ALJHOOD®

من أكثر التخصصات طلباً .. في ظل التحول الرقمي

الدبلوم المهني الدولي في الأمن السيبراني

التدريب الهجين الحضوري والكتروني

يُساعدك على الحصول على شهادة فني أمن سيبراني معتمد CCT

EC-Council

مع تزايد هجمات برامج الفدية، وتسريبات البيانات، وفشل الأنظمة، أصبح من الضروري حماية عملك من المخاطر السيبرانية لضمان استمراره

بطاقة معلومات البرنامج:

مدة التدريب	:	(6) أسابيع، (115) ساعة 3 أسابيع تدريب صفي : 75 ساعة تدريبية 3 أسابيع تدريب عن بُعد(زووم) : 40 ساعة تدريبية
مكان التدريب	:	قاعات الجهود – حي الأندلس - طرابلس
تاريخ الانعقاد	:	2024/12/08م لغاية 2025/01/16م
توقيت التدريب	:	09:00 صباحاً – 02:00 مساءاً
لغة التدريب	:	اللغة العربية مع بعض المصطلحات الفنية باللغة الإنجليزية
الشهادة	:	شهادة دبلوم معتمدة من مجموعة الجهود المشتركة بشرط الا يقل الحضور عن 85%.
شهادة الاعتماد	:	شهادة فني أمن سيبراني CCT معتمد من EC –Council عند استيفاء كافة متطلبات الدبلوم والنجاح في الاختبار المعتمد.
EC -Council	:	مجلسEC –Council (المجلس الدولي لمستشاري التجارة الإلكترونية) هو أكبر هيئة توثيق في العالم لمحترفي أمن المعلومات. يعتبر مجلسEC –Council منظمة تعتمد على الأعضاء توثق الأفراد في مجالات مختلفة من أمن المعلومات والأعمال الإلكترونية. لقد قدم مجلسEC –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 لمجلسEC –Council للتدريب المعتمد، ويمكننا الترويج وتقديم جميع خدماتهم في المنطقة وتدريب شهادتهم المهنية والمعتمدة دوليا.
أساليب التدريب	:	– إسلوب العصف الذهني. – إسلوب الحالات العملية. – إسلوب مجموعات العمل. – المختبرات الافتراضية الخاصة. – الرخص الدولية الداعمة للتطبيق. – إسلوب سيناريوهات من واقع عمل المتدربين.
القيمة المضافة	:	– عقد تقييم قبلي Pre: لقياس مستوى المشاركين قبل التدريب. – عقد تقييم بعدي Post: لقياس مستوى المشاركين قبل التدريب. **قياس القيمة المعرفية المضافة (KVA) = التقييم البعدي – التقييم القبلي**

الفئة المستهدفة:

- العاملين في إدارة تكنولوجيا المعلومات .
- مدراء ومشرفين ادارة أمن المعلومات.
- العاملين في إدارة مراقبة أمن المعلومات.
- العاملين في إدارات تدقيق الأمن السيبراني.
- الخريجين الجدد المؤهلين لسوق العمل.

جميع العاملين في المؤسسات الذين يستخدمون التكنولوجيا.

ملخص الدبلوم التدريبي:

تم تصميم هذا الدبلوم في الأمن السيبراني بما يتوافق مع إحتياجات سوق العمل المحلية لهذا التخصص، ويتم التدريب في هذا الدبلوم 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" مبادئ برمجة صفحات الإنترنت " ومقدمة في أمن الشبكات "و " الجريمة الإلكترونية و مخاطرها" و" أمن شبكات الحاسب ".

اضافة الى "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." ، سيشرف على التدريب من خبراء ومدربين من الجهود من حملة الشهادات المهنية الدولية ومن أصحاب الخبرات العملية.

التطبيقات العملية:

يعد التدريب العملي جزءاً أساسياً من دبلوم الأمن السيبراني، حيث يهدف إلى تزويد المشاركين بالمهارات التطبيقية والمعرفة العملية التي يحتاجونها لحماية الأنظمة والشبكات من التهديدات الإلكترونية المتزايدة، يتميز هذا التدريب بتركيزه على التطبيقات العملية الحقيقية، حيث يتاح للمتدربين فرصة العمل على حالات واقعية ومحاكاة هجمات إلكترونية، حيث يتضمن التدريب العملي مجموعة متنوعة من الأنشطة مثل تحليل البرمجيات الخبيثة، وإكتشاف الثغرات الأمنية، وتطبيق إجراءات الحماية المتقدمة.

كما يشمل التدريب إستخدام أدوات وتقنيات حديثة في مجال الأمن السيبراني، مما يضمن حصول المشاركين على تجربة تعليمية شاملة تتماشى مع أحدث التطورات في هذا المجال، ومن خلال هذا التدريب، يتعلم المشاركون كيفية بناء أنظمة آمنة، وتطوير سياسات وإجراءات أمان فعالة، والاستجابة بسرعة وفعالية للحوادث الأمنية. بالإضافة إلى ذلك، يعزز التدريب العملي قدرات المشاركين في التفكير النقدي وحل المشكلات، مما يؤهلهم لمواجهة التحديات المعقدة في بيئة العمل الحقيقية.

أهداف الدبلوم التدريبي:

يهدف الدبلوم إلى تزويد المتدربين بالمعرفة والمهارات اللازمة لحماية المعلومات والأنظمة السيبرانية من التهديدات والهجمات السيبرانية، وتتضمن أهداف هذا الدبلوم 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 الدبلوم إلى تعريف المتدرب بمختلف أنواع التهديدات السيبرانية التي تواجه المؤسسات والأفراد، يتم تحليل ودراسة أمثلة عملية للهجمات السيبرانية المشهورة وتقنيات الإختراق المستخدمة.
- 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 والإحتيال الإلكتروني.
- التعامل مع الهجمات السيبرانية: يتدرب الدارسين على التعامل مع هجمات القرصنة الإلكترونية والتحقق منها والتحليل الرقمي وإستعادة الأنظمة وتطبيق إجراءات الطوارئ اللازمة للتعامل مع الهجمات السيبرانية.

المحاور الرئيسية للتدريب:

المحور الأول : الأمن السيبراني وأمن المعلومات

- **الأمن السيببراني:**
  - مفهوم الأمن السيبراني.
  - أنواع الأمن السيبراني.
  - أهمية الأمن السيبراني.
  - دراسة حالات عملية واقعية وتحليلها.
- **فهم الهجمات والتهديدات السيبرانية:**
  - تحليل الهجمات الشائعة (البرمجيات الخبيثة، الهجمات الموجهة، هجمات DOS).
  - مفهوم أمن المعلومات وأهدافه (السرية، النزاهة، التوفر).
  - مقدمة إلى CIA Triad.
  - كيفية تحقيق السرية والنزاهة والتوافر في الأنظمة.
  - دراسة حالات عملية واقعية وتحليلها.

المحور الثاني: السياسات والإجراءات الأمنية

- **سياسة الأمن والتنظيم:**
  - كتابة وتطبيق سياسات الأمان.

- دراسة حالات عملية واقعية وتحليلها.

- **إدارة المخاطر:**
  - تحليل المخاطر.
  - تقييم المخاطر.
  - استراتيجيات إدارة المخاطر.
- **إستمرارية الأعمال وخطط التعافي من الكوارث:**
  - تخطيط الإستمرارية وخطط التعافي.
  - تنفيذ محاكاة لكوارث افتراضية وتقييم الاستجابة.

المحور الثالث : الشبكات وأساسيات الشبكات الأمنية

- **أساسيات الشبكات (OSI Model, TCP/IP):**
  - شرح تفصيلي لنموذج OSI وTCP/IP.
  - أدوات تحليل الشبكة مثل Wireshark.
- **تقنيات التشفير الأساسية:**
  - مقدمة إلى التشفير.
  - تطبيقات عملية لتقنيات التشفير.
- **الجدران النارية وأنظمة كشف التسلل:**
  - إعداد وإستخدام الجدران النارية.
  - إستخدام أنظمة كشف التسلل (IDS/IPS).

المحور الرابع : الأمن المادي وإدارة الهوية والوصول

- **الأمن المادي:**
  - تقنيات الأمن المادي وأهميتها.
  - أمثلة على تطبيقات الأمن المادي.
- **إدارة الهوية والوصول (IAM):**
  - أساسيات IAM.
  - أمثلة على تطبيقات IAM.
- **تقنيات المصادقة والتفويض:**
  - طرق المصادقة المختلفة.
  - تطبيق عملي لتقنيات المصادقة والتفويض.

المحور الخامس : المهارات العملية والتطبيقية

- **أنظمة التشغيل والأمن:**
  - أمان نظام التشغيل Windows.
  - إعدادات الأمان في Windows.
  - أدوات الأمان في Windows.
- **أمان نظام التشغيل Linux:**

- إعدادات الأمان في Linux.
- أدوات الأمان في Linux.

- **أدوات وتكتيكات مراقبة النظام:**
  - مراقبة النظام واكتشاف التهديدات.
  - أدوات مراقبة النظام مثل Nagios وSplunk.

المحور السادس : الشبكات والأمن المتقدم

- **أمان الشبكات اللاسلكية:**
  - تقنيات تأمين الشبكات اللاسلكية.
  - إعداد وإختبار الشبكات اللاسلكية.
- **إعداد وتحليل السجلات (Logging):**
  - إعداد أنظمة السجلات.
  - تحليل السجلات لاكتشاف التهديدات.
- **استراتيجيات الدفاع المتقدم (Defence in Depth):**
  - مفهوم الدفاع المتعمق.
  - تطبيق استراتيجيات الدفاع المتقدم.

المحور السابع : أمن التطبيقات والبرمجيات:

- **أمان تطوير البرمجيات (Secure SDLC)**
  - مقدمة إلى دورة حياة تطوير البرمجيات الآمنة.
  - أمثلة على أفضل الممارسات.
- **حماية تطبيقات الويب (10 OWASP Top):**
  - دراسة 10 OWASP Top.
  - تطبيق عملي لحماية تطبيقات الويب.
- **إختبار الاختراق للتطبيقات**
  - مقدمة إلى إختبار الاختراق.
  - إستخدام أدوات مثل Burp Suite لإختبار التطبيقات.

المحور الثامن : إختبار الاختراق والتحقيق الجنائي الرقمي

- **أساسيات إختبار الاختراق:**
  - أنواع إختبار الاختراق.
  - إعداد وإستخدام أدوات إختبار الاختراق.
- **أدوات إختبار الاختراق (Suite Metasploit, Nmap, Burp):**
  - مقدمة إلى الأدوات المختلفة.
  - تطبيق عملي لإختبار الاختراق بإستخدام الأدوات.
- **التحقيق الجنائي الرقمي (Digital Forensics):**
  - أساسيات التحقيق الجنائي الرقمي.

- أدوات التحقيق الجنائي الرقمي.

المحور التاسع : التهديدات المتقدمة وحلولها

- **التهديدات المتقدمة (APT):**
  - مقدمة إلى التهديدات المتقدمة.
  - تحليل أمثلة على التهديدات المتقدمة.
- **تكتيكات وأساليب المهاجمين:**
  - دراسة تكتيكات المهاجمين.
  - دراسة حالات عملية واقعية وتحليلها.
- **تحليل البرمجيات الخبيثة:**
  - مقدمة إلى تحليل البرمجيات الخبيثة.
  - أدوات تحليل البرمجيات الخبيثة.

المحور العاشر: الحوسبة السحابية والأمان

- **مبادئ الأمان في الحوسبة السحابية:**
  - أساسيات الحوسبة السحابية.
  - تحديات الأمان في السحابة.
- **أمان خدمات AWS, Azure, Google Cloud:**
  - إعداد وتأمين الخدمات السحابية.
  - دراسة حالات عملية واقعية وتحليلها.
- **إدارة الهوية والوصول السحابية (Cloud IAM):**
  - أساسيات IAM في السحابة.
  - دراسة حالات عملية واقعية وتحليلها.

المحور الحادي عشر: أمان الأجهزة المحمولة وإنترنت الأشياء

- **أمان الأجهزة المحمولة:**
  - تحديات الأمان في الأجهزة المحمولة.
  - أمان إنترنت الأشياء (IoT).
  - تحديات الأمان في إنترنت الأشياء.
  - دراسة حالات عملية واقعية وتحليلها.
- **الحماية من التهديدات الخاصة بهذه التقنيات:**
  - استراتيجيات الحماية
  - دراسة حالات عملية واقعية وتحليلها.

المحور الثاني عشر: أتمتة الأمان وأدوات السيكوبس

- **أتمتة الأمان (Security Automation):**
  - مقدمة إلى أتمتة الأمان.
  - أدوات الأتمتة.

- دراسة حالات عملية واقعية وتحليلها.

- **أدوات السيكوبس (Security Operations):**
  - مقدمة إلى سيكوبس.
  - أدوات السيكوبس.
- **مقدمة إلى DevSecOps:**
  - مبادئ DevSecOps.
  - دراسة حالات عملية واقعية وتحليلها.

الحصول على شهادة فني أمن سيبراني معتمد CCT:

تم إعتماد المحاور الرئيسية للتدريب في هذا الدبلوم لتتوائم ومتطلبات المعهد الدولي EC –Council وللحصول 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 –Council 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.

تفاصيل إختبار CCT:

- الاختبار اونلاين.
- نسبة النجاح 70% .
- مدة الإختبار 3 ساعات.
- الإختبار متوفر باللغة الإنجليزية.
- 60 سؤالاً (نمط الاختيار المتعدد).

إنتهت العرض الفني ،