النشرة الفنية للبرنامج التحضيري

شهادة فني أمن سيبر اني معتمد CCT

Certified Cybersecurity Technician

(10) أيام، (40) ساعة

يبدأ بتاريخ 2024/06/30م

تدريب صفي(F2F) – ليبيا

06 - 5522807
info@aljhood.com
www.aljhood.com
jordan amman queen rania st building.155

بطاقة معلومات البرنامج التحضيري:

مدة التدريب	:	(10) أيام، (40) ساعة
مكان التدريب	:	طرابلس، ليبيا
تاريخ الانعقاد	:	30 /06 -2024/07/11م
توقيت التدريب	:	الساعة 09:00 صباحا – 01:00 ظهرا
شهادة التدريب	:	شهادة صادرة من مجموعة الجهود المشتركة (الجهود) "نسبة الحضور لاتقل عن 90%"
شهادة الاعتماد	:	شهادة حضور صادرة من EC- Council وشهادة CCT في حال حقق المشارك متطلبات الحصول على الشهادة المعتمدة دوليا.
لغة التدريب	:	اللغة العربية مع بعض المصطلحات الفنية باللغة الإنجليزية
أساليب التدريب	:	– إسلوب العصف الذهني. – حالات وسيناريوهات عملية. – مجموعات العمل وتطبيقات جماعية. – حالات وتطبيقات عملية من واقع العمل.
الفئة المستهدفة	:	– محلل أمن النظم – محلل أمن المعلومات – مسؤول الأمن الرقمي – مطور برمجيات الأمن الرقمي – العاملين في مجال تشفير البيانات
EC -Council	:	مجلس EC-Council (المجلس الدولي لمستشاري التجارة الإلكترونية) هو أكبر هيئة توثيق في العالم لمحترفي أمن المعلومات. يعتبر مجلس EC-Council منظمة تعتمد على الأعضاء توثق الأفراد في مجالات مختلفة من أمن المعلومات والأعمال الإلكترونية. لقد قدم مجلس EC-Council خلال أكثر من 15 عامًا برامج تدريب وتوثيق عالية الجودة من خلال شبكة كبيرة من الشركاء الرسميين، مما خدم أكثر من 500,000 محترف في مجال أمن المعلومات في أكثر من 140 دولة، من خلال عدد متزايد من الشركات الرائدة والشركاء والمنظمات الحكومية. نمت شبكة الشركاء لديهم لتشمل أكثر من 2,000 شريك رسمي في كل من التدريب التجاري والأكاديمي، وتعد الجهود الآن مركزًا معتمدًا لمجلس EC-Councilللتدريب المعتمد، ويمكننا الترويج وتقديم جميع خدماتهم في المنطقة وتدريب شهادتهم المهنية والمعتمدة دوليا.

الأردن / عمان – شارع الملكة رانيا العبدالله – بناية رقم 155 – الموقع الالكتروني : www.aljhood.com

تفاصيل إختبار CCT	: – الاختبار اونلاين. – نسبة النجاح 70% . – مدة الإختبار 3 ساعات. – 60 سؤالاً (نمط الاختيار المتعدد). – الإختبار متوفر باللغة الإنجليزية.

ملخص البرنامج التدريبي CCT:

تم تصميم هذا البرنامج في الأمن السيبراني بما يتوافق مع إحتياجات سوق العمل المحلية لهذا التخصص، ويتم التدريب في هذا البرنامج على المهارات التخصصية في: مجال الأمن السيبراني: " الخوارزميات والمنطق " و"تكنولوجيا المعلومات والإتصالات " و" أساسيات التشفير" و"نظم التشغيل" و"أمن إنترنت الأشياء و الحوسبة السحابية" و"نظم التشغيل" و" أساسيات الأمن السيبراني" و" الإنترنت و شبكات الحاسب " و"أساسيات البرمجة بلغة البايثون" و" مبادئ برمجة صفحات الإنترنت " ومقدمة في أمن الشبكات "و " الجريمة الإلكترونية و مخاطرها" و" أمن شبكات الحاسب ".

اضافة الى " تكنولوجيا الذكاء الاصطناعي " و "أمن الحكومة الإلكترونية " و " الإختراق الأخلاقي وأساليب الحماية "و " مقدمة في الأدلة الجنائية الرقمية " و " موضوعات مختارة في الأمن السيبراني" ويتم التركيز أثناء التدريب علي الجانب العملي التطبيقي وربطه بالجانب النظري في معظم المقررات التخصصية وذلك عن طريق تكثيف التدريبات العملية الأساسية وتطبيق برنامج التدريب التعاوني مع القطاعات ذات العلاقة بتخصص المتدرب إضافة إلى مهارات عامة في "اللغة الإنجليزية"،و"تطبيقات الحاسب الآلي"، و"التعرف على عالم الأعمال" و"مهارات التعلم."

تم إعتماد المحاور الرئيسية للتدريب في هذا البرنامج بالتوائم مع متطلبات المعهد الدولي EC-counsel للحصول على شهادة فني أمن سيبراني معتمد CCT ويمكن أن يتم التدريب باستخدام منهج تدريبي يقوم على لغتين العربية والإنجليزية ويتم عقد الإختبار النهائي باللغة الإنجليزية وسيتولى المدرب مساعدة المتدربين بتقديم الدعم اللغوي والفني وتدريبهم على كيفية التعامل مع الإختبار وفي يجتاز المتدرب الإختبار بنجاح يتحصل على شهادة من EC-counsel حيث انها المعهد الاول في العالم في الأمن السيبراني وتعتبر شهاداته من أفضل الشهادات العالمية، سيشرف على التدريب فريق خبراء ومدربين من الجهود من حملة الشهادات المهنية الدولية ومن أصحاب الخبرات العملية.

الأهداف التدريبية:

يهدف البرنامج إلى تزويد المتدربين بالمعرفة والمهارات اللازمة لحماية المعلومات والأنظمة السيبرانية من التهديدات والهجمات الإلكترونية، وتتضمن أهداف هذا البرنامج ما يلي:

- إدارة الأمن السيبراني: يتعلم المتدربين كيفية تنفيذ وإدارة برامج الأمن السيبراني في المؤسسات. يتناول المناهج المعترف بها في مجال إدارة الأمن السيبراني وكيفية تطبيقها بفاعلية، بما في ذلك تقييم المخاطر وإعداد سياسات الأمن والتدريب والتوعية.
- فهم التهديدات السيبرانية: يهدف البرنامج إلى تعريف المتدرب بمختلف أنواع التهديدات السيبرانية التي تواجه المؤسسات والأفراد، يتم تحليل ودراسة أمثلة عملية للهجمات السيبرانية المشهورة وتقنيات الإختراق المستخدمة.

الأردن / عمان – شارع الملكة رانيا العبدالله – بناية رقم 155 – الموقع الالكتروني : www.aljhood.com

- حماية البيانات والأنظمة: يتعلم المتدربين كيفية تطبيق الإجراءات الأمنية اللازمة لحماية البيانات والأنظمة السيبرانية. يتعلمون تقنيات التشفير والتوقيع الرقمي والمصادقة والتحكم في الوصول وغيرها من الأدوات والتقنيات المستخدمة في الحماية.
- اكتشاف الإختراق والاستجابة للحوادث: يتعلم المتدربين كيفية اكتشاف الإختراقات المحتملة وتحليلها والاستجابة لها بطريقة فعالة وسريعة. يشمل ذلك تقنيات التحليل الرقمي والتحقق من الحوادث واستعادة الأنظمة وتقييم الأضرار.
- القوانين والتشريعات السيبرانية: يتعلم المتدربين عن التشريعات واللوائح المتعلقة بالأمن السيبراني والخصوصية. يتناول المواضيع المتعلقة بالتشريعات الدولية والمحلية وأخلاقيات القرصنة الإلكترونية والاحتيال الإلكتروني.
- التعامل مع الهجمات السيبرانية: يتدرب الدارسين على التعامل مع هجمات القرصنة الإلكترونية والتحقق منها والتحليل الرقمي واستعادة الأنظمة وتطبيق إجراءات الطوارئ اللازمة للتعامل مع الهجمات السيبرانية.

المحاور الرئيسية:

المحور الأول: تهديدات وضعف أمن المعلومات

المحور الثاني: هجمات أمن المعلومات

المحور الثالث: أساسيات أمن الشبكات

المحور الرابع: التحقق من الهوية والمصادقة والتفويض

المحور الخامس: ضوابط أمن الشبكات - الضوابط الإدارية

المحور السادس: ضوابط أمن الشبكات - الضوابط الفيزيائية

المحور السابع: ضوابط أمن الشبكات - الضوابط التقنية

المحور الثامن: تقنيات وأدوات تقييم أمن الشبكات

المحور التاسع: استمرارية الأعمال واستعادة الكوارث

المحور العاشر: أمان التطبيقات الافتراضي والحوسبة السحابية

المحور الحادي عشر: أمان الشبكات اللاسلكية

المحور الثاني عشر: أمان الأجهزة المحمولة

المحور الثالث عشر: أمان الأشياء المتصلة بالإنترنت والتكنولوجيا الصناعية

المحور الرابع عشر: التشفير

المحور الخامس عشر: أمان البيانات

المحور السادس عشر: حل مشاكل الشبكات

المحور السابع عشر: مراقبة حركة المرور على الشبكة

المحور الثامن عشر: مراقبة وتحليل سجلات الشبكة

المحور التاسع عشر: الاستجابة للحوادث

المحور العشرون: التحقيق الجنائي الحاسوبي

المحور الحادي والعشرون: إدارة المخاطر

الأردن / عمان – شارع الملكة رانيا العبدالله – بناية رقم 155 – الموقع الالكتروني : www.aljhood.com