

المعيار المهني

لمهنة محلل عمليات أمن سيبراني
المستوى المهني

- 4 كلمة معالي وزير العمل- رئيس مجلس تنمية وتطوير المهارات المهنية والتقنية
- 5 كلمة معالي رئيس هيئة تنمية وتطوير المهارات المهنية والتقنية
- 6 2- أسماء السادة أعضاء لجنة المهارات / لجنة الخبراء (هيئة DACUM)
- 7 3- قائمة المصطلحات
- 8 4- قائمة الاختصارات
- 8 1-4 قائمة اختصارات مصطلحات المهنة
- 8 2-4 قائمة اختصارات مصطلحات المعيار المهني
- 9 5- بيانات عامة عن المعايير
- 10 6- وصف المعيار
- 10 1-6 وصف عام للمعيار المهني لوظيفة / مهنة محلل عمليات أمن سيراني
- 10 2-6 الغاية من المعايير المهنية لمهنة محلل عمليات أمن سيراني
- 10 3-6 السياقات التمهيدية وخلفية تطوير المعيار
- 11 4-6 المسوغات والمبررات
- 11 5-6 العمليات المنفذة
- 11 6-6 الجهات الفاعلية والمؤسسات المشاركة في التنمية
- 11 7-6 ملكية هذه المعايير
- 11 8-6 عملية التحقق
- 12 9-6 وصف ونطاق المهنة
- 12 10-6 اسم المهنة
- 12 11-6 المستوى المهني
- 12 12-6 أماكن العمل المحتملة
- 12 13-6 العلاقات مع الشركاء
- 12 14-6 القوانين والأنظمة المتعلقة بالمهنة
- 13 15-6 الاعتراف بالتعلم المسبق (الخبرات السابقة والمؤهلات التعليمية)
- 13 1-15-6 ذوي خبرات ومؤهل جامعي متخصص
- 13 2-15-6 ذوي خبرات
- 13 16-6 المخطط التنظيمي للمهنة / العلاقات البيئية
- 13 17- المخاوف والنظرة المستقبلية للمهنة:
- 13 1-17-6 المخاوف
- 14 2-17-6 النظرة المستقبلية
- 14 18-6 المعايير ومرجعيات المواصفات العالمية
- 15 7- الإطار المرجعي للكفايات المهنية / الفنية
- 37 8- معايير الأداء
- 66 9 - سلوكيات وأخلاقيات العامل (القيم الأخلاقية)
- 67 10- قواعد السلامة والصحة المهنية

- 67 1-10 بروتوكول موقع العمل والإجراءات الوقائية
- 67 2-10 آليات تقليل حدوث المخاطر
- 67 3-10 تنظيم مواقع العمل
- 67 4-10 معدات الوقاية الشخصية
- 68 5-10 الأجهزة والآلات والأدوات والمعدات والمواد
- 68 11-شروط الالتحاق بالبرنامج
- 68 12- وصف بيئة العمل في ظل قانون العمل الأردني
- 68 1-12 ساعات العمل
- 69 2-12 الظروف البيئية
- 69 3-12 متطلبات بيئة العمل
- 69 13- معيار مدة التنفيذ ونقل المهارة
- 70 14- قائمة المراجع
- 70 1-14 المراجع العربية
- 71 15- قائمة الملاحق
- 71 1-15 قائمة الواجبات والمهام طبقا لمخطط DACUM
- 71 2-15 خطة التدريب
- 71 3-15 الوصف التدريبي
- 71 4-15 ملاحظات إرشادية للمدرسين
- 71 5-15 مواد تدريب المعلم / المدرب
- 71 6-15 مواد تدريب المتعلم / المتدرب
- 71 7-15 أنشطة البرنامج التدريبي
- 71 8-15 نموذج الامتحان النهائي (نظري)
- 71 9-15 نموذج الامتحان النهائي (عملي)
- 71 10-15 نموذج بطاقة التمرين
- 71 11-15 نموذج امتحان نهائي (اختيار من متعدد)
- 71 12-15 موجهات كتابة محتوى الكتاب
- 71 13-15 دليل العروض التقديمية
- 71 14-15 مواصفات وشروط المدرسين (معايير اختيار المدرسين)

كلمة معالي وزير العمل- رئيس مجلس تنمية وتطوير المهارات المهنية والتقنية

تعتبر وزارة العمل من الوزارات الخدمية التي تسعى إلى تقديم الخدمات للمواطنين، ومن أبرز الخدمات التي تقوم الوزارة بتقديمها، خدمات (الإشراف على شؤون العمل والعمال، تشغيل الاردنيين في الداخل والخارج والمساهمة في تنظيم سوق العمل الأردني ووضع التعليمات اللازمة لتوفير فرص العمل والتشغيل للأردنيين داخل المملكة وخارجها وبالتعاون مع الجهات المختصة.

تأكيدا لذلك يسر مجلس تنمية وتطوير المهارات المهنية والتقنية في إطار جهوده الرامية لإصلاح قطاع التدريب والتعليم المهني والتقني، والهادفة إلى تمكين هيئة تنمية وتطوير المهارات المهنية والتقنية؛ ليكون مسؤولا عن إعداد معايير الاعتماد وضبط الجودة لترخيص واعتماد مؤسسات التدريب والتعليم المهني والتقني وإجراء اختبارات المزاوله لممارسي الأعمال المهنية، ومنح إجازة المزاوله المهنية؛ أن يقدم المعايير المهنية لمهنة محلل عمليات أمن سيبراني / المستوى المهني والتي تم إعدادها بالشراكة والتنسيق مع مشروع التعليم والتدريب المهني والتعليم العالي الموجه نحو سوق العمل (MOVE-HET)، المنفذ من قبل الوكالة الألمانية للتعاون الدولي GIZ والممول من الوزارة الاتحادية الألمانية للتعاون الاقتصادي والتنمية (BMZ) وبالتعاون مع شركة GFA بألمانيا (GFA Consulting Group)، والشركة الوطنية للتشغيل والتدريب وشركة إبسيلون لتطوير التعليم والتدريب .

ونظرا لأهمية موضوع المعايير المهنية؛ يأتي هذا الدليل للرجوع إليه والاستفادة منه عند بناء البرامج التدريبية والاختبارات المهنية واعتمادها، بما يساهم في تحسين مستوى التدريب والخريجين، كما يعد مرجعا فنيا لذوي العلاقة سواء كان في التشغيل والتوظيف، أو إعداد التشريعات....إلخ.

وإذ يصادق المجلس على هذه السلسلة من المعايير المهنية فإنه يرجو أن يكون قد ساهم من خلال هذا الجهد الجماعي الذي تم العمل عليه بجهد متواصل للفرق القطاعية واللجان الفنية، في بناء المعايير المهنية ذات الأولوية للتدريب في سوق العمل الأردني، وأن يكون محفزاً لمزيد من الأدلة التي تعنى بالقطاعات المهنية الأخرى .

وختاماً أسأل المولى العلي القدير أن تكون هذه السلسلة من المعايير المهنية عوناً رئيساً ومساعداً لتطوير العمل في هيئة تنمية وتطوير المهارات المهنية والتقنية بشكل عام و العاملين في مجال تحليل الأمن السيبراني المهنيين بأماكن العمل المختلفة ومدربيهم بشكل خاص، وقد روعي في إعداد هذه المعايير الحدائق ومواكبة التطور بما يخدم عملية إعداد المهنيين وتلبية احتياجات تنفيذ البرامج التدريبية بكفاءة وفاعلية، ومن المؤمل أن ينعكس أثر هذا المجهود على تحسين نوعية التدريب وتطوير أداء المدرسين ورفع سوية الخريجين، بحيث يكون متجاوباً ومتوائماً مع متطلبات واحتياجات سوق العمل في أردننا الغالي، والله نسال أن يوفقنا لما فيه الخير والصلاح.

وزير العمل. رئيس مجلس تنمية وتطوير المهارات المهنية والتقنية

(يوسف الشمالي)

كلمة معالي رئيس هيئة تنمية وتطوير المهارات المهنية والتقنية

تأسست هيئة تنمية وتطوير المهارات المهنية والتقنية في عام 2019 بمقتضى المادة 31 من الدستور الأردني، وبناء على قانون رقم (9) من سنة 2019؛ قانون تنمية وتطوير المهارات المهنية والتقنية؛ والذي تم اعداده بما يتوافق مع توصيات الاستراتيجية الوطنية لتنمية الموارد البشرية (وضع هيكل تنظيمية واضحة لحاكمية القطاع لضمان اجراء تطبيق المسائلة في انحاء القطاع). وانطلاقاً من رؤية الهيئة المتمثلة في إعداد قوى بشرية تمتلك المهارة والخبرة المهنية والتقنية تلبي احتياجات سوق العمل وقادرة على المشاركة بالمشاريع الريادية وإعداد وتأهيل القوى العاملة لسوق العمل وإكسابهم المهارات الأدائية والاتجاهية الصحيحة وتمكينهم من مواكبة التطور السريع في سوق العمل، الأمر الذي يستدعي وجود مرجعية قياسية (معايير مهنية) يتم في ضوئها ضبط نواتج العملية التدريبية، وتحسين ارتباطها بالاحتياجات النوعية لسوق العمل، ويتم إعدادها بمشاركة فاعلة من الشركاء الاجتماعيين، بالإضافة إلى مزودي التدريب بحيث تمثل هذه المعايير المهنية الركيزة الأساسية في إعداد وتطوير المناهج وبناء البرامج التدريبية وتصميم الاختبارات المهنية، كونها المعيار أو المحك الذي يحتكم إليه لبيان مدى ملائمة الخريج أو المتدرب لاحتياجات ومتطلبات أسواق العمل المحلية والإقليمية.

كما أن عملية تطوير وتنمية الموارد البشرية للحاق بهذا التطور السريع في أسواق العمل الوطنية والدولية يقتضي وجود الكوادر المؤهلة لذلك، وهذه الكوادر -ومنها مقدمو خدمات تحليل عمليات الأمن السيبراني - يجب أن يكون لهم ولأدائهم مرجعية قياسية (معايير مهنية) يتم في ضوئها ضبط تقديم خدمات أنظمة تحليل عمليات الأمن السيبراني ونواتجها، على أن يتم إعداد هذه المعايير المرجعية بمشاركة فعالة من الشركاء الاجتماعيين، بالإضافة إلى مقدمي الخدمات أنفسهم ومزوديها .

تأسيساً على ذلك تم بناء المعايير المهنية في هذا الدليل المهني وفق مخطط دايكوم DACUM من قبل خبراء ومختصين ممارسين للمهنة، بالإضافة إلى خبراء تعليم وتدريب وشركات متخصصة في المجال (كبيرة - متوسطة - صغيرة) الحجم؛ بهدف إيجاد وصف دقيق لمتطلبات التدريب والتشغيل اعتماداً على تصنيف وتوصيف مهني معتمد، وقد تم اعتماد التصنيف الأردني المعياري للمهن ٢٠٢١ -JSCO- والإطار الوطني للمؤهلات في المملكة الأردنية الهاشمية 2020 كمرجعين أساسيين في إعداد المعايير المهنية الوطنية مع ما هو ملائم ومناسب لمتطلبات سوق العمل الأردني الحالية والمستقبلية؛ بهدف أن تكون إطاراً مرجعياً ليس فقط لمزودي تدريب المهنيين بتحليل عمليات أمن سيبراني ومن في حكمهم، بل أيضاً لتكون مرجعاً لمقدمي خدمات أنظمة تحليل عمليات أمن سيبراني أنفسهم .

وأخيراً فإن الهيئة إذ تبذل كل الجهد في هذا السياق فإنها تسعى إلى تحقيق الأهداف التي أنشئت من أجلها، ومنها إعداد معايير مهنية تقود إلى اعتماد وإصدار التراخيص اللازمة لمزودي الخدمات، ومنح إجازة مزاوله المهن، وهي هنا تسعى لمنح ترخيص مزاوله المهنة على المستوى "المهني" وهو ما يوازي المستوى (الرابع) طبقاً للإطار الوطني للمؤهلات في المملكة الأردنية الهاشمية.

إن هذه المبادرة من هيئة تنمية وتطوير المهارات المهنية والتقنية تعد نقطة انطلاق نحو المضي قدماً لتطوير برامج متخصصة بالدرجات العلمية الأعلى طبقاً لقواعد الاعتراف بالتعليم المسبق ومستويات الإطار الوطني للمؤهلات في المملكة الأردنية الهاشمية.
والله الموفق،

رئيس هيئة تنمية وتطوير المهارات المهنية والتقنية

(الدكتورة رغدة الفاعوري)

2- أسماء السادة أعضاء لجنة المهارات / لجنة الخبراء (هيئة DACUM)

الميسرون وأعضاء اللجنة

خبير دولي أول وميسر DACUM (GIZ) - MOVE-HET - GFA	الدكتور أبو الفضل عبده
المستشار الفني الإقليمي - MOVE-HET (GIZ)	الأستاذ محمود الشرييني
إبسيلون لتطوير التعليم والتدريب - EBSILON	الأستاذ جودي سعيد
مدير الاعتماد - هيئة تنمية وتطوير المهارات المهنية والتقنية	المهندس أيمن الوريكات
مدير وحدة تطوير الأداء المؤسسي - الشركة الوطنية للتشغيل والتدريب	المهندس مهند الخضيرى

لجنة الخبراء (ورشة DACUM)

الاسم	الجهة
المهندس / رakan حسان	Zain Group, Mobile telecommunication company
المهندس / أحمد مصلح	Green Circle
المهندسة / شروق العساف	Green Circle
المهندس / محمد أحمد الخضيرى	Green Circle
المهندس / محمد ناجي	Green Circle
المهندس / محمود ياسين سليم	IRIS Technology
المهندس / جهاد أمجد عقل	Shabkati Network Solutions
المهندس / محمد على الرفاعي	Cuber Security Awareness Ass
المهندسة / إيمان الحجايا	الشركة الوطنية للتشغيل والتدريب
المهندسة سارة ياسين العدوان	الشركة الوطنية للتشغيل والتدريب
المهندسة / فرح حسين النعيمات	الشركة الوطنية للتشغيل والتدريب
السيدة / هبة أحمد أبو حمور	الشركة الوطنية للتشغيل والتدريب
المهندسة / ولاء سالم العموش	الشركة الوطنية للتشغيل والتدريب
السيد / محمد هاني عوض الله	هيئة تنمية وتطوير المهارات المهنية والتقنية

3- قائمة المصطلحات

<ul style="list-style-type: none"> • هو المقاييس المرجعية المتعلقة بقياس مدى تلبية الفرد لمتطلبات الأداء. • هو مجموعة المقاييس المرجعية التي من خلالها يمكن التحقق من مدى امتلاك الفرد الكفايات - المعارف والمهارات والسلوكيات - للقيام بالعمل في المهنة بالطريقة الصحيحة. 	<p>المعيار المهني</p>
<p>إطار وطني للمؤهلات الأردنية: الأكاديمية والمهنية، يتضمن تصنيفاً هرمياً لجميع مستويات المؤهلات والشهادات المرتبطة ببرامج التعليم العالي والتعليم العام والتدريب والتعليم المهني والتقني ضمن واصفات لكل مستوى لتحديد المعارف والمهارات والكفايات التي ينبغي أن تكون مرتبطة بالمؤهل.</p>	<p>الإطار الوطني الاردني للمؤهلات</p>
<p>شهادة تمنح لخريج برنامج تعليمي او تدريبي معين له حد أدنى من ساعات التعليم والتدريب.</p>	<p>المؤهل</p>
<p>القدرة على أداء نشاط منتج بدرجة إتقان / مستوى أداء بحسب معايير سوق العمل.</p>	<p>كفاية</p>
<p>تمثل وحدة الكفاية مهمة رئيسة أو دوراً رئيساً من أدوار شغل العامل في عمل أو مهنة محددة.</p>	<p>وحدة الكفاية</p>
<p>أحد لبنات بناء وحدة الكفاية ويمثل نشاطاً رئيساً أو واجباً من واجبات الشغل الذي تغطيه وحدة الكفاية.</p>	<p>عنصر الكفاية</p>
<p>محك مرجعي أو مقياس لمراقبة أو تقويم كفاءة وفاعلية العمليات، ويستخدم لتحقيق المساءلة وتحديد مواطن التحسين.</p>	<p>معيار أداء العمليات</p>
<p>محك مرجعي أو مقياس لمراقبة أو تقويم كفاءة وفاعلية الخدمة / المنتج النهائي، ويستخدم لتحقيق المساءلة وتحديد مواطن التحسين.</p>	<p>معيار اداء المنتج</p>
<p>تشمل فئة مستوى العامل المهني الأعمال التي يتطلب إنجازها توافر مهارات عملية ومعلومات مهنية تغطي إطار المهنة بشكل كامل لدى شاغليها لتمكينهم من ممارسة مهام وواجبات العمل / المهنة بدرجة إتقان بحسب متطلبات سوق العمل، ولتمكينهم من توزيع العمل على المرؤوسين، وتنمية مهاراتهم. يحتاج الأفراد في هذه الفئة إلى تأهيل وتعليم مهني يوازي إنهاء مرحلة التعليم الثانوي كأساس كحد أدنى وتعادل المستوى الرابع على الاطار الوطني الاردني للمؤهلات _ المسار المهني.</p>	<p>المستوى المهني</p>

4- قائمة الاختصارات

1-4 قائمة اختصارات مصطلحات المهنة

الاختصار باللغة الإنجليزية	المصطلح باللغة الإنجليزية	المصطلح باللغة العربية
SOC	SECURITY operations center	مركز أمن المعلومات
VUL	Vulnerabilities	الثغرات
CST	Cyber Security Threats	تهديدات الأمن السيبراني
CR	Cyber Risks	المخاطر السيبرانية
	Assets	الأصول
	Incidents	الأحداث السيبرانية
	Ticket	تذكرة دعم فني
SIEM	Security info and event management	نظام المعلومات الأمنية وإدارة الأحداث
OS	Operating System	أنظمة التشغيل
	Stake holders	أصحاب المصلحة
	Risk Management	إدارة المخاطر
	Classification	تصنيف
	Policies and Procedures	السياسات والإجراءات
	RACI matrix	مصفوفة راكي (مصفوفة توزيع المسؤوليات)
	Alternative plans	خطط بديلة

2-4 قائمة اختصارات مصطلحات المعيار المهني

OS	Occupational Standards
TVSDC	Technical and Vocational Skills Development Commission
JNQF	Jordanian National Qualification framework
UC	Unite competency
EC	Element Competency
OS-SDC-SC1-022	OS: Occupational Standard SDC: Skills Development Commission SC: Cyber Security 1: Nr of the OS 022: year 2022

5- بيانات عامة عن المعايير

الصناعي - الخدمات - المدني - العسكري عمليات الأمن السيبراني	القطاع	العاملون في أنظمة تحليل عمليات الأمن سيبراني	المهن ذات الصلة
		حسب التصنيف الدولي المعياري للمهن - 08	الرمز
		حسب التصنيف العربي المعياري للمهن - 08	
		حسب التصنيف الأردني المعياري للمهن - 2021	
هيئة تنمية وتطوير المهارات المهنية والتقنية	موافق عليه من قبل	الشركة الوطنية للتشغيل والتدريب بالتعاون مع الوكالة الألمانية للتعاون الدولي GIZ وشركة إسيلون لتطوير التعليم والتدريب	مطور من خلال
	تاريخ الموافقة		تاريخ المراجعة
800 ساعة تدريبية	عدد الساعات المعتمدة المطلوبة	الإطار الوطني للمؤهلات المستوى الرابع - المسار المهني	مستوى المؤهل الدال
			مؤهل مرجعي رقم
	الرمز		المعايير الوطنية التي ترتبط مع المعايير

6- وصف المعيار

1-6 وصف عام للمعيار المهني لوظيفة / مهنة محلل عمليات أمن سيراني

" هو الشخص الذي يقوم بتحليل العمليات الخاصة بالأمن السيراني والتصدي للهجمات الإلكترونية وإعداد التقارير وتقييم وتنفيذ سياسات واستراتيجيات الأمان لمنع الانتهاكات والتأكد من تأمين كافة البيانات والمعلومات بحسب التعليمات، وضبط ومعايرة الأجهزة بحسب التعليمات والقيم المقررة، وتطبيق إجراءات وتعليمات السلامة والصحة المهنية".

2-6 الغاية من المعايير المهنية لمهنة محلل عمليات أمن سيراني

الغاية من المعايير المهنية لمهنة محلل عمليات أمن سيراني والتي تم إعدادها بمشاركة فاعلة من الخبراء الممارسين في سوق العمل وخبراء التدريب والمدربين في الشركة الوطنية للتشغيل والتدريب والمؤسسات التدريبية في قطاع التدريب والتعليم المهني والتقني هي سد الفجوة بين الكفايات المهنية لخريجي برامج أنظمة تحليل عمليات الأمن سيراني على وجه العموم وخريجي الشركة على وجه الخصوص وما يحتاجه قطاع العمل في مجال تحليل عمليات الأمن سيراني من خلال تصميم برامج تدريبية تؤهل الخريج إلى الانخراط في سوق العمل والمنافسة فيه.

3-6 السياقات التمهيدية وخلفية تطوير المعيار

في ضوء رؤية هيئة تنمية وتطوير المهارات المهنية والتقنية والتي تتمثل في إعداد (قوى بشرية تمتلك المهارة والخبرة المهنية والتقنية تلبي احتياجات سوق العمل وقادرة على المشاركة بالمشاريع الريادية) وتبعا لرسالتها التي تسعى لتنفيذها وهي (تحفيز الشباب على الالتحاق بالتدريب والتعليم المهني والتقني في المملكة مما يساهم في خلق فرص العمل وترسيخ مفهوم ريادة الأعمال وحل مشكلتي الفقر والبطالة والإسهام في النمو الاقتصادي)

وكذلك تبعا لأهدافها المتمثلة في:

- تشجيع جميع أشكال التعلم وتطوير المهارات والاعتراف بها ضمن المنظومة التعليمية وسوق العمل بالإضافة لخلق خيارات جديدة للتعليم والتدريب المهني والتقني ذات مستوى عال بما يتناسب مع مستويات الإطار الوطني للمؤهلات.
- تحسين جودة التعليم والتدريب المهني والتقني من خلال وضع معايير ثابتة لتعيين وتدريب المدربين في القطاع، ومواءمة المعايير وضمان الجودة بين جميع المؤسسات، ورفع مستوى التنسيق مع القطاع الخاص.
- تنويع طرق تمويل قطاع التعليم والتدريب المهني والتقني، بما في ذلك تشجيع الشركات ما بين القطاعين العام والخاص.
- الترويج للتعليم والتدريب المهني والتقني كفرصة ذهبية للتعلم منذ عمر مبكر لضمان العيش الكريم.

وكذلك تبعا لقانون رقم (9) لسنة 2019 قانون تنمية وتطوير المهارات المهنية والتقنية والذي تم اعده بما يتوافق مع توصيات الاستراتيجية الوطنية لتنمية الموارد البشرية (وضع هياكل تنظيمية واضحة لحاكمة

القطاع لضمان اجراء تطبيق المسائلة في انحاء القطاع) وخاصة المادة 3-ب 5- (تنظيم العمل المهني بمستوياته وفق الإطار الوطني للمؤهلات وإجازة ممارسة المهن بالتنسيق مع الجهات المعنية وفق التشريعات المعمول بها).

وكذلك نتائج دراسة وتحليل سوق العمل الأردني الذي أكد وجود فجوة أداء واسعة في بعض وظائف التحكم المبرمجة (PLC)

4-6 المسوغات والمبررات

تبعاً لنتائج تحليل سوق العمل الأردني هناك ضرورة ملحة لتطوير معيار مهني لوظيفة محلل عمليات أمن سيراني / مهني تلبية لاحتياجات سوق العمل المحلي والإقليمي.

5-6 العمليات المنفذة

- تم إجراء تحليل لسوق العمل الأردني وتحديد فجوات الأداء.
- تم التنسيق مع الجهة المانحة (الوكالة الألمانية للتعاون الدولي GIZ) للتمويل.
- تم عقد ورشة عمل (DACUM) بفندق جينيفا 13-15 نوفمبر 2022
- تم عقد اجتماع عمل للمراجعة المبدئية مع هيئة تنمية المهارات المهنية والتقنية.
- تم تطوير المعيار في ضوء نتائج الاجتماع مع هيئة تنمية المهارات المهنية والتقنية.

6-6 الجهات الفاعلية والمؤسسات المشاركة في التنمية

شاركت عدة جهات فاعلة في تطوير المعيار منها مؤسسات دولية مثل: الوكالة الألمانية للتعاون الدولي GIZ وشركة GFA للتدريب والاستشارات بالإضافة إلى مؤسسات أردنية تمثلت في هيئة تنمية المهارات المهنية والتقنية والشركة الوطنية للتشغيل والتدريب وشركة إبسيلون لتطوير التعليم والتدريب وبعض الشركات المتخصصة في المجال.

7-6 ملكية هذه المعايير

كامل ملكية هذه المعايير للوكالة الألمانية للتعاون الدولي (GIZ) وهيئة تنمية وتطوير المهارات المهنية والتقنية.

8-6 عملية التحقق

بعد انتهاء ورشة عمل الداكم وفي اليوم التالي تم عقد ورشة عمل للتحقق من مخطط الداكم وقوائم الداكم وهي نواتج ورشة العمل الأولى.

اشتملت ورشة التحقق من مخطط الداكم وقوائمه على خبراء جدد يتمتعون بمستوى أعلى من الخبرة بالمقارنة مع الذين حضروا ورشة عمل الداكم الأولى في المهنة كما تضمنت عدداً من المشرفين والمهندسين الذين شاركوا وجاهة أو عبر شبكة الإنترنت بالإضافة إلى أعضاء هيئة الداكم الذين حضروا ورشة عمل الداكم الأولى ليكونوا ممثلين عن هيئة الداكم في لجنة التحقق ليفسروا لأعضاء اللجنة ما يحتاجون إليه حين يقومون بفحص ناتج ورشة العمل الأولى. روعي ألا يكون هناك عضو في لجنة التحقق رئيساً أو مشرفاً على أي عضو من أعضاء اللجنة ليكون هناك حرية في الإدلاء بالمعلومات لدى الجميع بنفس الدرجة.

قام الميسر بتصميم مستندات التحقق من مخطط الداكم وقوائمه وتمت طباعة المخطط ومستندات التحقق عقب انتهاء ورشة عمل الداكم. حضر مطوري المناهج الاجتماع مع ممثلين من الهيئة الأولى وخبراء جدد من سوق العمل لم يسبق لهم المشاركة في الهيئة الأولى لمراجعة المخطط الذي تم التوصل اليه والتأكيد على التوافق على كل ما ورد فيه.

9-6 وصف ونطاق المهنة

هذه الوظيفة خاصة بتحليل عمليات الأمن السيراني ويتحدد نطاقها بوظيفة محلل عمليات أمن سيراني / مهني.

10-6 اسم المهنة

محلل عمليات أمن سيراني / المستوى المهني.

11-6 المستوى المهني

المستوى الرابع طبقا للإطار الوطني للمؤهلات في المملكة الأردنية الهاشمية.

12-6 أماكن العمل المحتملة

- جميع القطاعات والشركات في القطاعين العام والخاص - الدوائر الحكومية المدنية والعسكرية
- المصانع
- الجهات الأمنية

13-6 العلاقات مع الشركاء

- وزارة العمل
- النقابات المهنية
- مزودي التدريب والتأهيل
- شركات الإنترنت المحلية والإقليمية والدولية

14-6 القوانين والأنظمة المتعلقة بالمهنة

- قانون تنظيم العمل المهني.
- قانون الضمان الاجتماعي.
- قانون ضريبة الدخل.
- قوانين الاتصال عبر الإنترنت

15-6 الاعتراف بالتعلم المسبق (الخبرات السابقة والمؤهلات التعليمية)

1-15-6 ذوي خبرات ومؤهل جامعي متخصص

المتدربون حاملو الدرجة الجامعية (البكالوريوس) فأعلى في تخصص مرتبط بالبرنامج التدريبي ولديه خبرة أربع سنوات فأكثر يتم إعفاؤه من 50 % من ساعات التدريب المؤسسي بالإضافة إلى 50 % من التدريب الميداني.

2-15-6 ذوي خبرات

المتدربون ذوي خبرة ستة سنوات فأكثر يتم إعفاؤه من 65 % من ساعات التدريب المؤسسي بالإضافة إلى 65 % من التدريب الميداني.

16-6 المخطط التنظيمي للمهنة / العلاقات البيئية



17- المخاوف والنظرة المستقبلية للمهنة:

1-17-6 المخاوف

- ندرة وجود الكفاءات اللازمة لممارسة هذه الوظيفة.
- عدم وجود برامج تدريبية مختصة بمجال المهنة.
- عدم التزام الموظفين بأخلاقيات المهنة وإفشاء سرية المعلومات.
- عدم تطبيق السياسات الأمنية المطلوبة لهذه الوظيفة.

2-17-6 النظرة المستقبلية

- تنظيم قطاع العمل في الأمن السيبراني.
- متابعة اخر المستجدات والتحديات في مجال أمن المعلومات.
- استحداث برامج تدريبية تلائم كافة المستويات العلمية للأفراد.
- تطوير ادوات وحلول محلية لتهديدات السيبرانية على مستوى الدولة.
- زيادة نشر البرامج النوعية حول مخاطر أمن المعلومات الجرائم الإلكترونية لجميع أفراد المجتمع.

18-6 المعايير ومرجعيات المواصفات العالمية

المشتغل في هذه الوظيفة يجب أن يكون على دراية بحدود ما يتعلق بعمله من المعايير العالمية المتعلقة بالوظيفة، ومن الأمثلة عليها:

ISO/IEC 27001	نظام إدارة أمن المعلومات
ISO 90001	نظام إدارة الجودة
ISO 140001	نظام إدارة البيئة
ISO 31000	نظام إدارة المخاطر
Occupational Safety and Health Administration (OSHA)	معياري هيئة السلامة والصحة المهنية

7- الإطار المرجعي للكفايات المهنية / الفنية

وصف الوحدة

وصف الوحدات

رمز المعيار:	OS-SDC-CS1-022	اسم المعيار:	محلل عمليات أمن سيراني / المستوى المهني
--------------	----------------	--------------	---

رمز الوحدة:	UC1	اسم الوحدة:	الوحدة الأولى: استخدام نظام جمع وتحليل البيانات والأحداث السيرانية
-------------	-----	-------------	--

الغاية من وحدة الكفاية: بعد الانتهاء من دراسة هذه الوحدة (الكفاية) والتفاعل مع أنشطتها وخبراتها يجب أن يصبح المتدرب قادراً على:

تعرف آلية التعامل مع النظام وجمع البيانات وتحليلها ومراقبة الشاشات اللازمة والتميز بين المخاطر والتهديدات والعمليات الاعترافية وتصنيف الأحداث حسب رموز درجات الخطورة ومراقبة ومتابعة صحة أداء النظام ومراقبة ومتابعة صحة أداء أجهزة الشبكات.

وحدات الكفاية الوطنية التي تعتمد عليها هذه الوحدة (إن وجدت)

1	
2	

عناصر الكفاية داخل وحدة الكفاية

1	آلية التعامل مع النظام.
---	-------------------------



2	جمع البيانات ويحللها.
3	مراقبة الشاشات اللازمة ويحللها.
4	التمييز بين المخاطر والتهديدات والعمليات الاعترافية ويتعامل معها.
5	تصنيف الأحداث حسب رموز درجات الخطورة.
6	مراقبة ومتابعة صحة أداء النظام.
7	مراقبة ومتابعة صحة أداء أجهزة الشبكات.

وصف الوحدة

وصف الوحدات

محلل عمليات أمن سيراني / المستوى المهني

اسم المعيار:

OS-SDC-CS1-022

رمز المعيار:

الوحدة الثانية: إعداد تقارير يومية دورية حول أهم المخاطر إلى العملاء

اسم الوحدة:

UC2

رمز الوحدة:

الغاية من وحدة الكفاية: بعد الانتهاء من دراسة هذه الوحدة (الكفاية) والتفاعل مع أنشطتها وخبراتها يجب أن يصبح المتدرب قادراً على:

التعامل مع واجهة مراقبة الأحداث من خلال قراءة الشاشات وتدوين الملاحظات وتمييز الأحداث حسب أنواعها وتصنيفها وحسب درجة المخاطر وتمييز حسابات العميل من الحسابات الأخرى وإدراك سياسات العمل في إدارة المخاطر وإتقان استخراج المعلومات حول المخاطر المتعلقة مع العميل في جدول زمني وترتيب مستخرجات النظام حسب تسلسل الأحداث في تقرير يقدم للجهة المعنية.

وحدات الكفاية الوطنية التي تعتمد عليها هذه الوحدة (إن وجدت)

1

2

عناصر الكفاية داخل وحدة الكفاية

التعامل مع واجهة مراقبة الأحداث من خلال قراءة الشاشات ويدون الملاحظات.

1

تمييز الأحداث حسب أنواعها وتصنيفها وحسب درجة المخاطر.

2



تميز حسابات العميل من الحسابات الأخرى.	3
إدراك سياسات العمل في إدارة المخاطر.	4
إتقان استخراج المعلومات حول المخاطر المتعلقة مع العميل في جدول زمني.	5
ترتيب مستخرجات النظام حسب تسلسل الأحداث في تقرير يقدم للجهة المعنية	6

وصف الوحدة

وصف الوحدات

محلل عمليات أمن سيبراني / المستوى المهني

اسم المعيار:

OS-SDC-CS1-022

رمز المعيار:

الوحدة الثالثة: تحديد المخاطر والتهديدات في أنظمة التشغيل وأنظمة الشبكات

اسم الوحدة:

UC3

رمز الوحدة:

الغاية من وحدة الكفاية: بعد الانتهاء من دراسة هذه الوحدة (الكفاية) والتفاعل مع أنشطتها وخبراتها يجب أن يصبح المتدرب قادراً على:

التنسيق مع المختصين حول جاهزية عمل أنظمة التشغيل والشبكات ومراقبة أنظمة التشغيل والشبكات من خلال شاشات النظام وتحديد التهديدات والمخاطر وتصنيفها. تحليل معطيات أنظمة التشغيل المدرجة على النظام تحليلاً أولياً وتتبع تسلسل إجراءات تصنيف المخاطر لأنظمة التشغيل والتميز بين التنبيهات الصحيحة والكاذبة التي تؤثر على نظام الشبكات ومراجعة التهديدات والمخاطر الأكثر تكراراً والتي تؤثر على نظام الشبكات والتشغيل.

وحدات الكفاية الوطنية التي تعتمد عليها هذه الوحدة (إن وجدت)

1

2

عناصر الكفاية داخل وحدة الكفاية



التنسيق مع المختصين حول جاهزية عمل أنظمة التشغيل والشبكات.	1
مراقبة أنظمة التشغيل والشبكات من خلال شاشات النظام.	2
تحديد التهديدات والمخاطر ويصنفها.	3
تحليل معطيات أنظمة التشغيل المدرجة على النظام تحديلاً أولياً.	4
تتبع تسلسل إجراءات تصنيف المخاطر لأنظمة التشغيل.	5
التمييز بين التنبيهات الصحيحة والكاذبة التي تؤثر على نظام الشبكات.	6
مراجعة التهديدات والمخاطر الأكثر تكراراً والتي تؤثر على نظام الشبكات والتشغيل.	7

وصف الوحدة

وصف الوحدات

رمز المعيار:

OS-SDC-CS1-022

اسم المعيار:

محلل عمليات أمن سيبراني / المستوى المهني

رمز الوحدة:

UC4

اسم الوحدة:

الوحدة الرابعة: تحديد التهديدات والمخاطر السيبرانية لموظفي وعملاء الشركة

الغاية من وحدة الكفاية: بعد الانتهاء من دراسة هذه الوحدة (الكفاية) والتفاعل مع أنشطتها وخبراتها يجب أن يصبح المتدرب قادراً على:

مراقبة شاشات النظام وسجل الأحداث المتعلقة بأنظمة التشغيل والشبكات وإعداد قائمة بأنظمة التشغيل والشبكات التي تخص موظفي الشركة وعملاء وتحديد مخاطر وتهديدات الأمن السيبراني المتوقعة ومقارنة المخاطر والتهديدات الحالية بما سبق وحسب الكشف السابق المقدم من المختصين وتتبع التهديدات والتنبيهات الأمنية - إن وجدت- وتحديد الجهة المعنية بالمخاطر والتهديدات سواء عملاء أو موظفين واقتراح الخطط البديلة للتعامل مع التهديدات.

وحدات الكفاية الوطنية التي تعتمد عليها هذه الوحدة (إن وجدت)

1

2

عناصر الكفاية داخل وحدة الكفاية

1

مراقبة شاشات النظام وسجل الأحداث المتعلقة بأنظمة التشغيل والشبكات.



إعداد قائمة بأنظمة التشغيل والشبكات التي تخص موظفي الشركة والعملاء.	2
تحديد مخاطر وتهديدات الأمن السيبراني المتوقعة.	3
مقارنة المخاطر والتهديدات الحالية بما سبق وحسب الكشف السابق المقدم من المختصين.	4
تتبع التهديدات والتنبيهات الأمنية - إن وجدت-	5
تحديد الجهة المعنية بالمخاطر والتهديدات سواء عملاء أو موظفين.	6
اقترح الخطط البديلة للتعامل مع التهديدات.	7

وصف الوحدة

وصف الوحدات

رمز المعيار:

OS-SDC-CS1-022

اسم المعيار:

محلل عمليات أمن سيراني / المستوى المهني

رمز الوحدة:

UC5

اسم الوحدة:

الوحدة الخامسة: تقديم تقرير تحليل المخاطر إلى مسؤول عمليات أمن المعلومات

الغاية من وحدة الكفاية: بعد الانتهاء من دراسة هذه الوحدة (الكفاية) والتفاعل مع أنشطتها وخبراتها يجب أن يصبح المتدرب قادراً على:

التأكد من إدراج جميع الأحداث الصادرة من النظام والتنسيق الأحداث ويكتبها ضمن معايير نموذج التقرير المقرر وتمييز بين ماهية التقارير ويحدد درجة أهميتها و مراجعة تسلسل كتابة عناصر التقرير وتسليم تقرير المخاطر إلى مسؤول أمن المعلومات أو القسم المعني و مناقشة التقرير المقدم منه مع المعنيين و حفظ التقارير والتغذية الراجعة عليها وتزويد نسخ للمعنيين.

وحدات الكفاية الوطنية التي تعتمد عليها هذه الوحدة (إن وجدت)

1

2

عناصر الكفاية داخل وحدة الكفاية

1

التأكد من إدراج جميع الأحداث الصادرة من النظام.

2

التنسيق الأحداث ويكتبها ضمن معايير نموذج التقرير المقرر.



3	تمييز بين ماهية التقارير ويحدد درجة أهميتها.
4	مراجعة تسلسل كتابة عناصر التقرير.
5	تسليم تقرير المخاطر إلى مسؤول أمن المعلومات أو القسم المعني.
6	مناقشة التقرير المقدم منه مع المعنيين.
7	حفظ التقارير والتغذية الراجعة عليها وتزويد نسخ للمعنيين.

وصف الوحدة

وصف الوحدات

رمز المعيار:

OS-SDC-CS1-022

اسم المعيار:

محلل عمليات أمن سيرباني / المستوى المهني

رمز الوحدة:

UC6

اسم الوحدة:

الوحدة السادسة: تنفيذ مسحات حول الثغرات المستجدة

الغاية من وحدة الكفاية: بعد الانتهاء من دراسة هذه الوحدة (الكفاية) والتفاعل مع أنشطتها وخبراتها يجب أن يصبح المتدرب قادراً على:

مراقبة التنبيهات والتهديدات الظاهرة على شاشات النظام واستخدام الأدوات اللازمة للكشف عن الثغرات الأمنية واستخدام قائمة الأصول لتحديد هوية الأنظمة المتعرضة للثغرات المستجدة ومراقبة حدوث أية ثغرة مستجدة على النظام والتنسيق بين التنبيهات الأمنية والفقرات الظاهرة على النظام وتحديد الثغرات الأمنية وأهميتها وتحديد أسماء البرامج التي يمكن أن يستخدمها الدخلاء في نشر كائنات خبيثة وتقديم بلاغ عن الثغرات المحتمل حدوثها.

وحدات الكفاية الوطنية التي تعتمد عليها هذه الوحدة (إن وجدت)

1

2

عناصر الكفاية داخل وحدة الكفاية

1

مراقبة التنبيهات والتهديدات الظاهرة على شاشات النظام.

2

استخدام الأدوات اللازمة للكشف عن الثغرات الأمنية.

3	استخدام قائمة الأصول لتحديد هوية الأنظمة المتعرضة للثغرات المستجدة.
4	مراقبة حدوث أية ثغرة مستجدة على النظام.
5	التنسيق بين التنبيهات الأمنية والفقرات الظاهرة على النظام.
6	تحديد الثغرات الأمنية وأهميتها.
7	تحديد أسماء البرامج التي يمكن أن يستخدمها الدخلاء في نشر كائنات خبيثة.
8	تقديم بلاغ عن الثغرات المحتمل حدوثها.

وصف الوحدة

وصف الوحدات

رمز المعيار:	OS-SDC-CS1-022	اسم المعيار:	محلل عمليات أمن سيبراني / المستوى المهني
--------------	----------------	--------------	--

رمز الوحدة:	UC7	اسم الوحدة:	الوحدة السابعة: التواصل بشأن تصعيد وتبليغ العمليات الخطرة إلى الأقسام المعنية
-------------	-----	-------------	---

الغاية من وحدة الكفاية: بعد الانتهاء من دراسة هذه الوحدة (الكفاية) والتفاعل مع أنشطتها وخبراتها يجب أن يصبح المتدرب قادراً على:

تنفيذ التحليلات على الشبكات والأجهزة للكشف عن أية عمليات خطرة قد تحدث وتجهيز قائمة بأسماء المعنيين (مسؤولين، أقسام) داخل الشركة أو المؤسسة و الإبلاغ عن العمليات الخطرة إلى الأقسام المعنية و تصعيد البلاغ حسب درجة خطورته للمسؤول المعني مباشرة و متابعة إجراءات التصعيد و توثيق البلاغات والإجراءات الأمنية الطارئة و متابعة التحديث على أسماء الأشخاص والجهات المعنية بالتصعيد والبلاغ.

وحدات الكفاية الوطنية التي تعتمد عليها هذه الوحدة (إن وجدت)

1	
2	

عناصر الكفاية داخل وحدة الكفاية

1	تنفيذ التحليلات على الشبكات والأجهزة للكشف عن أية عمليات خطرة قد تحدث.
2	تجهيز قائمة بأسماء المعنيين (مسؤولين، أقسام) داخل الشركة أو المؤسسة.
3	الإبلاغ عن العمليات الخطرة إلى الأقسام المعنية.



تصعيد البلاغ حسب درجة خطورته للمسؤول المعني مباشرة.	4
متابعة إجراءات التصعيد.	5
توثيق البلاغات والإجراءات الأمنية الطارئة.	6
متابعة التحديث على أسماء الأشخاص والجهات المعنية بالتصعيد والبلاغ.	7

وصف الوحدة

وصف الوحدات

رمز المعيار:	OS-SDC-CS1-022	اسم المعيار:	محلل عمليات أمن سيراني / المستوى المهني
رمز الوحدة:	UC8	اسم الوحدة:	الوحدة الثامنة: مراقبة السلوك (للشبكة والمستخدمين) وحركة البيانات

الغاية من وحدة الكفاية: بعد الانتهاء من دراسة هذه الوحدة (الكفاية) والتفاعل مع أنشطتها وخبراتها يجب أن يصبح المتدرب قادراً على:
استخدام أدوات وبرامج مراقبة سلوك الشبكة ومراقبة بيانات حركة الدخول والخروج للنظام أو الشبكة ومراقبة أي نشاط غير معتاد أو عمليات الخروج من النظام أو الشبكة ومتابعة حركة البيانات من حيث مصفوفة الصلاحيات وجمع البيانات من العديد من نقاط البيانات والأجهزة لتقديم تحليل مفصل وملاحظة أية ثغرات في سلوك المستخدمين أو أجهزة الشبكة وتوثيق المتغيرات ضمن سجلات مرتبطة بفترات زمنية.

وحدات الكفاية الوطنية التي تعتمد عليها هذه الوحدة (إن وجدت)

1	
2	

عناصر الكفاية داخل وحدة الكفاية

1	استخدام أدوات وبرامج مراقبة سلوك الشبكة.
2	مراقبة بيانات حركة الدخول والخروج للنظام أو الشبكة.
3	مراقبة أي نشاط غير معتاد أو عمليات الخروج من النظام أو الشبكة.



متابعة حركة البيانات من حيث مصفوفة الصلاحيات.	4
جمع البيانات من العديد من نقاط البيانات والأجهزة لتقديم تحليل مفصل.	5
ملاحظة أية ثغرات في سلوك المستخدمين أو أجهزة الشبكة.	6
توثيق المتغيرات ضمن سجلات مرتبطة بفترات زمنية.	7

وصف الوحدة

وصف الوحدات

محلل عمليات أمن سيراني / المستوى المهني

اسم المعيار:

OS-SDC-CS1-022

رمز المعيار:

الوحدة التاسعة: تطبيق سياسات مركز عمليات أمن المعلومات وحسب وقت مناوبة العمل

اسم الوحدة:

UC9

رمز الوحدة:

الغاية من وحدة الكفاية: بعد الانتهاء من دراسة هذه الوحدة (الكفاية) والتفاعل مع أنشطتها وخبراتها يجب أن يصبح المتدرب قادراً على:

الاطلاع على سياسات أمن المعلومات والمعايير الخاصة بها وتطبيق إجراءات السياسات ويلتزم بها و اختبار التعديلات في السياسات والتأكد من فعاليتها ومتابعة أي تحديث يجري على سياسات أمن المعلومات والإبلاغ عن أية معوقات في السياسات تتعارض أو تعوق سير العمل ومراقبة شبكة وأنظمة التوثيق للتأكد من عدم وجود إخلال في تطبيق السياسات.

وحدات الكفاية الوطنية التي تعتمد عليها هذه الوحدة (إن وجدت)

1

2

عناصر الكفاية داخل وحدة الكفاية

1 الاطلاع على سياسات أمن المعلومات والمعايير الخاصة بها.

1

2 تطبيق إجراءات السياسات ويلتزم بها.

2



اختبار التعديلات في السياسات ويتأكد من فعاليتها.

3

متابعة أي تحديث يجري على سياسات أمن المعلومات.

4

الإبلاغ عن أية معوقات في السياسات تتعارض أو تعوق سير العمل.

5

مراقبة شبكة وأنظمة التوثيق للتأكد من عدم وجود إخلال في تطبيق السياسات.

6

وصف الوحدة

وصف الوحدات

رمز المعيار:	OS-SDC-CS1-022	اسم المعيار:	محلل عمليات أمن سيبراني / المستوى المهني
رمز الوحدة:	UC10	اسم الوحدة:	الوحدة العاشرة: التفاعل مع أحداث الأمن السيبراني

الغاية من وحدة الكفاية: بعد الانتهاء من دراسة هذه الوحدة (الكفاية) والتفاعل مع أنشطتها وخبراتها يجب أن يصبح المتدرب قادراً على:

بدأ إجراءات الاستجابة لأحداث الأمن السيبراني وتقييم الحدث الأمني تقييماً مبدئياً وإبلاغ الرئيس المباشر بالحدث الأمني السيبراني والتواصل مع الأطراف الفاعلة والاحتفاظ بقائمة مكالمات أصحاب المصلحة و احتواء الحادث الأمني في حدود صلاحياته و تتبع مصدر التهديد السيبراني و حفظ دليل الحدث الأمني السيبراني و التقدير المبدئي للأضرار التي نتجت عن الحادث الأمني السيبراني و تأمين نشاط الأجهزة والشبكات و توثيق الخطوات المتخذة لتصحيح الحدث الأمني السيبراني.

وحدات الكفاية الوطنية التي تعتمد عليها هذه الوحدة (إن وجدت)

1	
2	
الغاية من وحدة الكفاية: بعد الانتهاء من دراسة هذه الوحدة (الكفاية) والتفاعل مع أنشطتها وخبراتها يجب أن يصبح المتدرب قادراً على:	
1	بدأ إجراءات الاستجابة لأحداث الأمن السيبراني.
2	تقييم الحدث الأمني تقييماً مبدئياً.
3	إبلاغ الرئيس المباشر بالحدث الأمني السيبراني.

4	التواصل مع الأطراف الفاعلة.
5	الاحتفاظ بقائمة مكالمات أصحاب المصلحة.
6	احتواء الحادث الأمني في حدود صلاحياته.
7	تتبع مصدر التهديد السيبراني.
8	حفظ دليل الحدث الأمني السيبراني.
9	التقدير المبدئي للأضرار التي نتجت عن الحادث الأمني السيبراني.
10	تأمين نشاط الأجهزة والشبكات.
11	توثيق الخطوات المتخذة لتصحيح الحدث الأمني السيبراني.

وصف الوحدات

رمز المعيار:	OS-SDC-CS1-022	اسم المعيار:	محلل عمليات أمن سيبراني / المستوى المهني
رمز الوحدة:	UC11	اسم الوحدة:	الوحدة الحادية عشرة: استقبال طلبات الدعم الفني الخاص بعمليات الأمن السيبراني

الغاية من وحدة الكفاية: بعد الانتهاء من دراسة هذه الوحدة (الكفاية) والتفاعل مع أنشطتها وخبراتها يجب أن يصبح المتدرب قادراً على:

استقبال طلبات الدعم الفني وتصنيفها وتحديد طبيعة الدعم الفني المطلوب وتوصيله إلى القسم المختص وإبلاغ الجهات المعنية بالدعم الفني المطلوب كل حسب تخصصه ومتابعة طلبات الدعم الفني المقدمة من الأقسام المعنية بالأمن السيبراني وتنفيذ المهام والأعمال المطلوبة والمذكورة في طلب الدعم الفني في نطاق اختصاصه وتقديم الدعم والمساعدة الفنية للزملاء في حدود صلاحياته بالأمن السيبراني وتقديم الدعم الفني للزملاء في حدود صلاحياته بالأمن السيبراني وتحديد الأدوات المطلوبة للقيام بأعمال دعم الزملاء ودعم العملاء في حدود صلاحياته بالأمن السيبراني وحفظ البيانات والمعلومات المتعلقة بعمليات الدعم الفني.

وحدات الكفاية الوطنية التي تعتمد عليها هذه الوحدة (إن وجدت)

1	
2	

عناصر الكفاية داخل وحدة الكفاية

1	استقبال طلبات الدعم الفني.
2	تصنيف طلبات الدعم الفني.
3	تحديد طبيعة الدعم الفني المطلوب وتوصيله إلى القسم المختص.
4	إبلاغ الجهات المعنية بالدعم الفني المطلوب كل حسب تخصصه.



متابعة طلبات الدعم الفني المقدمة من الأقسام المعنية بالأمن السيبراني.	5
تنفيذ المهام والأعمال المطلوبة والمذكورة في طلب الدعم الفني في نطاق اختصاصه.	6
تقديم الدعم والمساعدة الفنية للزملاء في حدود صلاحياته بالأمن السيبراني.	7
تقديم الدعم الفني للعملاء في حدود صلاحياته بالأمن السيبراني.	8
تحديد الأدوات المطلوبة للقيام بأعمال دعم الزملاء في حدود صلاحياته بالأمن السيبراني.	9
تحديد الأدوات المطلوبة للقيام بأعمال دعم العملاء في حدود صلاحياته بالأمن السيبراني.	10
حفظ البيانات والمعلومات المتعلقة بعمليات الدعم الفني.	11

محلل عمليات أمن سيبراني - المستوى المهني

قائمة الوحدات وعناصر الكفايات

رقم الوحدة	اسم وحدة الكفاية	رقم العنصر	اسم عنصر الكفاية	معيار الأداء على أساس العمليات	معيار الأداء على أساس المنتج
UC1	الوحدة الأولى: استخدام نظام جمع وتحليل البيانات والأحداث السبيرانية	EC1.1	آلية التعامل مع النظام.	طبقا للإجراءات	عدم إلحاق الضرر بأجهزة النظام
		EC1.2	جمع البيانات وتحليلها.	طبقا للإجراءات	تحليل البيانات كامل
		EC1.3	مراقبة الشاشات اللازمة ويحللها.	طبقا للإجراءات	تحليل الشاشات كامل
		EC1.4	التمييز بين المخاطر والتهديدات والعمليات الاعترافية ويتعامل معها.	طبقا للإجراءات	المخاطر والتهديدات والعمليات الاعترافية محددة بدقة.
		EC1.5	تصنيف الأحداث حسب رموز درجات الخطورة.	حسب الكاتلوج & المخطط	الأحداث مصنفة حسب رموز درجات الخطورة.
		EC1.6	مراقبة ومتابعة صحة أداء النظام.	حسب الكاتلوج & المخطط	النظام يعمل بكفاءة
		EC1.7	مراقبة ومتابعة صحة أداء أجهزة الشبكات.	طبقا للإجراءات	النظام يعمل بكفاءة

معزز المعرفة

آلية التعامل مع النظام.
جمع البيانات وتحليلها.
مراقبة الشاشات اللازمة ويحللها.
التمييز بين المخاطر والتهديدات
والعمليات الاعترافية ويتعامل معها.
تصنيف الأحداث حسب رموز درجات
الخطورة.
مراقبة ومتابعة صحة أداء النظام.
مراقبة ومتابعة صحة أداء أجهزة
الشبكات.

معزز المهارات الأساسية الحياتية والعمل

الالتزام والانضباط
الاتصال والتواصل
أساسيات اللغة الانجليزية
مهارات الحاسوب واستخدام الانترنت
احترام وخصوصية مكان العمل
الالتزام بأخلاقيات العمل

شروط ومتطلبات الأداء

أجهزة النظام
نموذج تحليل البيانات
نموذج تحليل الشاشات
نموذج تحديد المخاطر والتهديدات
والعمليات الاعترافية.
نموذج تصنيف الأحداث حسب رموز
درجات الخطورة.
التهوية والاضاءة الجيدة في بيئة العمل
التقيد باللوائح والتعليمات المتعلقة
بالسلامة (الشركة & موقع العمل)
توفر معدات السلامة والصحة المهنية

إرشادات للتقييم

الاختبار (شفهي - تحريري) الملاحظة
والمراقبة وفق لوائح الرصد

محلل عمليات أمن سيراني - المستوى المهني

قائمة الوحدات وعناصر الكفايات

رقم الوحدة	اسم وحدة الكفاية	رقم العنصر	اسم عنصر الكفاية	معياري الأداء على أساس العمليات	معياري الأداء على أساس المنتج
UC2	الوحدة الثانية: إعداد تقارير يومية دورية حول أهم المخاطر إلى العملاء	EC2.1	التعامل مع واجهة مراقبة الأحداث من خلال قراءة الشاشات ويدون الملاحظات.	طبقا للإجراءات	ملاحظات واجهة مراقبة الأحداث من خلال قراءة الشاشات.
		EC2.2	تمييز الأحداث حسب أنواعها وتصنيفها وحسب درجة المخاطر.	طبقا للإجراءات	الأحداث مميزة حسب أنواعها وتصنيفها وحسب درجة المخاطر.
		EC2.3	تمييز حسابات العميل من الحسابات الأخرى.	طبقا للإجراءات	حسابات العميل مميزة من الحسابات الأخرى.
		EC2.4	إدراك سياسات العمل في إدارة المخاطر.	طبقا للإجراءات	تطبيق سياسات العمل في إدارة المخاطر بصورة واضحة.
		EC2.5	إتقان استخراج المعلومات حول المخاطر المتعلقة مع العميل في جدول زمني.	حسب الكاتلوج & المخطط	استيفاء المعلومات حول المخاطر المتعلقة مع العميل في جدول زمني.
		EC2.6	ترتيب مستخرجات النظام حسب تسلسل الأحداث في تقرير يقدم للجهة المعنية	حسب الكاتلوج & المخطط	ترتيب مستخرجات النظام حسب تسلسل الأحداث في تقرير يقدم للجهة المعنية

شروط ومتطلبات الأداء

معزز المعرفة

نموذج ملاحظات واجهة مراقبة الأحداث
من خلال قراءة الشاشات.
نموذج تمييز الأحداث حسب أنواعها
وتصنيفها وحسب درجة المخاطر.
نموذج تمييز حسابات العميل من
الحسابات الأخرى.
سياسات العمل في إدارة المخاطر.
استيفاء المعلومات حول المخاطر
المتعلقة مع العميل في جدول زمني.
ترتيب مستخرجات النظام حسب تسلسل
الأحداث في تقرير يقدم للجهة المعنية
التهوية والاضاءة الجيدة في بيئة العمل
التقيد باللوائح والتعليمات المتعلقة
بالسلامة (الشركة & موقع العمل)
توفر معدات السلامة والصحة المهنية
إرشادات للتقييم

الاختبار (شفهي - تحريري) الملاحظة
والمراقبة وفق لوائح الرصد

التعامل مع واجهة مراقبة الأحداث من
خلال قراءة الشاشات ويدون
الملاحظات.
تمييز الأحداث حسب أنواعها وتصنيفها
وحسب درجة المخاطر.
تمييز حسابات العميل من الحسابات
الأخرى.
إدراك سياسات العمل في إدارة المخاطر.
إتقان استخراج المعلومات حول
المخاطر المتعلقة مع العميل في جدول
زمني.
ترتيب مستخرجات النظام حسب
تسلسل الأحداث في تقرير يقدم للجهة
المعنية
معزز المهارات الأساسية الحياتية والعمل

الالتزام والانضباط
الاتصال والتواصل
أساسيات اللغة الانجليزية
مهارات الحاسوب واستخدام الانترنت
احترام وخصوصية مكان العمل
الالتزام بأخلاقيات العمل

محلل عمليات أمن سيرباني - المستوى المهني

قائمة الوحدات وعناصر الكفايات

رقم الوحدة	اسم وحدة الكفاية	رقم العنصر	اسم عنصر الكفاية	معيار الأداء على أساس العمليات	معيار الأداء على أساس المنتج
UC3	الوحدة الثالثة: تحديد المخاطر والتهديدات في أنظمة التشغيل وأنظمة الشبكات	EC3.1	التنسيق مع المختصين حول جاهزية عمل أنظمة التشغيل والشبكات.	طبقا للإجراءات	تمام التنسيق مع المختصين حول جاهزية عمل أنظمة التشغيل والشبكات.
		EC3.2	مراقبة أنظمة التشغيل والشبكات من خلال شاشات النظام.	طبقا للإجراءات	استيفاء نموذج مراقبة أنظمة التشغيل والشبكات من خلال شاشات النظام.
		EC3.3	تحديد التهديدات والمخاطر ويصنفها.	طبقا للإجراءات	استيفاء نموذج تحديد التهديدات والمخاطر وتصنيفها.
		EC3.4	تحليل معطيات أنظمة التشغيل المدرجة على النظام تحليلا أوليا.	طبقا للإجراءات	استفاء نموذج تحليل معطيات أنظمة التشغيل المدرجة على النظام تحليلا أوليا.
		EC3.5	تتبع تسلسل إجراءات تصنيف المخاطر لأنظمة التشغيل.	حسب الكاتلوج & المخطط	تسلسل إجراءات تصنيف المخاطر لأنظمة التشغيل متتبعه حسب المخطط.

التنبهات الصحيحة والكاذبة التي تؤثر على نظام الشبكات مميزة حسب المخطط.	حسب الكاتلوج & المخطط	التمييز بين التنبهات الصحيحة والكاذبة التي تؤثر على نظام الشبكات.	EC3.6
التهديدات والمخاطر الأكثر تكرارا والتي تؤثر على نظام الشبكات والتشغيل محددة ومراجعة باستمرار.	طبقا للإجراءات	مراجعة التهديدات والمخاطر الأكثر تكرارا والتي تؤثر على نظام الشبكات والتشغيل.	EC3.7

شروط ومتطلبات الأداء

نموذج التنسيق مع المختصين حول جاهزية عمل أنظمة التشغيل والشبكات. نموذج مراقبة أنظمة التشغيل والشبكات من خلال شاشات النظام. نموذج تحديد التهديدات والمخاطر وتصنيفها. نموذج تحليل معطيات أنظمة التشغيل المدرجة على النظام تحليلا أوليا. المدرجة على النظام تحليلا أوليا. نموذج تتبع تسلسل إجراءات تصنيف المخاطر لأنظمة التشغيل. نموذج تمييز التنبهات الصحيحة والكاذبة التي تؤثر على نظام الشبكات. نموذج تحديد ومراجعة التهديدات والمخاطر الأكثر تكرارا والتي تؤثر على نظام الشبكات والتشغيل. التهوية والاضاءة الجيدة في بيئة العمل التقيد باللوائح والتعليمات المتعلقة

معزز المعرفة

التنسيق مع المختصين حول جاهزية عمل أنظمة التشغيل والشبكات. مراقبة أنظمة التشغيل والشبكات من خلال شاشات النظام. تحديد التهديدات والمخاطر ويصنفها. تحليل معطيات أنظمة التشغيل المدرجة على النظام تحليلا أوليا. تتبع تسلسل إجراءات تصنيف المخاطر لأنظمة التشغيل. التمييز بين التنبهات الصحيحة والكاذبة التي تؤثر على نظام الشبكات. مراجعة التهديدات والمخاطر الأكثر تكرارا والتي تؤثر على نظام الشبكات والتشغيل.

بالسلامة (الشركة & موقع العمل)
توفر معدات السلامة والصحة المهنية

إرشادات للتقييم

الاختبار (شفهي - تحريري) الملاحظة
والمراقبة وفق لوائح الرصد

معزز المهارات الأساسية الحياتية والعمل

الالتزام والانضباط
الاتصال والتواصل
أساسيات اللغة الانجليزية
مهارات الحاسوب واستخدام الانترنت
احترام وخصوصية مكان العمل
الالتزام بأخلاقيات العمل

محلل عمليات أمن سيراني - المستوى المهني

قائمة الوحدات وعناصر الكفايات

رقم الوحدة	اسم وحدة الكفاية	رقم العنصر	اسم عنصر الكفاية	معييار الأداء على أساس العمليات	معييار الأداء على أساس المنتج
UC4	الوحدة الرابعة: تحديد التهديدات والمخاطر السيرانية لموظفي وعملاء الشركة	EC4.1	مراقبة شاشات النظام وسجل الأحداث المتعلقة بأنظمة التشغيل والشبكات.	طبقا للإجراءات	شاشات النظام مراقبة وتم تسجيل الأحداث المتعلقة بأنظمة التشغيل والشبكات.
		EC4.2	إعداد قائمة بأنظمة التشغيل والشبكات التي تخص موظفي الشركة والعملاء.	طبقا للإجراءات	قائمة بأنظمة التشغيل والشبكات التي تخص موظفي الشركة والعملاء مستوفاة بدقة.
		EC4.3	تحديد مخاطر وتهديدات الأمن السيراني المتوقعة.	طبقا للإجراءات	مخاطر وتهديدات الأمن السيراني المتوقعة محددة بدقة.
		EC4.4	مقارنة المخاطر والتهديدات الحالية بما سبق وحسب الكشف السابق المقدم من المختصين.	طبقا للإجراءات	المخاطر والتهديدات الحالية تمت مقارنتها بما سبق وحسب الكشف السابق المقدم من المختصين.
		EC4.5	تتبع التهديدات والتنبيهات الأمنية - إن وجدت-	حسب الكاتلوج & المخطط	التهديدات والتنبيهات الأمنية - إن وجدت- متتبعة حسب المخطط.

الجهة المعنية بالمخاطر والتهديدات سواء عملاء أو موظفين محددة.	حسب الكاتلوج & المخطط	تحديد الجهة المعنية بالمخاطر والتهديدات سواء عملاء أو موظفين.	EC4.6
الخطط البديلة للتعامل مع التهديدات موجودة وجاهزة للتطبيق.	طبقا للإجراءات	اقتراح الخطط البديلة للتعامل مع التهديدات.	EC4.7

شروط ومتطلبات الأداء

نموذج مراقبة شاشات النظام.
قائمة بأنظمة التشغيل والشبكات التي تخص موظفي الشركة والعملاء.
نموذج تحديد مخاطر وتهديدات الأمن السيبراني المتوقعة.
نموذج مقارنة المخاطر والتهديدات الحالية بما سبق.
نموذج تتبع التهديدات والتنبيهات الأمنية - إن وجدت-
بيانات اتصال الجهة المعنية بالمخاطر والتهديدات سواء عملاء أو موظفين.
نموذج الخطط البديلة للتعامل مع التهديدات.
التهوية والاضاءة الجيدة في بيئة العمل
التقيد باللوائح والتعليمات المتعلقة بالسلامة (الشركة & موقع العمل)
توفر معدات السلامة والصحة المهنية

إرشادات للتقييم

معزز المعرفة

مراقبة شاشات النظام وسجل الأحداث المتعلقة بأنظمة التشغيل والشبكات.
إعداد قائمة بأنظمة التشغيل والشبكات التي تخص موظفي الشركة والعملاء.
تحديد مخاطر وتهديدات الأمن السيبراني المتوقعة.
مقارنة المخاطر والتهديدات الحالية بما سبق وحسب الكشف السابق المقدم من المختصين.
تتبع التهديدات والتنبيهات الأمنية - إن وجدت-
تحديد الجهة المعنية بالمخاطر والتهديدات سواء عملاء أو موظفين.
اقتراح الخطط البديلة للتعامل مع التهديدات.

معزز المهارات الأساسية الحياتية والعمل

الالتزام والانضباط

الاتصال والتواصل

أساسيات اللغة الانجليزية

مهارات الحاسوب واستخدام الانترنت

احترام وخصوصية مكان العمل

الالتزام بأخلاقيات العمل

الاختبار (شفهي - تحريري) الملاحظة
والمراقبة وفق لوائح الرصد

محلل عمليات أمن سيبراني - المستوى المهني

قائمة الوحدات وعناصر الكفايات

رقم الوحدة	اسم وحدة الكفاية	رقم العنصر	اسم عنصر الكفاية	معيار الأداء على أساس العمليات	معيار الأداء على أساس المنتج
UC5	الوحدة الخامسة: تقديم تقرير تحليل المخاطر إلى مسؤول عمليات أمن المعلومات	EC5.1	التأكد من إدراج جميع الأحداث الصادرة من النظام.	طبقا للإجراءات	إدراج جميع الأحداث الصادرة من النظام.
		EC5.2	تنسيق الأحداث ويكتبها ضمن معايير نموذج التقرير المقرر.	طبقا للإجراءات	الأحداث منسقة ومكتوبة ضمن معايير نموذج التقرير المقرر.
		EC5.3	تمييز بين ماهية التقارير ويحدد درجة أهميتها.	طبقا للإجراءات	التقارير مميزة ومحدد درجة أهميتها.
		EC5.4	مراجعة تسلسل كتابة عناصر التقرير.	طبقا للإجراءات	تسلسل كتابة عناصر التقرير مراجعة بدقة
		EC5.5	تسليم تقرير المخاطر إلى مسؤول أمن المعلومات أو القسم المعني.	حسب الكاتلوج & المخطط	تقرير المخاطر تم تسليمه إلى مسؤول أمن المعلومات أو القسم المعني.
		EC5.6	مناقشة التقرير المقدم منه مع المعنيين.	حسب الكاتلوج & المخطط	تمت مناقشة التقرير المقدم مع المعنيين.

التقارير محفوظة والتغذية الراجعة عليها وتم تزويد نسخ للمعنيين.	طبقا للإجراءات	حفظ التقارير والتغذية الراجعة عليها وتزويد نسخ للمعنيين.	EC5.7		
--	----------------	--	-------	--	--

شروط ومتطلبات الأداء

نموذج إدراج جميع الأحداث الصادرة من النظام.
نموذج تنسيق الأحداث ضمن معايير نموذج التقرير المقرر.
نموذج للتقارير محدد به درجة أهميتها.
نموذج تسلسل كتابة عناصر التقرير.
نموذج تسليم تقرير المخاطر إلى مسؤول أمن المعلومات أو القسم المعني.
خريطة مكان حفظ التقارير والتغذية الراجعة.
التهوية والاضاءة الجيدة في بيئة العمل
التقيد باللوائح والتعليمات المتعلقة بالسلامة (الشركة & موقع العمل)
توفر معدات السلامة والصحة المهنية

إرشادات للتقييم

الاختبار (شفهي - تحريري) الملاحظة والمراقبة وفق لوائح الرصد

معزز المعرفة

التأكد من إدراج جميع الأحداث الصادرة من النظام.
التنسيق الأحداث ويكتبها ضمن معايير نموذج التقرير المقرر.
تمييز بين ماهية التقارير ويحدد درجة أهميتها.
مراجعة تسلسل كتابة عناصر التقرير.
تسليم تقرير المخاطر إلى مسؤول أمن المعلومات أو القسم المعني.
مناقشة التقرير المقدم منه مع المعنيين.
حفظ التقارير والتغذية الراجعة عليها وتزويد نسخ للمعنيين.

معزز المهارات الأساسية الحياتية والعمل

الالتزام والانضباط
الاتصال والتواصل
أساسيات اللغة الانجليزية
مهارات الحاسوب واستخدام الانترنت
احترام وخصوصية مكان العمل
الالتزام بأخلاقيات العمل

محلل عمليات أمن سيبراني - المستوى المهني

قائمة الوحدات وعناصر الكفايات

رقم الوحدة	اسم وحدة الكفاية	رقم العنصر	اسم عنصر الكفاية	معياري الأداء على أساس العمليات	معياري الأداء على أساس المنتج
UC6	الوحدة السادسة: تنفيذ مسحات حول الثغرات المستجدة	EC6.1	مراقبة التنبيهات والتهديدات الظاهرة على شاشات النظام.	طبقا للإجراءات	نموذج مراقبة التنبيهات والتهديدات الظاهرة على شاشات النظام مستوفي.
		EC6.2	استخدام الأدوات اللازمة للكشف عن الثغرات الأمنية.	طبقا للإجراءات	الأدوات اللازمة للكشف عن الثغرات الأمنية مستخدمة بطريقة صحيحة.
		EC6.3	استخدام قائمة الأصول لتحديد هوية الأنظمة المتعرضة للثغرات المستجدة.	طبقا للإجراءات	قائمة الأصول لتحديد هوية الأنظمة المتعرضة للثغرات المستجدة مستخدمة بطريقة صحيحة.
		EC6.4	مراقبة حدوث أية ثغرة مستجدة على النظام.	طبقا للإجراءات	نموذج مراقبة حدوث أية ثغرة مستجدة على النظام.

التنبيهات الأمنية والفقرات الظاهرة على النظام مسجلة.	طبقا للإجراءات	التنسيق ما بين التنبيهات الأمنية والفقرات الظاهرة على النظام.	EC6.5
الثغرات الأمنية محددة .	حسب الكاتلوج & المخطط	تحديد الثغرات الأمنية وأهميتها.	EC6.6
أسماء البرامج التي يمكن أن يستخدمها الدخلاء في نشر كائنات خبيثة محددة بدقة.	حسب الكاتلوج & المخطط	تحديد أسماء البرامج التي يمكن أن يستخدمها الدخلاء في نشر كائنات خبيثة.	EC6.7
البلاغ عن الثغرات المحتمل حدوثها مسجل بدقة	طبقا للإجراءات	تقديم بلاغ عن الثغرات المحتمل حدوثها.	EC6.8

شروط ومتطلبات الأداء

نموذج مراقبة التنبيهات والتهديدات الظاهرة على شاشات النظام.
الأدوات اللازمة للكشف عن الثغرات الأمنية.
قائمة الأصول لتحديد هوية الأنظمة المتعرضة للثغرات المستجدة.
نموذج مراقبة حدوث أية ثغرة مستجدة على النظام.
نموذج تسجيل التنبيهات الأمنية والفقرات الظاهرة على النظام.
الثغرات الأمنية.
أسماء البرامج التي يمكن أن يستخدمها الدخلاء في نشر كائنات خبيثة.
نموذج تسجيل البلاغ عن الثغرات المحتمل حدوثها.

معزز المعرفة

مراقبة التنبيهات والتهديدات الظاهرة على شاشات النظام.
استخدام الأدوات اللازمة للكشف عن الثغرات الأمنية.
استخدام قائمة الأصول لتحديد هوية الأنظمة المتعرضة للثغرات المستجدة.
مراقبة حدوث أية ثغرة مستجدة على النظام.
التنسيق ما بين التنبيهات الأمنية والفقرات الظاهرة على النظام.
تحديد الثغرات الأمنية وأهميتها.
تحديد أسماء البرامج التي يمكن أن يستخدمها الدخلاء في نشر كائنات خبيثة.
تقديم بلاغ عن الثغرات المحتمل حدوثها.

التهوية والاضاءة الجيدة في بيئة العمل
التقيد باللوائح والتعليمات المتعلقة
بالسلامة (الشركة & موقع العمل)
توفر معدات السلامة والصحة المهنية

إرشادات للتقييم

الاختبار (شفهي - تحريري) الملاحظة
والمراقبة وفق لوائح الرصد

معزز المهارات الأساسية الحياتية والعمل

الالتزام والانضباط
الاتصال والتواصل
أساسيات اللغة الانجليزية
مهارات الحاسوب واستخدام الانترنت
احترام وخصوصية مكان العمل
الالتزام بأخلاقيات العمل

محلل عمليات أمن سيبراني - المستوى المهني

قائمة الوحدات وعناصر الكفايات

رقم الوحدة	اسم وحدة الكفاية	رقم العنصر	اسم عنصر الكفاية	معيار الأداء على أساس العمليات	معيار الأداء على أساس المنتج
UC7	الوحدة السابعة: التواصل بشأن تصعيد وتبليغ العمليات الخطرة إلى الأقسام المعنية	EC7.1	تنفيذ التحليلات على الشبكات والأجهزة للكشف عن أية عمليات خطيرة قد تحدث.	طبقا للإجراءات	التحليلات على الشبكات والأجهزة للكشف عن أية عمليات خطيرة قد تحدث منفذة بدقة.
		EC7.2	تجهيز قائمة بأسماء المعنيين (مسؤولين، أقسام) داخل الشركة أو المؤسسة.	طبقا للإجراءات	قائمة بأسماء المعنيين (مسؤولين، أقسام) داخل الشركة أو المؤسسة مجهزة.
		EC7.3	الإبلاغ عن العمليات الخطرة إلى الأقسام المعنية.	طبقا للإجراءات	تم الإبلاغ عن العمليات الخطرة إلى الأقسام المعنية حسب الإجراءات.
		EC7.4	تصعيد البلاغ حسب درجة خطورته للمسؤول المعني مباشرة.	طبقا للإجراءات	البلاغ تم تصعيده حسب درجة خطورته للمسؤول المعني مباشرة .
		EC7.5	متابعة إجراءات التصعيد.	حسب الكاتلوج & المخطط	تمت متابعة إجراءات التصعيد.

البلاغات والإجراءات الأمنية الطارئة موثقة.	حسب الكاتلوج & المخطط	توثيق البلاغات والإجراءات الأمنية الطارئة.	EC7.6	
التحديث على أسماء الأشخاص والجهات المعنية بالتصعيد والبلاغ يتم أولاً بأول.	طبقاً للإجراءات	متابعة التحديث على أسماء الأشخاص والجهات المعنية بالتصعيد والبلاغ.	EC7.7	

شروط ومتطلبات الأداء

نموذج تنفيذ التحليلات على الشبكات والأجهزة للكشف عن أية عمليات خطرة قد تحدث.
قائمة بأسماء المعنيين (مسؤولين، أقسام) داخل الشركة أو المؤسسة.
نموذج الإبلاغ عن العمليات الخطرة إلى الأقسام المعنية.
نموذج البلاغ حسب درجة خطورته.
نماذج إجراءات التصعيد.
نموذج توثيق البلاغات والإجراءات الأمنية الطارئة.
نموذج تحديث أسماء الأشخاص والجهات المعنية بالتصعيد والبلاغ.
التهوية والاضاءة الجيدة في بيئة العمل
التقيد باللوائح والتعليمات المتعلقة بالسلامة (الشركة & موقع العمل)
توفر معدات السلامة والصحة المهنية

إرشادات للتقييم

معزز المعرفة

تنفيذ التحليلات على الشبكات والأجهزة للكشف عن أية عمليات خطرة قد تحدث.
تجهيز قائمة بأسماء المعنيين (مسؤولين، أقسام) داخل الشركة أو المؤسسة.
الإبلاغ عن العمليات الخطرة إلى الأقسام المعنية.
تصعيد البلاغ حسب درجة خطورته للمسؤول المعني مباشرة.
متابعة إجراءات التصعيد.
توثيق البلاغات والإجراءات الأمنية الطارئة.
متابعة التحديث على أسماء الأشخاص والجهات المعنية بالتصعيد والبلاغ.

معزز المهارات الأساسية الحياتية والعمل

الاختبار (شفهي - تحريري) الملاحظة
والمراقبة وفق لوائح الرصد

محلل عمليات أمن سيراني - المستوى المهني

قائمة الوحدات وعناصر الكفايات

رقم الوحدة	اسم وحدة الكفاية	رقم العنصر	اسم عنصر الكفاية	معيار الأداء على أساس العمليات	معيار الأداء على أساس المنتج
UC8	الوحدة الثامنة: مراقبة السلوك (للشبكة والمستخدمين) وحركة البيانات	EC8.1	استخدام أدوات وبرامج مراقبة سلوك الشبكة.	طبقا للإجراءات	أدوات وبرامج مراقبة سلوك الشبكة مستخدمة.
		EC8.2	مراقبة بيانات حركة الدخول والخروج للنظام أو الشبكة.	طبقا للإجراءات	نماذج مراقبة بيانات حركة الدخول والخروج للنظام أو الشبكة مستوفاة.
		EC8.3	مراقبة أي نشاط غير معتاد أو عمليات الخروج من النظام أو الشبكة.	طبقا للإجراءات	نماذج مراقبة أي نشاط غير معتاد أو عمليات الخروج من النظام أو الشبكة مستوفاة.

نماذج متابعة حركة البيانات من حيث مصفوفة الصلاحيات مستوفاة.	طبقا للإجراءات	متابعة حركة البيانات من حيث مصفوفة الصلاحيات.	EC8.4
نماذج جمع البيانات من العديد من نقاط البيانات والأجهزة لتقديم تحليل مفصل مستوفاة.	حسب الكاتلوج & المخطط	جمع البيانات من العديد من نقاط البيانات والأجهزة لتقديم تحليل مفصل.	EC8.5
نموذج ملاحظة أية ثغرات في سلوك المستخدمين أو أجهزة الشبكة مستوفي.	حسب الكاتلوج & المخطط	ملاحظة أية ثغرات في سلوك المستخدمين أو أجهزة الشبكة.	EC8.6
نماذج توثيق المتغيرات ضمن سجلات مرتبطة بفترات زمنية مستوفاة.	طبقا للإجراءات	توثيق المتغيرات ضمن سجلات مرتبطة بفترات زمنية.	EC8.7

شروط ومتطلبات الأداء

أدوات وبرامج مراقبة سلوك الشبكة.
نماذج مراقبة بيانات حركة الدخول والخروج للنظام أو الشبكة.
نماذج مراقبة أي نشاط غير معتاد أو عمليات الخروج من النظام أو الشبكة.
نماذج متابعة حركة البيانات من حيث مصفوفة الصلاحيات.
نماذج جمع البيانات من العديد من نقاط البيانات والأجهزة لتقديم تحليل مفصل.
نموذج ملاحظة أية ثغرات في سلوك المستخدمين أو أجهزة الشبكة.

معزز المعرفة

استخدام أدوات وبرامج مراقبة سلوك الشبكة.
مراقبة بيانات حركة الدخول والخروج للنظام أو الشبكة.
مراقبة أي نشاط غير معتاد أو عمليات الخروج من النظام أو الشبكة.
متابعة حركة البيانات من حيث مصفوفة الصلاحيات.
جمع البيانات من العديد من نقاط البيانات والأجهزة لتقديم تحليل مفصل.
ملاحظة أية ثغرات في سلوك

المستخدمين أو أجهزة الشبكة.
توثيق المتغيرات ضمن سجلات مرتبطة
بفترات زمنية.

نماذج توثيق المتغيرات ضمن سجلات
مرتبطة بفترات زمنية.
التهوية والاضاءة الجيدة في بيئة العمل
التقيد باللوائح والتعليمات المتعلقة
بالسلامة (الشركة & موقع العمل)
توفر معدات السلامة والصحة المهنية

إرشادات للتقييم

معزز المهارات الأساسية الحياتية والعمل

الالتزام والانضباط

الاتصال والتواصل

أساسيات اللغة الانجليزية

مهارات الحاسوب واستخدام الانترنت

احترام وخصوصية مكان العمل

الالتزام بأخلاقيات العمل

الاختبار (شفهي - تحريري) الملاحظة
والمراقبة وفق لوائح الرصد

محلل عمليات أمن سيراني - المستوى المهني

قائمة الوحدات وعناصر الكفايات

رقم الوحدة	اسم وحدة الكفاية	رقم العنصر	اسم عنصر الكفاية	معيار الأداء على أساس العمليات	معيار الأداء على أساس المنتج
UC9	الوحدة التاسعة: تطبيق سياسات مركز عمليات أمن المعلومات وحسب وقت مناوبة العمل	EC9.1	الاطلاع على سياسات أمن المعلومات والمعايير الخاصة بها.	طبقا للإجراءات	سياسات أمن المعلومات والمعايير الخاصة بها تم الاطلاع عليها واستيعابها.
		EC9.2	تطبيق إجراءات السياسات ويلتزم بها.	طبقا للإجراءات	إجراءات السياسات مطبقة وملتزم بها.
		EC9.3	اختبار التعديلات في السياسات ويتأكد من فعاليتها.	طبقا للإجراءات	اختبار التعديلات في السياسات تم تنفيذه وتم التأكد من فعاليتها.
		EC9.4	متابعة أي تحديث يجري على سياسات أمن المعلومات.	طبقا للإجراءات	أي تحديث يجري على سياسات أمن المعلومات يتم متابعته.

أية معوقات في السياسات تتعارض أو تعوق سير العمل يتم رصدها والإبلاغ عنها.	حسب الكاتلوج & المخطط	الإبلاغ عن أية معوقات في السياسات تتعارض أو تعوق سير العمل.	EC9.5
سجل مراقبة شبكة وأنظمة التوثيق للتأكد من عدم وجود إخلال في تطبيق السياسات مستوفي جميع العناصر.	حسب الكاتلوج & المخطط	مراقبة شبكة وأنظمة التوثيق للتأكد من عدم وجود إخلال في تطبيق السياسات.	EC9.6

شروط ومتطلبات الأداء

سياسات أمن المعلومات والمعايير الخاصة بها.
إجراءات السياسات.
اختبار التعديلات في السياسات.
سجل متابعة تحديثات سياسات أمن المعلومات.
سجل رصد معوقات في السياسات.
سجل مراقبة شبكة وأنظمة التوثيق.
التهوية والاضاءة الجيدة في بيئة العمل
التقيد باللوائح والتعليمات المتعلقة
بالسلامة (الشركة & موقع العمل)
توفر معدات السلامة والصحة المهنية

إرشادات للتقييم

الاختبار (شفهي - تحريري) الملاحظة
والمراقبة وفق لوائح الرصد

معزز المعرفة

الاطلاع على سياسات أمن المعلومات والمعايير الخاصة بها.
تطبيق إجراءات السياسات ويلتزم بها.
اختبار التعديلات في السياسات ويتأكد من فعاليتها.
متابعة أي تحديث يجري على سياسات أمن المعلومات.
الإبلاغ عن أية معوقات في السياسات تتعارض أو تعوق سير العمل.
مراقبة شبكة وأنظمة التوثيق للتأكد من عدم وجود إخلال في تطبيق السياسات.

معزز المهارات الأساسية الحياتية والعمل

الالتزام والانضباط
الاتصال والتواصل
أساسيات اللغة الانجليزية

محلل عمليات أمن سيراني - المستوى المهني

قائمة الوحدات وعناصر الكفايات

رقم الوحدة	اسم وحدة الكفاية	رقم العنصر	اسم عنصر الكفاية	معيار الأداء على أساس العمليات	معيار الأداء على أساس المنتج
UC10	الوحدة العاشرة: التفاعل مع أحداث الأمن السيراني	EC10.1	بدأ إجراءات الاستجابة لأحداث الأمن السيراني.	طبقا للإجراءات	إجراءات الاستجابة لأحداث الأمن السيراني منفذة.
		EC10.2	تقييم الحدث الأمني تقييما مبدئيا.	طبقا للإجراءات	تقييم الحدث الأمني تقييما مبدئيا منفذ بدقة.
		EC10.3	إبلاغ الرئيس المباشر بالحدث الأمني السيراني.	طبقا للإجراءات	تم إبلاغ الرئيس المباشر بالحدث الأمني السيراني.
		EC10.4	التواصل مع الأطراف الفاعلة.	طبقا للإجراءات	تم التواصل مع الأطراف الفاعلة.



EC10.5	الاحتفاظ بقائمة مكالمات المصلحة.	حسب الكاتلوج & المخطط	سجل الاحتفاظ بقائمة مكالمات أصحاب المصلحة مستوفي.
EC10.6	احتواء الحادث الأمني في حدود صلاحياته.	حسب الكاتلوج & المخطط	تقرير احتواء الحادث الأمني - في حدود صلاحياته - مستوفي.
EC10.7	تتبع مصدر التهديد السيبراني.	طبقا للإجراءات	سجل تتبع مصدر التهديد السيبراني مستوفي.
EC10.8	حفظ دليل الحادث الأمني السيبراني.	طبقا للإجراءات	سجل حفظ دليل الحادث الأمني السيبراني مستوفي.
EC10.9	التقدير المبدئي للأضرار التي نتجت عن الحادث الأمني السيبراني.	طبقا للإجراءات	سجل التقدير المبدئي للأضرار التي نتجت عن الحادث الأمني السيبراني مستوفي.
EC10.10	تأمين نشاط الأجهزة والشبكات.	طبقا للإجراءات	النظام يعمل بكفاءة.
EC10.11	توثيق الخطوات المتخذة لتصحيح الحادث الأمني السيبراني.	طبقا للإجراءات	سجل توثيق الخطوات المتخذة لتصحيح الحادث الأمني السيبراني مستوفي.

شروط ومتطلبات الأداء

معزز المعرفة

إجراءات الاستجابة لأحداث الأمن السيبراني.
سجل تقييم الحدث الأمني تقييماً مبدئياً
منفذ بدقة.
سجل إبلاغ الرئيس المباشر بالحدث الأمني
السيبراني.
سجل التواصل مع الأطراف الفاعلة.
سجل الاحتفاظ بقائمة مكالمات أصحاب
المصلحة مستوفي.
تقرير احتواء الحادث الأمني .
سجل تتبع مصدر التهديد السيبراني.
سجل حفظ دليل الحدث الأمني السيبراني.
سجل التقدير المبدئي للأضرار التي نتجت
عن الحادث الأمني السيبراني.
سجل توثيق الخطوات المتخذة لتصحيح
الحدث الأمني السيبراني ي.
التهوية والاضاءة الجيدة في بيئة العمل
التقيد باللوائح والتعليمات المتعلقة
بالسلامة (الشركة & موقع العمل)
توفر معدات السلامة والصحة المهنية
إرشادات للتقييم

الاختبار (شفهي - تحريري) الملاحظة
والمراقبة وفق لوائح الرصد

بدأ إجراءات الاستجابة لأحداث الأمن
السيبراني.
تقييم الحدث الأمني تقييماً مبدئياً.
إبلاغ الرئيس المباشر بالحدث الأمني
السيبراني.
التواصل مع الأطراف الفاعلة.
الاحتفاظ بقائمة مكالمات أصحاب
المصلحة.
احتواء الحادث الأمني في حدود
صلاحياته.
تتبع مصدر التهديد السيبراني.
حفظ دليل الحدث الأمني السيبراني.
التقدير المبدئي للأضرار التي نتجت عن
الحادث الأمني السيبراني.
تأمين نشاط الأجهزة والشبكات.
توثيق الخطوات المتخذة لتصحيح
الحدث الأمني السيبراني.

معزز المهارات الأساسية الحياتية والعمل
الالتزام والانضباط
الاتصال والتواصل
أساسيات اللغة الانجليزية
مهارات الحاسوب واستخدام الانترنت
احترام وخصوصية مكان العمل
الالتزام بأخلاقيات العمل

محلل عمليات أمن سيبراني - المستوى المهني

قائمة الوحدات وعناصر الكفايات

رقم الوحدة	اسم وحدة الكفاية	رقم العنصر	اسم عنصر الكفاية	معيار الأداء على أساس العمليات	معيار الأداء على أساس المنتج
UC11	الوحدة الحادية عشرة: استقبال طلبات الدعم الفني الخاص بعمليات الأمن السيبراني	EC11.1	استقبال طلبات الدعم الفني.	طبقا للإجراءات	نموذج استقبال طلبات الدعم الفني مستوفي.
		EC11.2	تصنيف طلبات الدعم الفني.	طبقا للإجراءات	نموذج تصنيف طلبات الدعم الفني مستوفي.
		EC11.3	تحديد طبيعة الدعم الفني المطلوب وتوصيله إلى القسم المختص.	طبقا للإجراءات	نموذج تحديد طبيعة الدعم الفني المطلوب وتوصيله إلى القسم المختص مستوفي.

نموذج إبلاغ الجهات المعنية بالدعم الفني المطلوب كل حسب تخصصه مستوفي.	طبقا للإجراءات	إبلاغ الجهات المعنية بالدعم الفني المطلوب كل حسب تخصصه.	EC11.4
تقرير متابعة طلبات الدعم الفني المقدمة من الأقسام المعنية بالأمن السيبراني مستوفي.	حسب الكاتلوج & المخطط	متابعة طلبات الدعم الفني المقدمة من الأقسام المعنية بالأمن السيبراني.	EC11.5
تقرير تنفيذ المهام والأعمال المطلوبة والمذكورة في طلب الدعم الفني في نطاق اختصاصه مستوفي.	حسب الكاتلوج & المخطط	تنفيذ المهام والأعمال المطلوبة والمذكورة في طلب الدعم الفني في نطاق اختصاصه.	EC11.6
نموذج تقديم الدعم والمساعدة الفنية للزملاء في حدود صلاحياته بالأمن السيبراني مستوفي.	طبقا للإجراءات	تقديم الدعم والمساعدة الفنية للزملاء في حدود صلاحياته بالأمن السيبراني.	EC11.7
نموذج تقديم الدعم الفني للعملاء في حدود صلاحياته بالأمن السيبراني مستوفي.	طبقا للإجراءات	تقديم الدعم الفني للعملاء في حدود صلاحياته بالأمن السيبراني.	EC11.8
الأدوات المطلوبة للقيام بأعمال دعم الزملاء في حدود صلاحياته بالأمن السيبراني محددة بدقة.	طبقا للإجراءات	تحديد الأدوات المطلوبة للقيام بأعمال دعم الزملاء في حدود صلاحياته بالأمن السيبراني.	EC11.9
الأدوات المطلوبة للقيام بأعمال دعم العملاء في حدود صلاحياته بالأمن السيبراني محددة بدقة.	طبقا للإجراءات	تحديد الأدوات المطلوبة للقيام بأعمال دعم العملاء في حدود صلاحياته بالأمن السيبراني.	EC11.10

سجل حفظ البيانات والمعلومات المتعلقة بعمليات الدعم الفني مستوفى.	طبقا للإجراءات	حفظ البيانات والمعلومات المتعلقة بعمليات الدعم الفني.	EC11.11
--	----------------	---	---------

شروط ومتطلبات الأداء

نموذج استقبال طلبات الدعم الفني.
نموذج تصنيف طلبات الدعم الفني.
نموذج تحديد طبيعة الدعم الفني المطلوب وتوصيله إلى القسم المختص.
نموذج إبلاغ الجهات المعنية بالدعم الفني المطلوب كل حسب تخصصه.
تقرير متابعة طلبات الدعم الفني المقدمة من الأقسام المعنية بالأمن السيبراني.
تقرير تنفيذ المهام والأعمال المطلوبة والمذكورة في طلب الدعم الفني في نطاق اختصاصه.
نموذج تقديم الدعم والمساعدة الفنية للزملاء في حدود صلاحياته بالأمن السيبراني.
نموذج تقديم الدعم الفني للعملاء في حدود صلاحياته بالأمن السيبراني.
الأدوات المطلوبة للقيام بأعمال دعم الزملاء في حدود صلاحياته بالأمن السيبراني محددة بدقة.
الأدوات المطلوبة للقيام بأعمال دعم العملاء في حدود صلاحياته بالأمن السيبراني محددة بدقة.
سجل حفظ البيانات والمعلومات المتعلقة بعمليات الدعم الفني مستوفى.

معزز المعرفة

استقبال طلبات الدعم الفني.
تصنيف طلبات الدعم الفني.
تحديد طبيعة الدعم الفني المطلوب وتوصيله إلى القسم المختص.
إبلاغ الجهات المعنية بالدعم الفني المطلوب كل حسب تخصصه.
متابعة طلبات الدعم الفني المقدمة من الأقسام المعنية بالأمن السيبراني.
تنفيذ المهام والأعمال المطلوبة والمذكورة في طلب الدعم الفني في نطاق اختصاصه.
تقديم الدعم والمساعدة الفنية للزملاء في حدود صلاحياته بالأمن السيبراني.
تقديم الدعم الفني للعملاء في حدود صلاحياته بالأمن السيبراني.
تحديد الأدوات المطلوبة للقيام بأعمال دعم الزملاء في حدود صلاحياته بالأمن السيبراني.
تحديد الأدوات المطلوبة للقيام بأعمال دعم العملاء في حدود صلاحياته بالأمن السيبراني.
حفظ البيانات والمعلومات المتعلقة بعمليات الدعم الفني.

التهوية والاضاءة الجيدة في بيئة العمل
التقيد باللوائح والتعليمات المتعلقة
بالسلامة (الشركة & موقع العمل)
توفر معدات السلامة والصحة المهنية

إرشادات للتقييم

الاختبار (شفهي - تحريري) الملاحظة
والمراقبة وفق لوائح الرصد

معزز المهارات الأساسية الحياتية والعمل

الالتزام والانضباط
الاتصال والتواصل
أساسيات اللغة الانجليزية
مهارات الحاسوب واستخدام الانترنت
احترام وخصوصية مكان العمل
الالتزام بأخلاقيات العمل

9 - سلوكيات وأخلاقيات العامل (القيم الأخلاقية)

سلوكيات وأخلاقيات العامل في مهنة / وظيفة: محلل عمليات أمن سيبراني / مهني

- الالتزام بالقوانين والاحكام والسياسات الداخلية
- الأمانة والإخلاص.
- الحفاظ على سرية البيانات والمعلومات والخصوصية
- التواصل باحترام مع جميع الفئات.
- أمانة النظم (تعمل على حماية وتوافر سرية البيانات والنظم الواقعة تحت مسؤوليته)
- مشاركة المعرفة والخبرة مع الآخرين في المجال ضمن الحدود المسموحة.
- التعامل بمهنية عالية
- تحمُّل المسؤولية.
- التركيز على أدق التفاصيل التي تخص العمل
- الحرص على تقديم أفضل جودة ممكنة للعمل.
- مساعدة الآخرين ضمن حدود القدرة واحترامهم.
- التحلي بالأخلاق الحسنة كالصدق واللطف والوفاء بالوعود والإيجابية والتسامح.
- كسب ثقة صاحب العمل والعملاء.
- الالتزام بالمواعيد وحضور الاجتماعات.
- مساعدة الآخرين ضمن حدود القدرة واحترامهم.
- احترام سياسة وقواعد مؤسسة العمل.
- الاحتفاظ بأسرار العمل وعدم إفشاءها لأي شخص أو أية جهة.
- الالتزام بساعات العمل حسب المتفق عليها في عقد العمل.
- الاهتمام بالنظافة الشخصية والمظهر الخارجي.
- العمل بروح الفريق.
- عدم الخوض في المواضيع الحساسة مثل: الدين والسياسة والألعاب / الفرق الرياضية، النوع الاجتماعي (الجندر) ... الخ.
- تبادل المعلومات ومشاركتها مع الآخرين حسب نظام العمل.
- التحلي بالصبر وضبط الأعصاب والكياسة في التعاملات مع العملاء والزملاء.
- حسن الاستماع للمسؤول المباشر والعاملين والعملاء.

10- قواعد السلامة والصحة المهنية

1-10 بروتوكول موقع العمل والإجراءات الوقائية

- القاعة /المكان مهيبئ لإجراءات السلامة العامة.
- وجود نقاط تحكم بالدخول والخروج للمبنى.
- وجود تعليمات وإرشادات سلامة وصحة مهنية تحتوي على مجموعة من الإرشادات تضمن تطبيق ممارسات آمنة في العمل والحد من المخاطر المحتمل حدوثها في مواقع العمل الخاصة بالأمن السيبراني.

10-2 آليات تقليل حدوث المخاطر

- عن طريق لوحات استرشادية وانظمة انذار للحريق والكشف عنه وانظمة مراقبة كاميرات أمنية.
- تزويد العاملين بالتعليمات اللازمة لتنفيذ العمل بطرق صحيحة وآمنة.
- فرض تدابير رقابية شديدة على العاملين أثناء تنفيذ العمل.
- توفير جميع المعدات اللازمة ووسائل السلامة والحماية لكافة العاملين.
- التأكد من إصلاح أي خلل أو عطل فور حصوله في مواقع العمل الخاصة بالأمن السيبراني.

10-3 تنظيم مواقع العمل

- أن تكون معزولة عن باقي أقسام الشركة.
- أن تكون مؤمنة بوجود أفراد أمن المبنى.
- الحرص على وجود خطط منظمة لإخلاء الموقع في حالات الطوارئ.
- التأكد من وجود إنارة جيدة ومناسبة في الموقع لتعزيز الرؤية ليلا في مواقع العمل الخاصة بالأمن السيبراني.
- التأكد من أن كافة الأجهزة تعمل بكفاءة والعمل على تفقدها بشكل منتظم.
- تزويد العاملين الجدد بإرشادات السلامة العامة ومعدات الوقاية الشخصية منذ يومهم الأول.

10-4 معدات الوقاية الشخصية

- مواد اسعافات أولية
- نظام إطفاء الحريق.
- استخدام كافة الأفراد المعدات الواقية في جميع الأوقات في مواقع العمل الخاصة بالأمن السيبراني.
- تزويد كافة العاملين المتواجدين في الموقع بمعدات وقاية شخصية سليمة مثل الملابس العاكسة للضوء، ونظارات السلامة وواقيات الأذن.
- تدريب العاملين على استخدام معدات الوقاية الشخصية بشكل صحيح وفعال والتأكد من استخدامهم لها طيلة الوقت.

5-10 الأجهزة والآلات والأدوات والمعدات والمواد

المواد	الأدوات والمعدات	الأجهزة والآلات
أوراق	SIEM	خادم
أقلام	EDR	جهاز كمبيوتر
	برامج إدارة الثغرات	شاشات مراقبة
	Operation System	أدوات أمن وسلامة
		أجهزة اتصال
		كاميرات

11- شروط الالتحاق بالبرنامج

- المؤهل العلمي الأدنى: الثانوية العامة، توجيهي (ناجح)
- طبيعة مهام البرنامج تقبل ذوي الاحتياجات الخاصة
- طبيعة مهام البرنامج لا تقبل ذوي الإعاقة البصرية والعقلية والحركية في الأطراف العليا.

12- وصف بيئة العمل في ظل قانون العمل الأردني

1-12 ساعات العمل

- 24 ساعة / 7 أيام (مقسمة إلى 3 فترات)
- 8 ساعات يومياً (بدون حساب فترات الراحة والطعام).
- يمكن إعادة توزيع ساعات العمل بحد أقصى 11 ساعة يومياً (بما في ذلك فترات الراحة)
- بكل الأحوال حد أقصى 48 ساعة في الأسبوع (بدون احتساب الوقت المخصص للطعام والراحة).
- العمل الإضافي في الظروف الطارئة:
- ✓ يجوز تشغيل العامل أكثر من ساعات العمل اليومية أو الأسبوعية في حالات الطوارئ ولا يشترط موافقة العامل على العمل الإضافي في أية حالات طوارئ تحدد بمعرفة جهة الاختصاص.
- ✓ ساعات العمل بحد أقصى 11 ساعة يومياً (بما في ذلك فترات الراحة)
- ✓ يستحق أجر عمل إضافي.

2-12 الظروف البيئية

- ساعات عمل مرنة.
- أماكن العمل جيدة الإنارة والتهوية.
- الخصوصية في اللقاءات مع العملاء.
- اتصال بالإنترنت فائق السرعة.
- الاستقلالية في العمل.

3-12 متطلبات بيئة العمل

هذه المهنة تتطلب ما يلي:

- توفر الأدوات والمعدات اللازمة لممارسة المهنة.
- توفر الظروف البيئية المناسبة.
- توفير البرمجيات والأنظمة اللازمة لإتمام مراقبة أمن الشبكات.
- الاستجابة السريعة للمهام المطلوبة المحددة من قبل الرئيس المباشر.
- التواصل والتنسيق مع المسؤولين أو أشخاص لهم صلة بالعمل أو من الأقسام الأخرى.
- القيام بعمليات متكررة وإعادة الأنشطة العقلية ذاتها مراراً وتكراراً.
- الالتزام بجميع إجراءات وتعليمات ومعايير الصحة والسلامة المهنية.
- الالتزام بارتداء معدات الحماية والسلامة الشخصية مثل: النظارات ومعدات حماية السمع.....إلخ.
- استخدام الهاتف الخاص أثناء العمل في حالات محددة حسب النظم المتبعة داخل المؤسسة.
- اتخاذ القرارات اللازمة المتعلقة بالآخرين في ضوء النظم المعمول بها داخل المؤسسة.
- الحرص على السمعة الشخصية وسمعة المؤسسة التي يعمل بها قبل وأثناء وبعد الأعمال المكلف بها.
- الدقة في تنفيذ هذا العمل متطلباً مهماً بدرجة عالية.
- استخدام البريد الإلكتروني ووسائل التواصل المعتمدة داخل المؤسسة حسب طبيعة العمل.
- كتابة التقارير والملاحظات الإلكترونية والورقية.

13- معيار مدة التنفيذ ونقل المهارة

المدة التقديرية للتدريب بالساعة (المستوى المهني)	الكفايات
520 ساعة تدريبية	المعارف ومهارات الاستخدام والمهارات الفنية المهنية
280 ساعة تدريبية (أو حسب ما تحدده هيئة تنمية وتطوير المهارات المهنية والتقنية)	التدريب في مواقع العمل ojt
800 ساعة تدريبية	إجمالي الساعات التدريبية

14- قائمة المراجع

1-14 المراجع العربية

- التصنيف الأردني المعياري للمهن (2021)، الأردن.
- الإطار العام للمناهج الأردنية (2022)، المركز الوطني لتطوير المناهج، الأردن.
- الإطار الوطني للمؤهلات في المملكة الأردنية الهاشمية (2020).
- تقرير حالة البلاد (2021) - مجال الموارد البشرية، سوق العمل والتشغيل وقطاع التعليم والتدريب المهني والتقني، المجلس الاقتصادي والاجتماعي الأردني، الأردن.
- الأردن 2025 – رؤية واستراتيجية وطنية، الأردن.

2-14 المراجع الأجنبية

Almaz, F. (2022). A new way of doing business during the COVID-19 pandemic: An example of the DACUM analysis. *Management: Journal of Contemporary Management Issues*, 27(1), 337-359.

Borden, T., & Cox, R. A. (2022). *Technician's guide to programmable controllers*. Cengage Learning.

DACUM International Training Center, Ohio University, USA

<https://cete.osu.edu/programs/dacum-international-training-center/>

International Organization for Scientific Research (IOSR).

<https://www.iosrjournals.org/>

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2022). Cyber security in iot-based cloud computing: A comprehensive survey. *Electronics*, 11(1), 16.

Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. *Authorea Preprints*.

Zhang, Z., Ning, H., Shi, F., Farha, F., Xu, Y., Xu, J., ... & Choo, K. K. R. (2022). Artificial intelligence in cyber security: research advances, challenges, and opportunities. *Artificial Intelligence Review*, 55(2), 1029-1053.

15- قائمة الملاحق

1-15 قائمة الواجبات والمهام طبقا لمخطط DACUM

2-15 خطة التدريب

3-15 الوصف التدريبي

4-15 ملاحظات إرشادية للمدرسين

5-15 مواد تدريب المعلم / المدرب

6-15 مواد تدريب المتعلم / المتدرب

7-15 أنشطة البرنامج التدريبي

8-15 نموذج الامتحان النهائي (نظري)

9-15 نموذج الامتحان النهائي (عملي)

10-15 نموذج بطاقة التمرين

11-15 نموذج امتحان نهائي (اختيار من متعدد)

12-15 موجّهات كتابة محتوى الكتاب

13-15 دليل العروض التقديمية

14-15 مواصفات وشروط المدرسين (معايير اختيار المدرسين)