهلات الخاصة بهم، وغير ذلك مما له علاقة بطبيعة العمل.

د. معلومات المتطلبات الفنية المفروضة على مقدمي الخدمات، والأدوات والاشتراكات التقنية، وأي بنية تحتية لتقنية المعلومات؛ لها صلة بتنفيذ خدمات مركز عمليات الأمن السيبراني المُدَار، وغير ذلك.

هـ. أي دليل أو وثيقة، أو مستند، أو إثبات تطلبه الهيئة، للتحقق من التزام مقدم خدمات مركز عمليات الأمن السيبراني المُدَار بالأحكام الواردة في هذا الإطار، والوثائق الأخرى الصادرة عن الهيئة، وغيرها من الجهات المعنية.

٦,٢١ الالتزام بنسب التوطين للوظائف، من الكفاءات الوطنية؛ وفق ما تقرّه الهيئة، والجهات المختصة.

٦,٢٢ الالتزام بالقرارات الصادرة عن الهيئة، في أي خلافات قد تنشأ مع الجهة المستفيدة، تجاه الخدمات المقدمة بموجب الترخيص.

٦,٢٣ التطبيق الدائم والمستمر لجميع ضوابط الأمن السيبراني، الصادرة عن الهيئة، التي تنطبق على مقدم الخدمة؛ وتشمل -دون حصر- الضوابط الأساسية للأمن السيبراني، وضوابط الأمن السيبراني للأنظمة الحساسة، وضوابط الأمن السيبراني للبيانات، وتقديم وثائق سنوية تثبت الالتزام بالضوابط المعتمدة من قبل الهيئة.

٦,٢٤ تقديم خدمات مركز عمليات الأمن السيبراني المُدَار على مدار الساعة، وطوال أيام الأسبوع، وطوال العام.

٦,٢٥ الالتزام بتقديم جميع خدمات مركز عمليات الأمن السيبراني المُدَار؛ على النحو الوارد في الملحق (أ) من هذا الإطار بالنسبة للمستوى الأول. وتقديم خدمة واحدة على الأقل؛ على النحو الوارد في الملحق (أ) من هذا الإطار بالنسبة للمستوى الثاني.

٦,٢٦ الالتزام بإشعار الهيئة فوراً عندما يطرأ أي تغيّر في ملكية كيان مقدم الخدمة، بأي شكل كان.

٦,٢٧ الالتزام بالحصول على موافقة الهيئة، الخطية المسبقة؛ قبل ترتيب أي إجراء من شأنه تحقيق تغيّر في ملكية كيان مقدم الخدمة، بأي شكل كان.

٦,٢٨ استيفاء متطلبات حصول العاملين لديه، بوصفهم محللي مراكز عمليات الأمن السيبراني المُدَارة، على شهادة تأهيل للعمل في مراكز عمليات الأمن السيبراني المُدارة، وتجديدها وفق هذا الإطار وما تقرره الهيئة.

٧. التعاقد من الباطن للقيام بخدمات مركز عمليات الأمن السيبراني المُدَار

٧,١ يجوز لمقدم الخدمة التعاقد من الباطن؛ للقيام بخدمات مركز عمليات الأمن السيبراني المُدَار، وفقًا للشروط الآتية:

٧,١,١ تقديم طلب خطي بذلك للهيئة، وفق المتطلبات التي تقررها الهيئة.

٧,١,٢ عدم السماح بمباشرة الجهة المتعاقد معها من الباطن لأي أعمال، قبل الحصول على موافقة مسبقة من الهيئة على الطلب المقدم، للتعاقد من الباطن.

٧,١,٣ تظل جميع الالتزامات الناشئة عن الترخيص في مواجهة الهيئة، مسؤولية مقدم الخدمة، وتكون أي اشتراطات، أو قيود تخالف ذلك في التعاقدات، بين مقدم الخدمة، والمتعاقد معه من الباطن؛ باطلة، ولا ترتّب أي أثر قانوني لها تجاه الهيئة.

٧,١,٤ يجب توثيق ترتيبات التعاقد من الباطن، ضمن هذا البند؛ في سجلات مقدم الخدمة الداخلية، والتقيّد بأي تعليمات للهيئة ذات صلة.

٧,٢ لا يجوز لمقدم الخدمة، التعاقد من الباطن، للقيام بخدمات مركز عمليات الأمن السيبراني المدُار؛ إلا مع مقدم خدمة آخر. ويشترط أن يكون التعاقد في مستوى الترخيص نفسه، في حال كانت الخدمات مقدمة للجهات المشمولة بتطبيق السياسة.

٧,٣ للهيئة وفق تقديرها المطلق؛ وضع حد أعلى للتعاقدات من الباطن، التي يجوز لمقدم الخدمة في المستوى الأول القيام بها.

٧,٤ في كل الأحوال يجب أن يفي المتعاقد معه من الباطن، بجميع الالتزامات المقررة على مقدم الخدمة بموجب هذا الإطار.

٨. متطلبات الحصول على شهادة التأهيل للعمل في مركز عمليات الأمن السيبراني المدُار

٨,١ يجب على الأفراد للعمل محللين في مراكز عمليات الأمن السيبراني المدُارة؛ إكمال متطلبات الحصول على شهادة التأهيل من الهيئة، واستيفاء جميع المتطلبات التنظيمية المنصوص عليها في الملحق (ج) من هذا الإطار.

٨,٢ يكون التقدّم بطلب للحصول على شهادة التأهيل، وتجديدها، وفق ما تقرره الهيئة في هذا الشأن.

٨,٣ تكون مدة شهادة التأهيل للعمل في مراكز عمليات الأمن السيبراني المُدَارة ثلاث (٣) سنوات؛ تبدأ من تاريخ إصدار الشهادة من قبل الهيئة.

٨,٤ يجوز طلب تجديد شهادة التأهيل للعمل في مراكز عمليات الأمن السيبراني المدُارة، في موعد لا يتجاوز (٩٠) يوم تقويمي؛ قبل تاريخ انتهاء الشهادة، وفي موعد أقصاه (٣٠) يوم تقويمي، قبل تاريخ انتهاء الشهادة واستيفاء جميع المتطلبات المنصوص عليها في الملحق (ج) وأي متطلبات ذات علاقة.

٨,٥ تحتفظ الهيئة وفقًا لتقديرها، بحق إلغاء شهادة التأهيل للفرد أو تعليقها، في الحالات التي تستلزم ذلك. ومن تلك الحالات على سبيل المثال لا الحصر:

أ. عدم الالتزام بالأحكام المنصوص عليها في هذا الإطار، وما يطرأ عليه من تعديلات.

ب. عدم الالتزام بأي وثائق، أو متطلبات تنظيمية، صادرة عن الهيئة، ويشمل ذلك القرارات والتنظيميات، والأطر والتعليمات، والتوجيهات، والتعاميم، وما في حكمها.

ج. تكرار حالات عدم الوفاء بالالتزامات المقررة على الفرد، بموجب هذا الإطار، وتنظيمات الهيئة ذات العلاقة.

د. الإخفاق في أي متطلبات، للحفاظ على الشهادة، وفق ما تقرره الهيئة.

٨,٦ لا يترتّب على تعليق شهادة التأهيل، أي تغيير في تاريخ انتهاء صلاحيتها.

٨,٧ لا يترتب على تغيير جهة العمل، من مقدم خدمة، إلى مقدم خدمة آخر، تأثير في صلاحية شهادة التأهيل ومدتها، ويجب في كل الأحوال، التقيد بما يصدر عن الهيئة، تجاه ذلك.

٨,٨ لا يُسمح للفرد الحاصل على شهادة التأهيل، بممارسة الأعمال ذات الصلة في مراكز عمليات الأمن السيبراني المُدارة، عند انتهاء الشهادة الصادرة له من الهيئة أو إلغائها أو تعليقها.

٩. أحكام عامّة

٩,١ يجب على أي جهة، تقدم خدمات مركز عمليات الأمن السيبراني المُدَار في المملكة، أو ترغب في تقديمها؛ الحصول على ترخيص بذلك من الهيئة، وفقًا للأحكام الواردة في هذا الإطار؛ وما تقرّه الهيئة.

٩,٢ ستقرر الهيئة مهلة تصحيحية للجهات العاملة في أنشطة الأمن السيبراني وخدماته، التي تدخل في نطاق هذا الإطار. ويجب على تلك الجهات معالجة أوضاعها، بما يتفق مع هذا الإطار، وما يصدر عن الهيئة.

٩,٣ ستصدر الهيئة التعليمات والضوابط ذات الصلة، التي يجب على الجهات العاملة في أنشطة الأمن السيبراني وخدماته التي تدخل في نطاق هذا الإطار؛ التقيّد بها في التعاقدات القائمة، أو المستقبلية لهم.

٩,٤ يجب على جميع الجهات التي تقدم خدمات الأمن السيبراني، التي تدخل في نطاق هذا الإطار؛ تقديم جميع الوثائق والمعلومات والتعاقدات، ذات الصلة بهذه الخدمات، وأي معلومات أخرى للهيئة، وفق ما تقرره، وذلك خلال مدة لا تتجاوز (٣٠) يومًا من تاريخ نفاذ هذا الإطار.

٩,٥ للهيئة وفق ما تقتضيه متطلبات تنظيم القطاع؛ فرض قيود أو متطلبات إضافية، أو إلغاؤها على مقدم الخدمة، أو الفرد الحاصل على شهادة التأهيل.

٩,٦ تحتفظ الهيئة بحقها في رفض أي طلبات للحصول على الترخيص، أو تجديده ،أو إلغائه بموجب هذا الإطار، أو الحصول على شهادة التأهيل وتجديدها.

٩,٧ يلتزم كلٌ من مقدم الخدمة، والفرد الحاصل على شهادة التأهيل، بتقديم التقارير الدورية إلى الهيئة، وأي معلومات أخرى تطلبها وفق ما تقرره.

٩,٨ مع مراعاة الأحكام الواردة في هذا الإطار، بشأن إلغاء الترخيص وشهادة التأهيل أو تعليقها، سوف تتخذ الهيئة القرارات اللازمة تجاه أي مخالفة مرتكبة، بموجب هذا الإطار، وفقاً لصلاحياتها النظامية.

٩,٩ تحتفظ الهيئة بحقها في فرض مقابلات مالية أخرى على مقدم الخدمة، والفرد الحاصل على شهادة التأهيل.

٩,١٠ تعد الملاحق الواردة في هذا الإطار؛ بالإضافة إلى وثيقة (المتطلبات الفنية لمقدمي خدمات مركز عمليات الأمن السيبراني المُدار) جزءاً من هذا الإطار، ويتم قراءتها والعمل بها كوثيقة واحدة.

٩,١١ تعد النسخة العربية من هذا الإطار؛ هي النسخة الرسمية المعتمدة، وفي حال وجود أي اختلافات بين نص النسخة الرسمية المكتوبة باللغة العربية، والترجمة إلى اللغات الأخرى؛ فيتم الرجوع إلى النسخة العربية.

٩,١٢ يجوز للهيئة مراجعة هذا الإطار وتحديثه، وفق متطلبات تنظيم قطاع الأمن السيبراني ويجب التقيّد بما يطرأ عليه من تحديث، وفق ما تقرره الهيئة.

١٠. الملاحق

الملحق (أ): خدمات مركز عمليات الأمن السيبراني المُدَار

هي خدمات تحصل عليها الجهة المستفيدة من مقدم الخدمة؛ بهدف مراقبة أحداث الأمن السيبراني في المنظومة التقنية، للجهة المستفيدة، لاكتشاف التهديدات السيبرانية، ومعرفة كيفية حدوثها، وتقديم التوصيات في كيفية معالجتها؛ ليتم تطبيقها من قبل الجهة المستفيدة. وتشمل هذه الخدمات -التي تحصل عليها الجهة المستفيدة من مقدم الخدمة- العمليات، وفرق العمل، والأنظمة وغيرها.

فيما يلي بيان بالحد الأدنى من خدمات مركز عمليات الأمن السيبراني المُدار:

١. المراقبة المستمرة واكتشاف التهديدات (Threat Monitoring and Detection)

تقديم خدمة المراقبة المستمرة للمنظومة التقنية في الجهة المستفيدة؛ وتشمل شبكات وأنظمة الجهة، واكتشاف التهديدات والهجمات السيبرانية في مراحلها المبكرة، وإصدار التنبيهات (Alerts) من خلال أدوات المراقبة والاكتشاف؛ باستخدام طرق اكتشاف مختلفة، مثل حالات اكتشاف معرّفة مسبقاً (detection use-cases) ومؤشرات الاختراق (Indicators of Compromise) وقواعد الاكتشاف (Detection Rules)، وتصنيف التنبيهات حسب خطورتها، وإصدار تنبيهات فورية للجهة المستفيدة عن التهديدات المكتشفة، وتقديم تقارير تقنية وتنفيذية دورية عن الحالة السيبرانية، وذلك عن طريق إدارة أدوات الأمن السيبراني المتخصصة وتشغيلها في المراقبة والاكتشاف.

٢. التحليل والتحقيق للتهديدات المكتشفة (Threat Analysis and Investigation)

قيام مقدم الخدمة بأعمال التحليل والتحقيق في التنبيهات المكتشفة، وربط الأحداث المختلفة، وفهمها ضمن سياق منظومة الجهة، والقدرة على تحديد التنبيهات الصحيحة، ذات العلاقة بحوادث سيبرانية حقيقية، وتحديد التنبيهات الخاطئة، بناءً على أسلوب منهجي للتحليل في جميع التهديدات، وتزويد الجهة المستفيدة بالتحليلات الأولية. بالإضافة إلى تقديم تحليلات شاملة، متضمنة مسببات التنبيهات والحوادث. كما تتضمّن قيام مقدم الخدمة، بعمل مسح لمؤشرات الاختراق (Sweeping) وتصيد التهديدات (Threat Hunting) وكذلك إجراء التحليل والتحقيق، في الحالات التي قامت الجهة المستفيدة بتبليغ مقدم الخدمة عنها.

٣. التوصيات لاحتواء التهديدات السيبرانية (Threat Containment Recommendations)

تقديم توصيات متكاملة، وفاعلة للجهة المستفيدة في كيفية احتواء التهديدات السيبرانية وتحييدها؛ ليتم تطبيقها من قبل الجهة المستفيدة، للسيطرة على مخاطر الهجمات والتهديدات المكتشفة.

الملحق (ب): مستويات ترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدَار، ومتطلبات الحصول على الترخيص، وتجديده، والمحافظة عليه

وفقًا لأحكام هذا الإطار؛ سوف تصدر الهيئة مستويين لترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدَار، وفقًا للنطاق المحدّد في الجدول الآتي:

مستوى الترخيص	النطاق
المستوى الأول	يسمح لمقدم الخدمة تقديم خدمات مركز عمليات الأمن السيبراني المُدَار لجميع الجهات؛ بما في ذلك الجهات الحكومية، والجهات التي تمتلك بنية تحتية وطنية حساسة، أو تقوم بتشغيلها، أو استضافتها.
المستوى الثاني	يسمح لمقدم الخدمة تقديم خدمات مركز عمليات الأمن السيبراني المُدَار لأي جهة؛ عدا الجهات الحكومية، والجهات التي تمتلك بنية تحتية وطنية حساسة، أو تقوم بتشغيلها، أو استضافتها.

يجب على الجهة التي ترغب في الحصول على ترخيص، تقديم خدمات مركز عمليات الأمن السيبراني المُدَار؛ استيفاء متطلبات الحصول على الترخيص وتجديده، والمحافظة عليه، وفق الجدول الآتي:

مستوى الترخيص	المتطلبات
المستوى الأول	١. أن يكون طالب الترخيص منشأة؛ مؤسسة بشكل نظامي في المملكة. ٢. تعبئة وتقديم نموذج طلب الترخيص. ٣. أن تكون ملكية المواطن أو المواطنين السعوديين للحصص أو الأسهم حسب الأحوال (سواء أكانت ملكية مباشرة، أم غير مباشرة، من خلال شركات مملوكة كلياً، أو جزئياً لمواطن أو أكثر) في المنشأة طالبة الترخيص، وفقًا للنسبة المقرّة لذلك من الهيئة. ٤. تقديم بيانات ملكيــة المنشأة (المباشرة وغير المباشرة) والمعلومات ذات الصلة (النظام الأساس، وعقد التأسيس، والسجل التجاري، وقائمة بجميع المسيطرين بما يبين عددهم، ونسبة الملكية التي يمتلكها كل منهم) والهيكل التنظيمي لمقدم الخدمة، ونسبة التوطين للمناصب القيادية. ٥. ألا يقل رأس المال عن (٥٠) خمسين مليون ريال سعودي. ٦. تقديم جميع خدمات مركز عمليات الأمن السيبراني المُدَار، على النحو الوارد في الملحق (أ). ٧. تقديم تقرير بالالتزام بجميع المتطلبات الفنية، المحددة في وثيقة (المتطلبات الفنية لمقدمي خدمات مركز عمليات الأمن السيبراني المُدار) واجتياز التقييم الذي تجريه الهيئة. ٨. توظيف وبدوام كامل لمحللي مركز عمليات الأمن السيبراني المُدار، من المواطنين السعوديين وفق الملحق (هـ) في الحد الأدنى. ٩. تقديم خطة العمل، التي سوف يجري تقديم الخدمة بموجبها؛ لمدة (٥) سنوات، تشمل -دون حصر-: أ. الرؤية واستراتيجية السوق، التي سيتبعها مقدم الخدمة. ب. البيانات المالية المبدئية للعمليات التشغيلية المنفذة على مدار (٥) سنوات. ج. خطة نقل المعرفة، في خدمات مركز عمليات الأمن السيبراني المُدَار. د. خارطة الطريق، ومستهدفات الاستثمار، المتعلقة بالموارد البشرية، والقدرات الفنية.

مستوى الترخيص	المتطلبات
المستوى الأول	١٠. تزويد الهيئة بتقرير عن برنامج الأمن السيبراني لمقدم خدمات مركز عمليات الأمن السيبراني المُدَار؛ لمراجعته. على أن يكون التقرير متوائماً مع وثيقة (المتطلبات الفنية لمقدمي خدمات مركز عمليات الأمن السيبراني المُدَار) الصادرة عن الهيئة. وأن يتضمّن - على سبيل المثال لا الحصر - ما يلي: أ. معلومات عن برنامج الأمن السيبراني لمقدم خدمات مراكز عمليات الأمن السيبراني المُدَارة. ب. الإجراءات العامة، ذات الصلة بتخزين البيانات ونقلها، ومراقبة الوصول إليها واستخدامها. ج. متطلبات الشبكة والأمن المادي؛ بما فيها إجراءات التشفير. د. إجراءات الإبلاغ عن حوادث الأمن السيبراني، والتحقق منها. هـ. معلومات عن فرق احتواء الحوادث، وقدراتهم. و. معلومات عن النسخ الاحتياطي، واستمرارية الأعمال. ز. إجراءات استعادة البيانات، أو إتلافها عند الانتهاء منها؛ دون أي تكاليف مالية على المستفيد من الخدمات. ح. اتفاقيات الخدمة المبرمة، مع المستفيدين من الخدمة. ١١. عندما تجري الاستعانة بخدمات أحد مقدمي خدمات الحوسبة السحابية (CSP) فإنه يجب أن يجري التعاقد مع مقدم خدمات حوسبة سحابية مرخص من قبل الجهة المختصة في المملكة.
المستوى الثاني	١. أن يكون طالب الترخيص؛ منشأة مؤسسة بشكل نظامي في المملكة. ٢. تعبئة وتقديم نموذج طلب الترخيص. ٣. أن تكون ملكية المواطن أو المواطنين السعوديين للحصص أو الأسهم حسب الأحوال (سواء أكانت ملكية مباشرة، أم غير مباشرة، من خلال شركات مملوكة كلياً، أو جزئياً لمواطن أو أكثر) في المنشأة طالبة الترخيص، وفقًا للنسبة المقرّة لذلك من الهيئة. ٤. تقديم بيانات ملكيــة المنشأة (المباشرة وغير المباشرة) والمعلومات ذات الصلة (النظام الأساس، وعقد التأسيس، والسجل التجاري، وقائمة بجميع المسيطرين بما يوضح عددهم ونسبة الملكية التي يمتلكها كل منهم) والهيكل التنظيمي لمقدم الخدمة، ونسبة التوطين لكل من المناصب القيادية. ٥. ألا يقل رأس المال عن (٥٠٠) خمسمائة ألف ريال سعودي. ٦. تقديم خدمة واحدة على الأقل، من خدمات مركز عمليات الأمن السيبراني المُدَار؛ على النحو الوارد في الملحق (أ). ٧. تقديم تقرير بالالتزام بجميع المتطلبات الفنية، المحددة في وثيقة (المتطلبات الفنية لمقدمي خدمات مركز عمليات الأمن السيبراني المُدار) واجتياز التقييم الذي تجريه الهيئة. ٨. توظيف وبدوام كامل، لمحللي مركز عمليات الأمن السيبراني المُدار، من المواطنين السعوديين وفق الملحق (و) في الحد الأدنى. ٩. تزويد الهيئة بتقرير عن برنامج الأمن السيبراني لمقدم خدمات مركز عمليات الأمن السيبراني المُدَار؛ لمراجعته، على أن يكون التقرير متوائماً مع وثيقة (المتطلبات الفنية

مستوى الترخيص	المتطلبات
المستوى الثاني	لمقدمي خدمات مركز عمليات الأمن السيبراني المُدار) الصادرة عن الهيئة؛ وأن يتضمّن - على سبيل المثال لا الحصر- ما يلي: أ. معلومات عن برنامج الأمن السيبراني لمقدم خدمات مركز عمليات الأمن السيبراني المُدَار. ب.الإجراءات العامة، ذات الصلة بتخزين البيانات ونقلها، ومراقبة الوصول إليها واستخدامها. ج. متطلبات الشبكة والأمن المادي، بما في ذلك إجراءات التشفير. د. إجراءات الإبلاغ عن حوادث الأمن السيبراني، والتحقق منها. هـ. معلومات عن فرق احتواء الحوادث، وقدراتهم. و. معلومات عن النسخ الاحتياطي، واستمرارية الأعمال. ز. إجراءات استعادة البيانات، أو إتلافها عند الانتهاء منها؛ دون أي تكاليف مالية على المستفيد من الخدمات. ح. اتفاقيات الخدمة المبرمة مع المستفيدين من الخدمة. ١٠. في حال تم الاستعانة بخدمات أحد مقدمي خدمات الحوسبة السحابية (CSP) فيجب أن يتم التعاقد مع مقدم خدمات حوسبة سحابية مرخص من قبل الجهة المختصة في المملكة.

الملحق (ج): متطلبات الحصول على شهادة التأهيل وتجديدها والمحافظة عليها

وفقًا لأحكام هذا الإطار؛ سوف تُصدر الهيئة شهادة التأهيل للأفراد في ثلاث فئات، حسب الآتي:

فئة الشهادة	متطلبات الحصول على شهادة التأهيل والمحافظة عليها وتجديدها
الفئة (أ)	١. أن يكون مواطناً سعودياً. ٢. التمتع بالمعارف، والمهارات، والقدرات اللازمة؛ لعمل محلل دفاع الأمن السيبراني، المحدد بموجب الإطار السعودي لكوادر الأمن السيبراني (سيوف). ٣. استيفاء أي من المتطلبات الآتية: أ. خبرة لمدة لا تقل عن سنة واحدة في عمل محلل مركز عمليات الأمن السيبراني، أو مسؤولًا في مجال الأمن السيبراني، أو الشبكات. ب. الحصول على درجة جامعية، من جامعة معترف بها، في تخصص تقنية المعلومات، أو الأمن السيبراني، أو علوم البيانات، أو أي مجال ذي صلة. ٤. إكمال الدورات التدريبية، واجتياز اختباراتها، وفق ما تحدده الهيئة. ٥. إكمال الساعات المطلوبة من التطوير المهني سنويًا (بما في ذلك دورات الأمن السيبراني، وحضور مؤتمرات الأمن السيبراني، وغيرها من أنشطة التعلم والتطوير، في مجال الأمن السيبراني).
الفئة (ب)	١. أن يكون مواطناً سعودياً. ٢. التمتع بالمعارف، والمهارات، والقدرات اللازمة لعمل محلل دفاع الأمن السيبراني؛ المحدد بموجب الإطار السعودي لكوادر الأمن السيبراني (سيوف). ٣. استيفاء أي من المتطلبات الآتية: أ. التمتع بخبرة (٣) سنوات في العمل بكونه محلل مركز عمليات الأمن السيبراني. ب. الحصول على شهادة سارية من الفئة (أ) لمدة (٣) سنوات، على الأقل. ٤. إكمال الدورات التدريبية، واجتياز اختباراتها، وفق ما تحدده الهيئة. ٥. إكمال الساعات المطلوبة من التطوير المهني سنويًا (بما في ذلك دورات الأمن السيبراني، وحضور مؤتمرات الأمن السيبراني، وغيرها من أنشطة التعلم والتطوير، في مجال الأمن السيبراني).
الفئة (ج)	١. أن يكون مواطناً سعودياً. ٢. التمتع بالمعارف والمهارات والقدرات اللازمة لعمل محلل دفاع الأمن السيبراني؛ المحدد بموجب الإطار السعودي لكوادر الأمن السيبراني (سيوف). ٣. استيفاء أي من المتطلبات الآتية: أ. التمتع بخبرة (٥) سنوات في العمل بكونه محلل مركز عمليات الأمن السيبراني. ب. الحصول على شهادة سارية من الفئة (ب) لمدة (٣) سنوات على الأقل. ٤. إكمال الدورات التدريبية، واجتياز اختباراتها، وفق ما تحدده الهيئة. ٥. إكمال الساعات المطلوبة من التطوير المهني سنويًا (بما في ذلك دورات الأمن السيبراني، وحضور مؤتمرات الأمن السيبراني، وغيرها من أنشطة التعلم والتطوير، في مجال الأمن السيبراني).

الملحق (د) :جدول المقابلات المالية لطلب ترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدَار

- يجب على مقدم الطلب، بموجب هذا الإطار؛ سداد المقابل المالي على النحو المقرر في هذا الملحق لطلب الحصول على الترخيص أو تجديده. وتحتفظ الهيئة بالحق في إجراء التعديلات التي تراها على هذا المقابل المالي و/ أو فرض مقابلات مالية أخرى على المرخص له.
- تكون جميع المقابلات المالية المدفوعة -بموجب هذا الملحق- غير مستردة.
- يبين الجدول الآتي المقابلات المالية لطلب الحصول على ترخيص تقديم خدمات مركز عمليات الأمن السيبراني المُدَار، أو تجديده بموجب هذا الإطار.

المقابل المالي لطلب الحصول على الترخيص أو تجديده	
مستوى الترخيص	**المقابل المالي لطلب الحصول على الترخيص أو تجديده**
المستوى الأول	50,000 ريال سعودي
المستوى الثاني	15,000 ريال سعودي

الملحق (هـ): جدول الحد الأدنى لعدد محللي مركز عمليات الأمن السيبراني المُدار ، المؤهلين بموجب هذا الإطار، الذين يتوجب على مقدم الخدمة في المستوى الأول توظيفهم (دوام بعمل كامل)

- يوضح الجدول الأتي الحد الأدنى من أعداد محللي مركز عمليات الأمن السيبراني المُدَار من المواطنين السعوديين لمقدم الخدمة في المستوى الأول. ويجب على مقدم الخدمة تقييم الحاجة إلى زيادة أعداد محللي مركز عمليات الأمن السيبراني المُدَار؛ للقدرة على الوفاء بالتزاماته، تجاه الجهات المستفيدة من خدماته، مع الأخذ في الحسبان الجوانب الفنية الخاصة بكل جهة مستفيدة؛ مثل حجم الأنظمة وتعقيدها، والتقنيات التي تتم مراقبتها.
- يجوز للهيئة -وفقًا للآلية التي تحددها- تقليص الحد الأدنى، من أعداد محللي مركز عمليات الأمن السيبراني المُدَار المطلوبة من مقدم الخدمة؛ إذا ثبت قيام مقدم الخدمة باستخدام الحلول المناسبة -بما فيها الأتمتة (Automation)- بما يقلل الاحتياج إلى عدد كبير، من محللي مركز عمليات الأمن السيبراني المُدَار.

عدد الجهات المستفيدة لدى مقدم الخدمة	عدد المحللين بدوام كامل (FTE) في الفئة (أ)	عدد المحللين بدوام كامل (FTE) في الفئة (ب)	عدد المحللين بدوام كامل (FTE) في الفئة (ج)	إجمالي عدد المحللين بدوام كامل (FTE)
١-٣٠	٢٠	١٠	٢	٣٢
٣١-٤٠	٢٥	١٢	٣	٤٠
٤١-٥٠	٣٠	١٥	٤	٤٩
٥١-٦٠	٣٥	١٧	٤	٥٦
٦١-٧٠	٤٠	٢٠	٥	٦٥
٧١-٨٠	٤٥	٢٢	٥	٧٢
٨١-٩٠	٥٠	٢٥	٦	٨١
+٩١	يجب على مقدم الخدمة إرسال طلب إلى الهيئة لتحديد الحد الأدنى لعدد محللي مركز عمليات الأمن السيبراني المُدار			

الملحق (و): جدول الحد الأدنى لعدد محللي مركز عمليات الأمن السيبراني المُدار المؤهلين بموجب هذا الإطار، الذي يتعين على مقدمة الخدمة في المستوى الثاني توظيفهم (دوام بعمل كامل)

- يبين الجدول الآتي الحد الأدنى من أعداد محللي مركز عمليات الأمن السيبراني المُدار من المواطنين السعوديين لمقدم الخدمة من المستوى الثاني. ويجب على مقدم الخدمة، تقييم الحاجة إلى زيادة أعداد محللي مركز عمليات الأمن السيبراني المُدار، للقدرة على الوفاء بالتزاماته تجاه الجهات المستفيدة من خدماته؛ مع الأخذ في الحسبان الجوانب الفنية الخاصة لكل جهة مستفيدة، مثل حجم الأنظمة وتعقيدها، والتقنيات التي تتم مراقبتها.
- يجوز للهيئة -وفقا للآلية التي تحددها- تقليص الحد الأدنى من أعداد محللي مركز عمليات الأمن السيبراني المُدار، المطلوبة من مقدم الخدمة؛ إذا ثبت قيام مقدم الخدمة باستخدامه الحلول المناسبة -بما فيها الأتمتة (Automation)- بما يقلل الاحتياج إلى عدد أكبر من محللي مركز عمليات الأمن السيبراني المُدَار.

عدد الجهات المستفيدة لدى مقدم الخدمة	عدد المحللين بدوام كامل (FTE) في الفئة (أ)	عدد المحللين بدوام كامل (FTE) في الفئة (ب)	عدد المحللين بدوام كامل (FTE) في الفئة (ج)	إجمالي عدد المحللين بدوام كامل (FTE)
١-١٠	٢	١	١	٤
١١-٢٠	٣	٢	٢	٧
٢١-٣٠	٤	٢	٢	٨
٣١-٤٠	٥	٣	٣	١١
٤١-٥٠	٦	٣	٣	١٢
٥١-٦٠	٧	٤	٤	١٥
٦١-٧٠	٨	٤	٤	١٦
٧١-٨٥	٩	٥	٥	١٩
+٨٦	يجب على مقدم الخدمة إرسال طلب إلى الهيئة؛ لتحديد الحد الأدنى لعدد محللي مركز عمليات الأمن السيبراني المُدار			


الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority