ملف البرنامج التدريبي: الأمن السيبراني (Cybersecurity)

نسخة غير قابلة للتداول إلا بإذن من شركة أوميديك للتدريب والاستشارات.

أهداف كورس الأمن السيبراني

- تمكين المشاركين من فهم أساسيات ومفاهيم الأمن السيبراني.
- إكساب مهارات اكتشاف الثغرات وتقييم المخاطر الرقمية.
- معرفة طرق تأمين الشبكات والأنظمة والتطبيقات.
- استراتيجيات الاستجابة للحوادث السيبرانية وتقليل تأثيرها.
- استخدام الأنظمة الحديثة والذكاء الاصطناعي في الدفاع السيبراني.
- تحسين المهارات الحالية للمتدربين في مجال الأمن السيبراني وتمكينهم من تطبيقها بفعالية.
- التحكم في المخاطر الرقمية مع تعظيم حماية الأصول المعلوماتية.
- زيادة الكفاءة في حماية البنية التحتية الرقمية للمؤسسات.

محاور كورس الأمن السيبراني

- المحور الأول: المفاهيم الأساسية للأمن السيبراني
  - تعريف الأمن السيبراني وأهميته.
  - الفرق بين أمن المعلومات والأمن السيبراني.
- المحور الثاني: تقييم المخاطر وإدارة الثغرات
  - أساليب تقييم المخاطر السيبرانية.
  - دراسة وتحليل الهجمات السيبرانية الشائعة.
- المحور الثالث: إدارة عمليات التأمين اليومية
  - تأمين الشبكات وأنظمة التشغيل.
  - متابعة التحديثات الأمنية وإدارة الوصول.
  - التعامل مع تهديدات الهندسة الاجتماعية.
- المحور الرابع: الاستجابة للحوادث والتحقيق الجنائي الرقمي
  - حساب تأثير الحوادث والخسائر.
  - إدارة خطط الاستجابة للحوادث.
- المحور الخامس: استراتيجيات الدفاع المتقدم
  - إدارة المخاطر السيبرانية المتقدمة.
  - تطوير استراتيجيات الدفاع السيبراني للمؤسسة.
  - دراسات حالة لهجمات سيبرانية عالمية.
- المحور السادس: الاتجاهات الحديثة في الأمن السيبراني
  - التحول الرقمي وتحديات الأمن السيبراني.
  - الأمن السيبراني في الحوسبة السحابية وإنترنت الأشياء (IoT).

الفئة المستهدفة

- مديرو تقنية المعلومات.
- المتخصصون في أمن المعلومات.
- مهندسو الشبكات والنظم.
- المطورون ومسؤولو المواقع الإلكترونية.
- الخريجون الجدد والمهتمون بدخول مجال الأمن السيبراني.

المخرجات المتوقعة

- شهادة معتمدة.
- مادة تدريبية + أدوات وبرامج جاهزة.
- مهارات عملية قابلة للتطبيق فوراً في سوق العمل.

معلومات التسجيل والتواصل

- **رسوم الاشتراك:** (تُحدد لاحقاً).
- **طرق الدفع:** جميع طرق الدفع متاحة.
- **بيانات التواصل:** يمكن التواصل لهذا الكورس على رقم 01000093444.

المواد الدراسية في كورس الأمن السيبراني

- المادة الأولى: أساسيات الأمن السيبراني
  - تعريف الأمن السيبراني وأهدافه (السرية، التكامل، التوافر).
  - الفرق بين أمن المعلومات والأمن السيبراني وأمن الشبكات.
  - دورة حياة الهجوم السيبراني (Cyber Kill Chain).
- المادة الثانية: تقييم المخاطر والثغرات
  - أساليب تقييم المخاطر وتصنيفها.
  - العوامل المؤثرة في زيادة الهجمات السيبرانية.
  - دراسة التهديدات السيبرانية على المستوى المحلي والدولي.
  - ورشة عمل تطبيقية على استخدام أدوات فحص الثغرات.
- المادة الثالثة: إدارة عمليات التأمين اليومية
  - صياغة سياسات أمن المعلومات وتطبيقها.
  - التعامل مع الموظفين وتوعيتهم (مخاطر الهندسة الاجتماعية).
  - متابعة سجلات النظام (Logs) واكتشاف الأنشطة المشبوهة.
  - حل المشكلات الأمنية الشائعة.
- المادة الرابعة: الاستجابة للحوادث والتحقيق الرقمي

- حساب تكلفة الاختراق وتأثيره على الأعمال.
- إدارة خطط الاستجابة والتعافي من الكوارث.
- إعداد التقارير الفنية للحوادث السيبرانية.
- مؤشرات الأداء الرئيسية (KPIs) لفرق الأمن السيبراني.
- المادة الخامسة: استراتيجيات الدفاع المتقدم
- إدارة المخاطر المتعلقة بالجهات الخارجية (Third-Party Risk).
- استراتيجيات تعظيم العائد على الاستثمار في الأمن السيبراني (ROI).
- دراسات حالة (Case Studies) من هجمات سيبرانية معروفة.

إمكانيات وخبرة المحاضر

- **الخبرة العملية:** أكثر من 10 سنوات في مجال الأمن السيبراني والاستجابة للحوادث، عمل مع كبرى الشركات في قطاعات البنوك والاتصالات.
- **المجالات التي عمل بها:**
- تقييم أمني للبنى التحتية الرقمية.
- إدارة فرق الاستجابة للحوادث السيبرانية.
- تطوير استراتيجيات الأمن السيبراني للمؤسسات.
- استشارات أمنية للشركات الناشئة والكبرى.
- **القدرات التدريبية:**
- أسلوب تدريبي تفاعلي قائم على محاكاة الهجمات الحقيقية ودراسات الحالة.
- تبسيط المفاهيم التقنية المعقدة وربطها بسيناريوهات عملية.
- خبرة في تدريب فرق الأمن السيبراني داخل الشركات الكبرى.
- **اللغات:** يجيد العربية والإنجليزية، مما يتيح استعراض أمثلة من السوق المحلي والدولي

ليه شهادة البورد الأمريكي المؤمنة مميزة في هذا الكورس؟

1. اعتماد دولي وموثوقية عالية :

يسهل التحقق من صحتها دوليًا، مما يضيف مصداقية للمتخصص أمام الشركات العالمية.

2. قيمة مضافة للمشاركين :

الشهادة تفتح فرص عمل في شركات دولية كبرى أو مع عملاء أجانب. وتعطي ميزة تنافسية قوية في سوق العمل المتطلب.

3. تعزيز الثقة في سوق الأمن السيبراني :

المجال حساس ويتعلق بأمن بيانات المؤسسات، ووجود شهادة دولية مؤمنة يعطي إشارة بأن المتدرب مؤهل علميًا وموثوق.

الأنشطة العملية (Labs & Workshops)

- **مشاريع تطبيقية:** عمل خطة استجابة لحادث سيبراني لمؤسسة افتراضية.
- **محاكاة واقعية:** استخدام معامل افتراضية (Virtual Labs) لتطبيق تقنيات الدفاع والهجوم.
- **دراسات حالة:** تحليل هجمات سيبرانية حقيقية وكيفية التعامل معها.

الأدوات والبرامج المستخدمة

- التعريف بأشهر أدوات الأمن السيبراني مثل Wireshark, Nmap, Metasploit.
- تدريبات عملية على أنظمة كشف التسلل (IDS) والجدران النارية (Firewalls).
- إشارة لتطبيقات الذكاء الاصطناعي في تحليل التهديدات السيبرانية.

المميزات الحصرية للمتدرب

- **الحصول على نماذج جاهزة:** سياسات أمنية - خطط استجابة للحوادث - تقارير تقييم مخاطر.
- استشارات مجانية لمدة شهر بعد الكورس.
- الانضمام لمجموعة خاصة (WhatsApp/Telegram) للتواصل المستمر مع المحاضر وزملاء الكورس.

رسالة من شركة أوميديك

في أوميديك، نؤمن أن المعرفة هي أقصر الطرق نحو القوة والتميز. لقد صممنا هذا البرنامج التدريبي في الأمن السيبراني ليكون أكثر من مجرد كورس، بل خطوة عملية حقيقية نحو بناء مستقبل مهني آمن وناجح. هدفنا أن نمكن كل مشارك من أدوات ومعرفة عالمية، مدعومة بخبرة واقعية وشهادة دولية مؤمنة، تمنحه الثقة ليصبح خبيرًا في مجاله. إذا كنت تقرأ هذا الملف الآن، فاعلم أن الاستثمار في نفسك هو أول وأذكى استثمار يمكن أن تقوم به، ونحن هنا لنسير معك في هذه الرحلة خطوة بخطوة.

أهلاً بك في عالم أوميديك - حيث يبدأ المستقبل من هنا.